A Nearly Optimal Lower Bound on the Approximate Degree of AC^0

Mark Bun — Princeton University

Justin Thaler — Georgetown University

Boolean Functions

$f:\{\text{-}1,\,1\}^n \rightarrow \{\text{-}1,\,1\}$

where -1 = TRUE and $+1$ = FALSE

<u>Ex.</u>

$$\text{AND}_n(x) = \begin{cases} -1 & \text{if } x = (-1)^n \\ 1 & \text{otherwise} \end{cases}$$

Approximate Degree

[Nisan-Szegedy92]

A real polynomial p ε-approximates Boolean f if

$$|\, p(x) - f(x)| \leq \varepsilon \quad \text{for all} \quad x \in \{-1, 1\}^n$$

$$\deg_\varepsilon(f) := \min\{\, d : \text{There is a degree-}d\text{ polynomial } p \text{ that } \varepsilon\text{-approximates } f\,\}$$

$\widetilde{\deg}(f) := \deg_{1/3}(f)$ is the approximate degree of f

Applications (Upper Bounds)

Learning Algorithms

$\varepsilon = 1/3$ *Agnostic Learning* [Kalai-Klivans-Mansour-Servedio05]

$\varepsilon = 1 - 2^{-\mathrm{poly}(n)}$ *Attribute-Efficient Learning*

[Klivans-Servedio06, Servedio-Tan-Thaler12]

$\varepsilon \to 1$ *PAC Learning* [Klivans-Servedio03]

Approximate Inclusion-Exclusion

[Kahn-Linial-Samorodnitsky96, Sherstov08]

Differentially Private Query Release

[Thaler-Ullman-Vadhan12, Chandrasekaran-Thaler-Ullman-Wan14]

Formula & Graph Complexity *Lower Bounds*

[Tal14,16ab]

Applications (Lower Bounds)

Approx. degree lower bounds ⇒ lower bounds in

- Quantum Query Complexity

  [Beals-Burhman-Cleve-Mosca-deWolf98, Aaronson-Shi02]
- Communication Complexity

  [Sherstov07, Shi-Zhu07, Chattopadhyay-Ada08, Lee-Shraibman08,…]
- Circuit Complexity

  [Minsky-Papert69, Beigel93, Sherstov08]

Oracle Separations [Beigel94, Bouland-Chen-Holden-Thaler-Vasudevan16]

Secret Sharing Schemes [Bogdanov-Ishai-Viola-Williamson16]

Approximate Degree of AC^0

AC^0 = $\{\wedge, \vee, \neg\}$-circuits (with unbounded fan-in) of constant depth and polynomial size

Approximate degree lower bounds underlie the best known lower bounds for AC^0 under:

- Approximate rank / quantum comm. complexity
- Multiparty (quantum) comm. complexity
- Discrepancy / margin complexity
- Sign-rank / unbounded error comm. complexity
- Majority-of-threshold and threshold-of-majority circuit size

Open Problem: What is the approximate degree of AC^0?

Approximate Degree of AC^0

Prior work:

$\text{Element-Distinctness}$ is a CNF with approximate degree $\Omega(n^{2/3})$ [Aaronson-Shi02]

This work:

<u>Main Theorem:</u> For every $\delta > 0$, there is an AC^0 circuit with approximate degree $\Omega(n^{1-\delta})$

- Depth = $\mathrm{O}(\log(1/\delta))$
- Also applies to DNF of width $(\log n)^{\mathrm{O}(\log(1/\delta))}$ (with quasipolynomial size)

Applications of Main Theorem

- An AC^0 circuit with *quantum communication complexity* $\Omega(n^{1-\delta})$

  Main Theorem + Pattern Matrix Method [Sherstov07]

- Improved *secret sharing schemes* with reconstruction in AC^0

  Main Theorem + [Bogdanov-Ishai-Viola-Williamson16]

- Nearly optimal separation between *certificate complexity* and approximate degree

  Main Theorem + some actual work

Roadmap

- Story 1: *Symmetrization* and the approximate degree of AND [Nisan-Szegedy92]

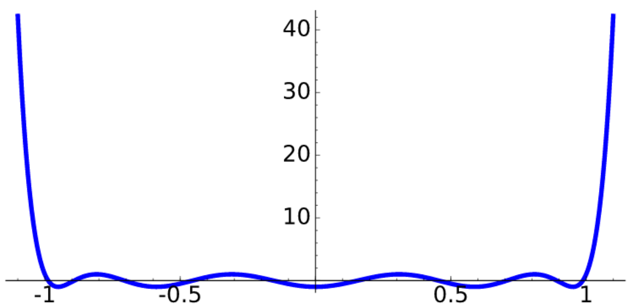
- Story 2: *Dual polynomials* and the approximate degree of AND-OR [B.-Thaler13 Sherstov13]

- Story 3: Hardness amplification in AC^0
  $\Rightarrow$ Main Theorem

Approximate Degree of AND_n

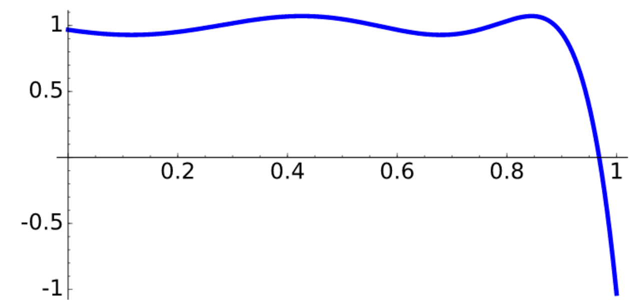
<u>Theorem:</u> $\widetilde{\deg}(\mathrm{AND}_n) = \Theta(n^{1/2})$ [Nisan-Szegedy92]

Upper bound: *Chebyshev polynomials*



$T_d(t)$

Affine Transformation



$Q_d(t)$

Approximate Degree of AND_n

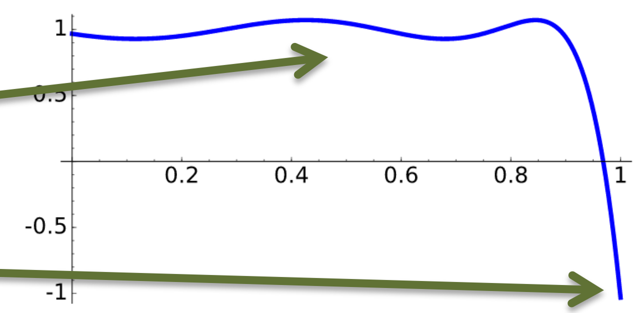
<u>Theorem:</u> $\widetilde{\deg}(\mathrm{AND}_n) = \Theta(n^{1/2})$ [Nisan-Szegedy92]

Upper bound: *Chebyshev polynomials*

For $d = O(n^{1/2})$:

$Q_d(t) \in [2/3, 4/3]$ for all $t \in [0, 1-1/n]$

$Q_d(1) = -1$



$Q_d(t)$

Approximating polynomial:

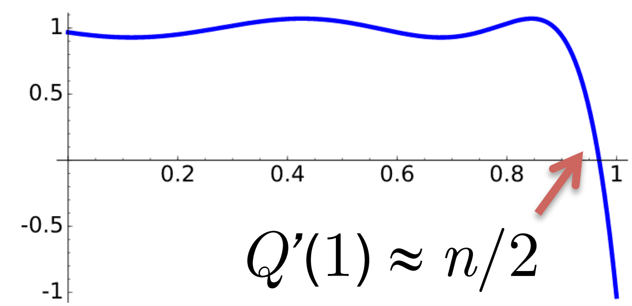
$$p(x) = Q_d(|x|/n) = Q_d(1/2 - ((x_1 + \ldots + x_n)/2n))$$

Approximate Degree of AND$_n$

<u>Theorem:</u> $\widetilde{\deg}(\text{AND}_n) = \Theta(n^{1/2})$ [Nisan-Szegedy92]

Lower bound: *Symmetrization* [Minsky-Papert69]

If $|p(x) - \text{AND}_n(x)| \leq 1/3$ for all $x \in \{-1, 1\}^n$, then there exists a **univariate** Q with $\deg(Q) \leq \deg(p)$ that looks like:



Markov's Inequality:

$$\max_{[0,1]} Q'(t) \leq (\deg(Q))^2 \cdot \max_{[0,1]} |Q(t)|$$

(Chebyshev polynomials are the extremal case)

$$\Rightarrow \deg(p) \geq \deg(Q) \geq \Omega(n^{1/2})$$

Approximate Degree of AND_n

Theorem: $\widetilde{\deg}(\text{AND}_n) = \Theta(n^{1/2})$ [Nisan-Szegedy92]

Lower bound: *Symmetrization* [Minsky-Papert69]

Symmetrization + Approximation Theory gives tight lower bounds for

- Symmetric Boolean functions [Paturi92]
- $\text{Element Distinctness}$ [Aaronson-Shi02]

Roadmap

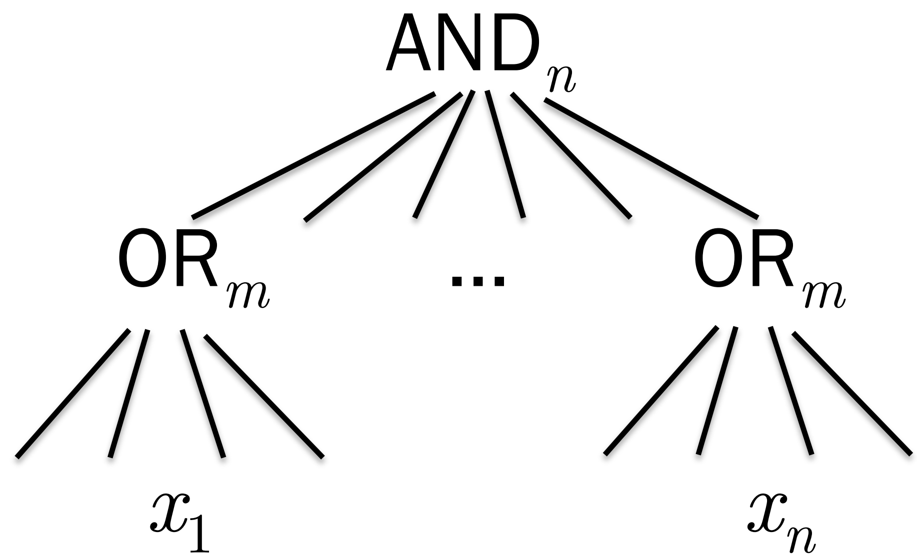
- Story 1: *Symmetrization* and the approximate degree of AND [Nisan-Szegedy92]

- Story 2: *Dual polynomials* and the approximate degree of AND-OR [B.-Thaler13 Sherstov13]

- Story 3: Hardness amplification in AC^0
  $\Rightarrow$ Main Theorem

The AND-OR Tree

Define $\mathrm{AND}_n \circ \mathrm{OR}_m : \{-1, 1\}^{nm} \rightarrow \{-1, 1\}$ by



<u>Theorem:</u> $\widetilde{\deg}(\mathrm{AND}_n \circ \mathrm{OR}_m) = \Theta(n^{1/2} m^{1/2})$

Approximate Degree of $\text{AND}_n \circ \text{OR}_m$

<u>Upper bound:</u> $\widetilde{\deg}(\text{AND}_n \circ \text{OR}_m) = O(n^{1/2} m^{1/2})$

- Quantum query algorithm [Hoyer-Mosca-deWolf03]
- General proof via *robust* polynomials

  [Buhrman-Newman-Röhrig-deWolf03, Sherstov12]

<u>Theorem:</u> For any functions f and g, we have

$$\widetilde{\deg}(f \circ g) \leq O(\widetilde{\deg}(f) \cdot \widetilde{\deg}(g))$$

Given $p \approx f$ and $q \approx g$, is $p \circ q \approx f \circ g$?

Not in general. But p can be made *robust to noise* in its inputs (without increasing its degree)

Approximate Degree of $\text{AND}_n \circ \text{OR}_m$

<u>Lower bound:</u> $\widetilde{\deg}(\text{AND}_n \circ \text{OR}_m) = \Omega(n^{1/2}m^{1/2})$

- Symmetrization alone does not seem powerful enough

  [Nisan-Szegedy92, Shi01, Ambainis03]

- Proof via *method of dual polynomials*

  [B.-Thaler13, Sherstov13]

The Method of Dual Polynomials

What is the best error ε to which a degree-d polynomial can approximate f?

Primal LP:
$$\min_{p,\varepsilon} \quad \varepsilon$$
$$\text{s.t.} \quad |p(x) - f(x)| \leq \varepsilon \quad \forall x \in \{-1,1\}^n$$

Dual LP:
$$\max_{\Psi} \sum_{x\in\{-1,1\}^n} \Psi(x) f(x)$$
$$\text{s.t.} \sum_{x\in\{-1,1\}^n} |\Psi(x)| = 1$$
$$\deg(p) \leq d \implies \sum_{x\in\{-1,1\}^n} \Psi(x) p(x) = 0$$

The Method of Dual Polynomials

Theorem: $\deg_\varepsilon(f) > d$ **if and only if** there exists a *dual polynomial* Ψ such that

1. $$\sum_{x \in \{-1,1\}^n} |\Psi(x)| = 1$$ (Ψ has L_1-*norm* 1)

2. $$\deg(p) \le d \implies \sum_{x \in \{-1,1\}^n} \Psi(x) p(x) = 0$$ (Ψ has *pure high degree* d)

3. $$\sum_{x \in \{-1,1\}^n} \Psi(x) f(x) > \varepsilon$$ (Ψ has *correlation* ε with f)

Approximate Degree of $\mathrm{AND}_n \circ \mathrm{OR}_m$

Lower bound: $\widetilde{\deg}(\mathrm{AND}_n \circ \mathrm{OR}_m) = \Omega(n^{1/2} m^{1/2})$

Proof idea (explicit in [B.-Thaler13], implicit in [Sherstov13])

- Begin with dual polynomials

  Ψ_{AND} witnessing $\widetilde{\deg}(\mathrm{AND}_n) > n^{1/2}$, and

  Ψ_{OR} witnessing $\widetilde{\deg}(\mathrm{OR}_m) > m^{1/2}$

- Combine Ψ_{AND} with Ψ_{OR} to obtain a dual polynomial $\Psi_{\mathrm{AND\text{-}OR}}$ for $\mathrm{AND}_n \circ \mathrm{OR}_m$

  Uses *dual block composition* technique

Dual Block Composition

[Shi-Zhu07, Lee09, Sherstov09]

Combine dual polynomials Ψ_f and Ψ_g via

$$\Psi_{f\circ g}(x) = 2^n \Psi_f(\operatorname{sgn}\Psi_g(x_1), \ldots, \operatorname{sgn}\Psi_g(x_n)) \prod_{i=1}^{n} |\Psi_g(x_i)|$$

Normalization to ensure $\Psi_{f\circ g}$ has L_1-norm 1

Booleanization of $(\Psi_g(x_1), \ldots, \Psi_g(x_n))$

Product distribution $|\Psi_g|$ x … x $|\Psi_g|$

By complementary slackness, tailored to showing optimality of robust approximations [Thaler14]

Dual Block Composition

[Shi-Zhu07, Lee09, Sherstov09]

Combine dual polynomials Ψ_f and Ψ_g via

$$\Psi_{f \circ g}(x) = 2^n \Psi_f(\operatorname{sgn} \Psi_g(x_1), \ldots, \operatorname{sgn} \Psi_g(x_n)) \prod_{i=1}^{n} |\Psi_g(x_i)|$$

1. $\Psi_{f \circ g}$ has L_1-norm 1 [Sherstov09]

2. $\Psi_{f \circ g}$ has pure high degree d [Sherstov09]

3. f = AND$_n$ and g = OR$_m$ ⇒ $\Psi_{f \circ g}$ has high correlation with $f \circ g$ [B.-Thaler13, Sherstov13]

Roadmap

- Story 1: *Symmetrization* and the approximate degree of AND [Nisan-Szegedy92]

- Story 2: *Dual polynomials* and the approximate degree of AND-OR [B.-Thaler13 Sherstov13]

- Story 3: Hardness amplification in AC^0 $\Rightarrow$ Main Theorem

Hardness Amplification in AC^0

Theorem 1: If $\widetilde{\deg}_{-,1/2}(f) > d$, then $\widetilde{\deg}_{1/2}(F) > t^{1/2}d$ for $F = \mathrm{OR}_t \circ f$ [B.-Thaler13, Sherstov13]

Theorem 2: If $\widetilde{\deg}_{-,1/2}(f) > d$, then $\widetilde{\deg}_{1-2^{-t}}(F) > d$ for $F = \mathrm{OR}_t \circ f$ [B.-Thaler14]

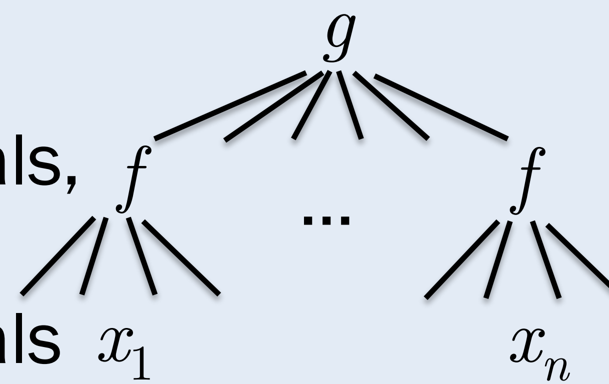
Theorem 3: If $\widetilde{\deg}_{-,1/2}(f) > d$, then $\deg_{\pm}(F) > \min\{t, d\}$ for $F = \mathrm{OR}_t \circ f$ [Sherstov14]

Theorem 4: If $\widetilde{\deg}_{+,1/2}(f) > d$, then $\widetilde{\deg}_{1-2^{-t}}(F) > d$ for $F = \text{ODD-MAX-BIT}_t \circ f$ [Thaler14]

Theorem 5: If $\widetilde{\deg}_{1/2}(f) > d$, then $\deg_{\pm}(F) > \min\{t, d\}$ for $F = \text{APPROX-MAJ}_t \circ f$ [Bouland-Chen-Holden-Thaler-Vasudevan16]

Hardness Amplification in AC^0

Theorem Template: If f is “hard” to approximate by low-degree polynomials, then $F = g \circ f$ is “even harder” to approximate by low-degree polynomials



Block Composition Barrier

Robust approximations, i.e.,

$$\widetilde{\deg}(g \circ f) \leq \mathrm{O}(\widetilde{\deg}(g) \cdot \widetilde{\deg}(f))$$

imply that block composition *cannot* increase approximate degree as a function of n

This Work: A New Hardness Amplification Theorem for Degree

Theorem: If $f : \{\text{-}1,\ 1\}^n \rightarrow \{\text{-}1,\ 1\}$

- is computed by a depth-k AC^0 circuit, and
- has approximate degree $\geq d$,

then there exists $F : \{\text{-}1,\ 1\}^{n \text{ polylog}(n)} \rightarrow \{\text{-}1,\ 1\}$ that

- is computed by a depth-$(k+3)$ AC^0 circuit, and
- has approximate degree $\geq \Omega(d^{2/3} \cdot n^{1/3})$

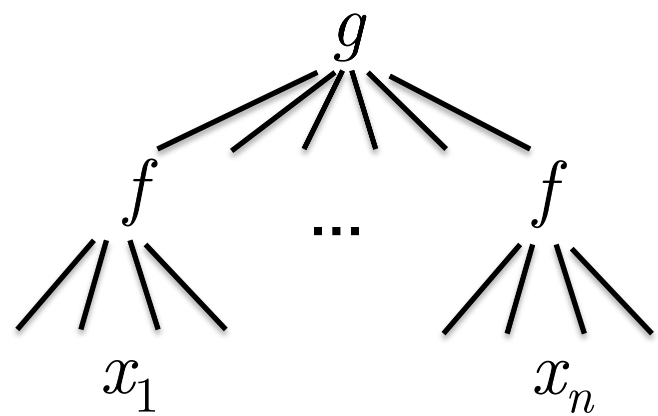
Remarks:

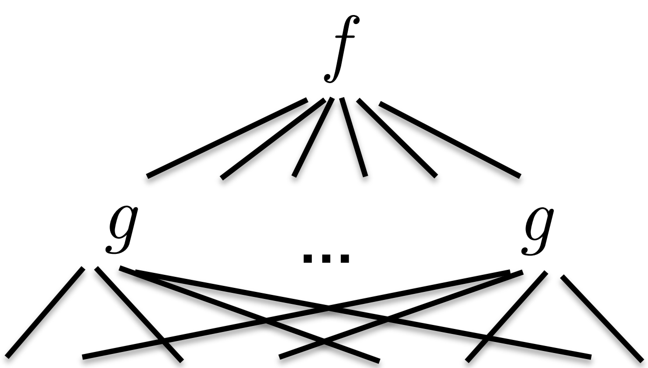
- Recursive application yields Main Theorem
- Analogous result for (monotone) DNF

Around the Block Composition Barrier

Prior work:

- Hardness amplification "from the top"
- Block composed functions





This work:

- Hardness amplification "from the bottom"
- Non-block-composed functions

Case Study: SURJECTIVITY

For $N \geq R$, define $\text{SURJ}_{N,R} : [R]^N \to \{\text{-}1, 1\}$ by

$\text{SURJ}_{N,R}(s_1, \ldots, s_N) = -1$ iff

For every $r \in [R]$, there exists an index i s.t. $s_i = r$

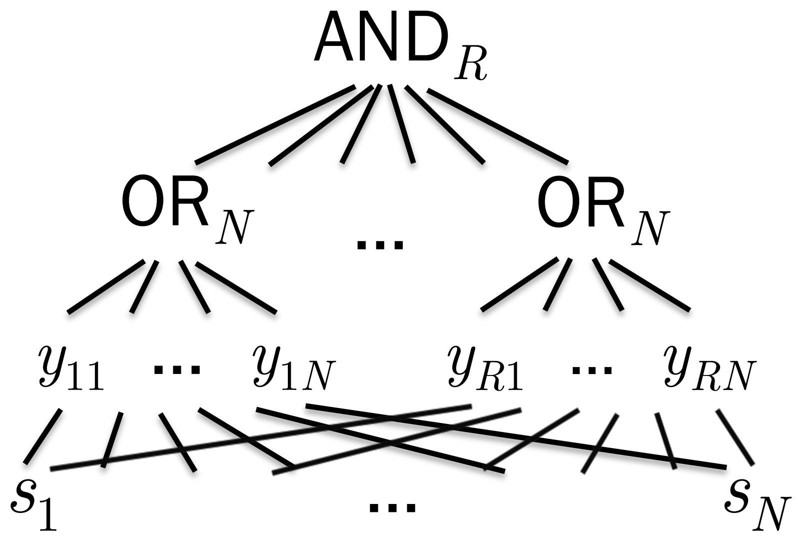
- Corresponds to a Boolean function on $\mathrm{O}(N \log_2 R)$ bits
- Has nearly maximal *quantum query complexity* $\Omega(R)$ [Beame-Machmouchi10]
- Exactly the outcome of hardness amplification construction applied to $f = \text{AND}_R$

Getting to Know SURJECTIVITY

SURJ$_{N,R}(s_1, \ldots, s_N) = -1$ iff
For every $r \in [R]$, there exists an index i s.t. $s_i = r$

Define auxiliary variables

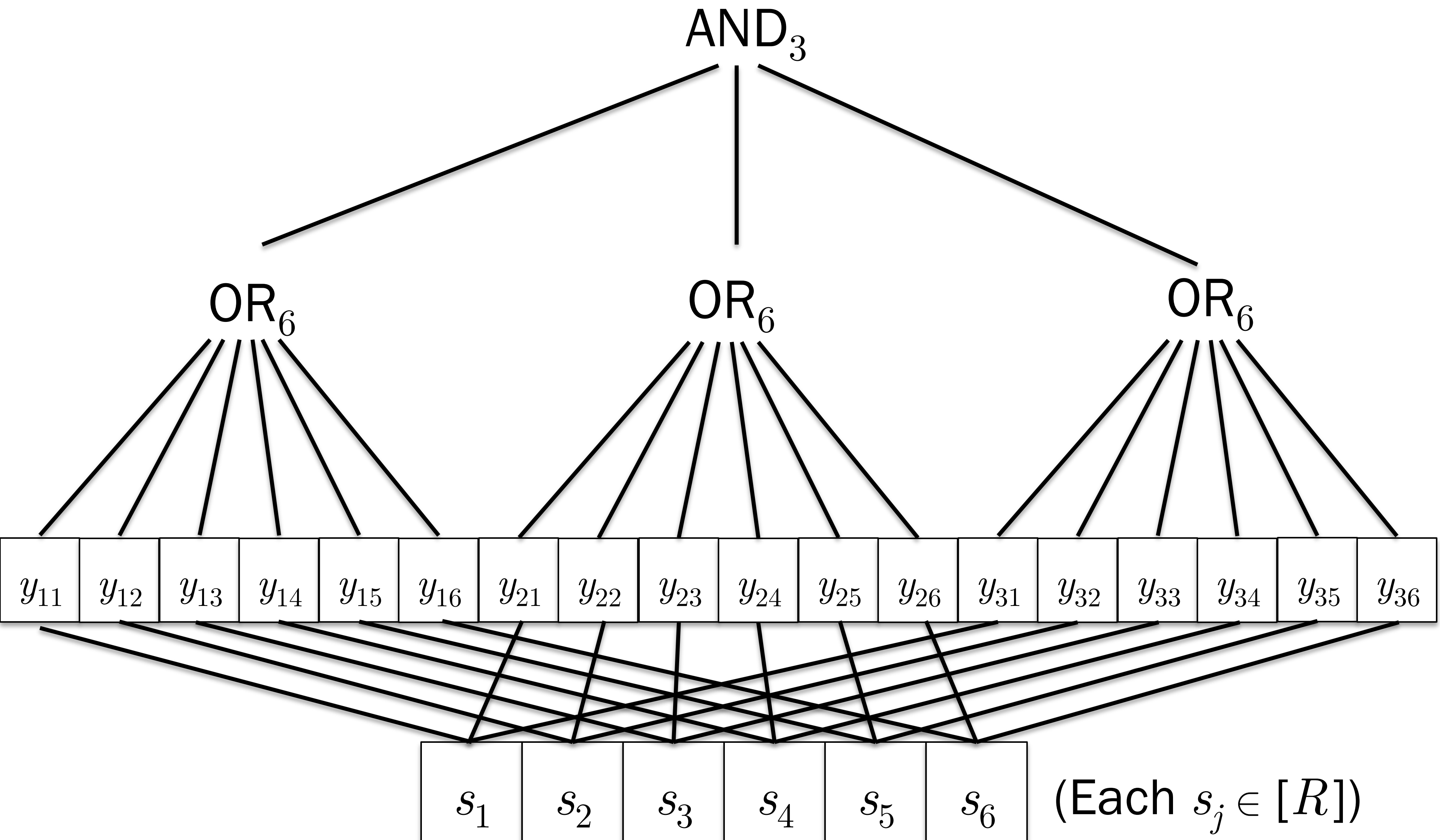
$$y_{r,i}(s) = \begin{cases} -1 & \text{if } s_i = r \\ 1 & \text{otherwise} \end{cases}$$



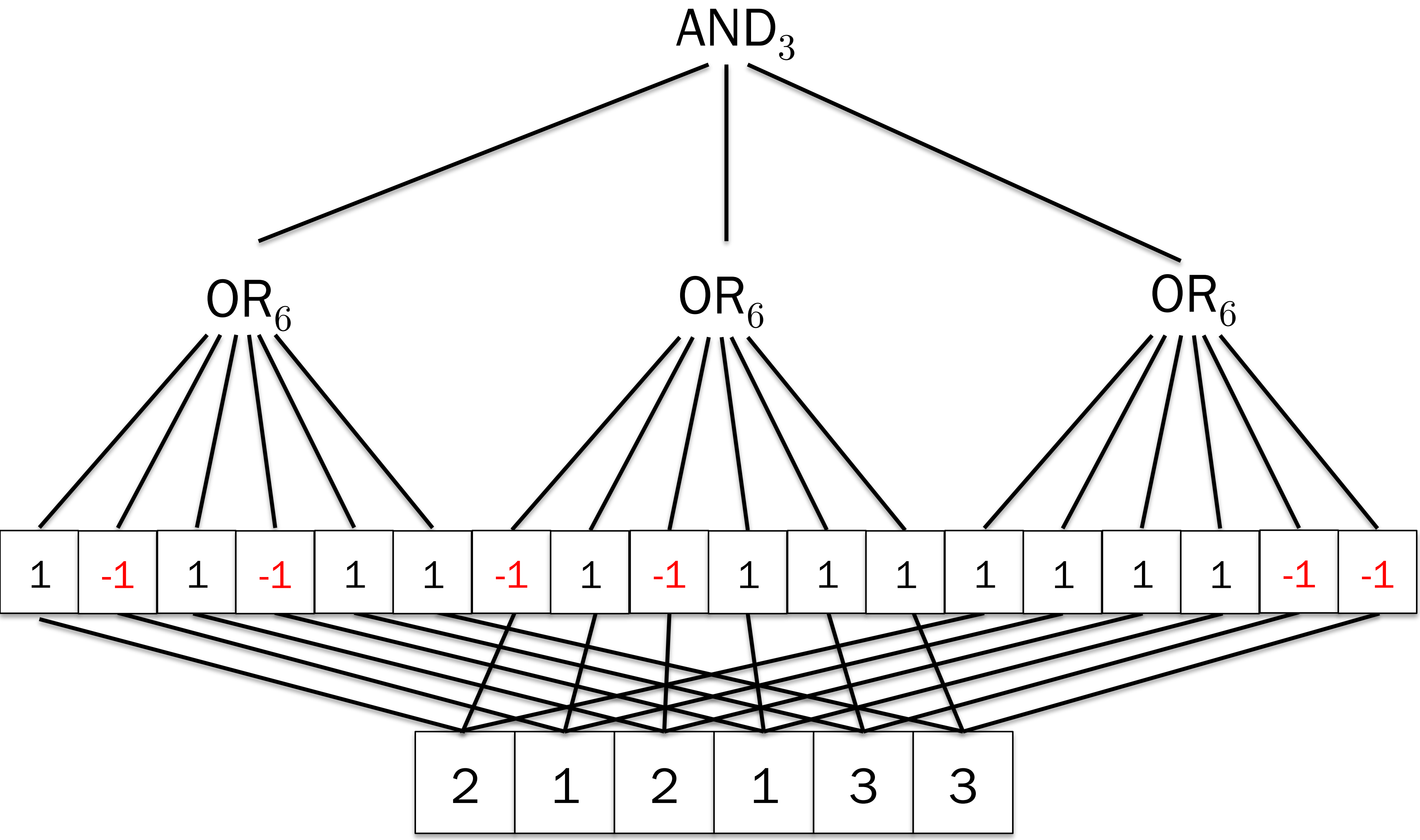
Then SURJ$_{N,R}(s_1, \ldots, s_N)$ =

AND$_R$ (OR$_N$ ($y_{11}, \ldots, y_{1N}$), ..., OR$_N$ ($y_{R1}, \ldots, y_{RN}$))

SURJECTIVITY Illustrated ($N=6,\ R=3$)



SURJECTIVITY Illustrated ($N=6,\ R=3$)



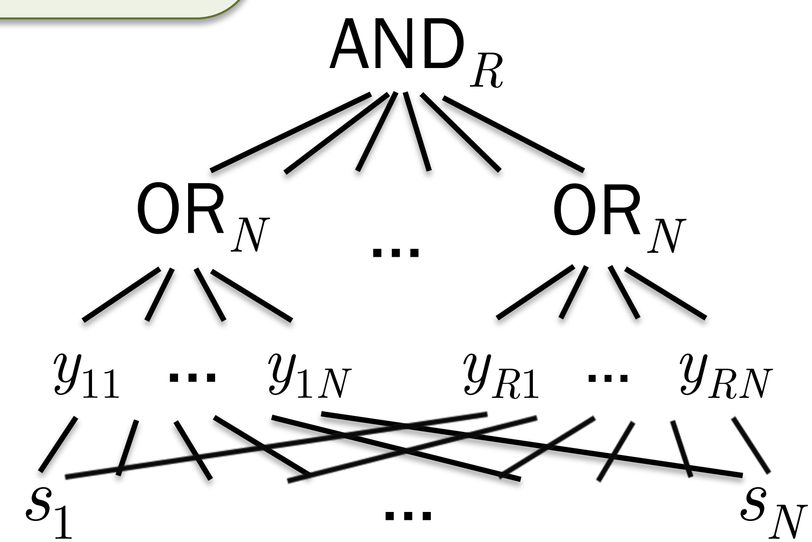
Getting to Know SURJECTIVITY

Observation: To approximate $\mathrm{SURJ}_{N,R}$, it suffices to approximate $\mathrm{AND}_R \circ \mathrm{OR}_N$ on inputs of Hamming weight N

ndex i s.t. $s_i = r$

Define auxiliary variables

$$y_{r,i}(s) = \begin{cases} -1 & \text{if } s_i = r \\ 1 & \text{otherwise} \end{cases}$$

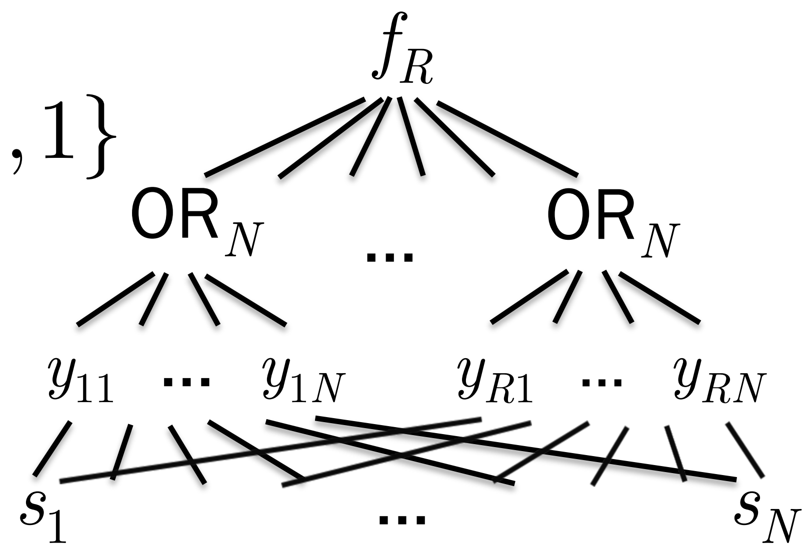


Then $\mathrm{SURJ}_{N,R}(s_1, \ldots, s_N) =$

$$\mathrm{AND}_R(\,\mathrm{OR}_N(y_{11}, \ldots, y_{1N}), \ldots, \mathrm{OR}_N(y_{R1}, \ldots, y_{RN})\,)$$

General Hardness Amplification Construction

Natural generalization for an arbitrary $f : \{-1,1\}^R \to \{-1,1\}$



$F(s_1, \ldots, s_N) =$
$f(\mathrm{OR}_N(y_{11}, \ldots, y_{1N}), \ldots, \mathrm{OR}_N(y_{R1}, \ldots, y_{RN}))$

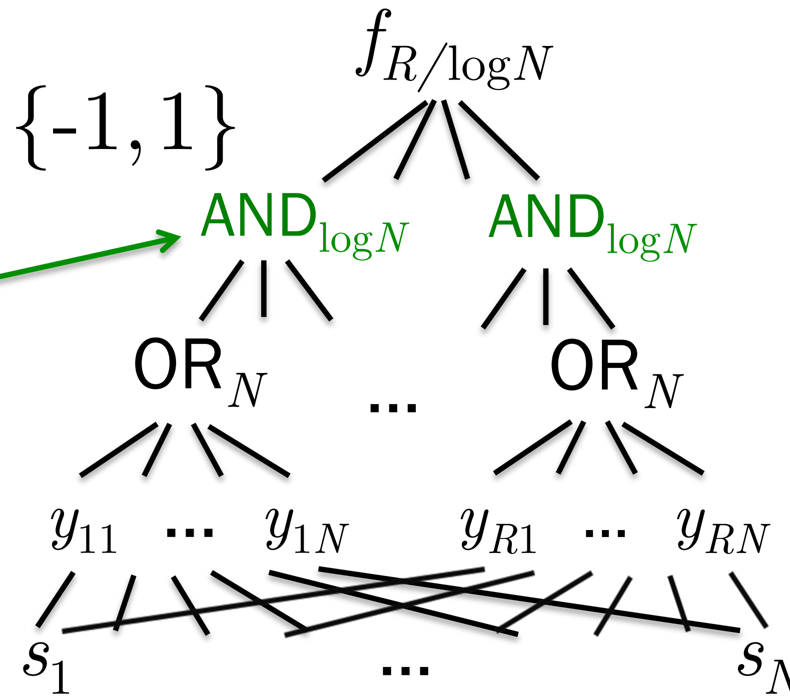
Fails dramatically for $f = \mathrm{OR}_R$! ($F(s)$ identically -1)

General Hardness Amplification Construction

Actual generalization for an

arbitrary $f : \{\text{-}1, 1\}^{R/\log N} \rightarrow \{\text{-}1, 1\}$

Fix: Force a level of alternation



$F(s_1, \ldots, s_N) =$

$(f \circ \mathrm{AND}_{\log N})(\mathrm{OR}_N(y_{11}, \ldots, y_{1N}), \ldots, \mathrm{OR}_N(y_{R1}, \ldots, y_{RN}))$

Remainder of This Talk:
Lower Bound for SURJECTIVITY

Overview of SURJECTIVITY Lower Bound

Theorem: For some $N = O(R)$,

$$\widetilde{\deg}(\mathsf{SURJ}_{N,R}) = \Omega(R^{2/3}) = \Omega(\widetilde{\deg}(\mathsf{AND}_R)^{2/3} \cdot R^{1/3})$$

(New proof of result of [Aaronson-Shi01, Ambainis03])

Stage 1: Apply *symmetrization* to reduce to

Builds on [Ambainis03]

Claim: $\widetilde{\deg}(\mathsf{AND}_R \circ \mathsf{OR}_N) = \Omega(R^{2/3})$ *even under the promise* that $|x| \leq N$

Stage 2: Prove Claim via *method of dual polynomials*

Refines AND-OR dual polynomial w/ techniques of [Razborov-Sherstov08]

Details of Stage 1

<u>Goal:</u> Transform

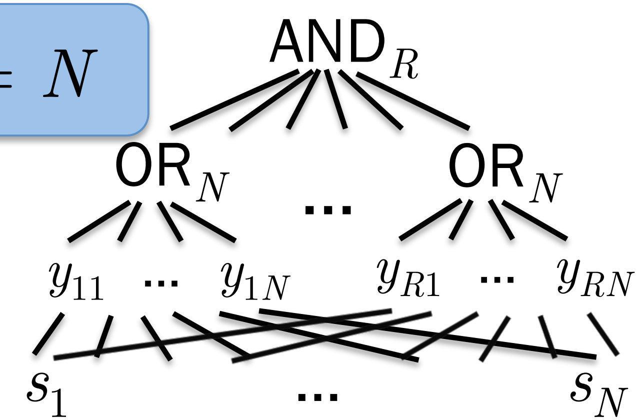
$p \approx \text{SURJ}_{N,R}$ into $q \approx \text{AND}_R \circ \text{OR}_N$ for $|x| \leq N$,

such that $\deg(q) \leq \deg(p)$

a) Symmetrize p to obtain P which depends only on Hamming weights $|y_1|, \ldots, |y_R|$ [Ambainis03]

$(s_1, \ldots, s_N) \in [R]^N$ iff $|y_1| + \ldots + |y_R| = N$

b) Let $q(x) = P(|x_1|, \ldots, |x_R|)$



Details of Stage 2

<u>Claim:</u> $\widetilde{\deg}(\mathrm{AND}_R \circ \mathrm{OR}_N) = \Omega(R^{2/3})$ even under the promise that $|x| \leq N$

is equivalent to

There exists a dual polynomial witnessing $\widetilde{\deg}(\mathrm{AND}_R \circ \mathrm{OR}_N) = \Omega(R^{2/3})$ which is supported on inputs with $|x| \leq N$

Does the dual polynomial we already constructed for $\mathrm{AND}_R \circ \mathrm{OR}_N$ satisfy this property? **NO**

Fixing the AND-OR Dual Polynomial

$$\Psi_{\text{AND-OR}}(x) = 2^R \Psi_{\text{AND}}(\operatorname{sgn}\Psi_{\text{OR}}(x_1), \ldots, \operatorname{sgn}\Psi_{\text{OR}}(x_R)) \prod_{i=1}^{R} |\Psi_{\text{OR}}(x_i)|$$

Ψ_{OR} *must* be nonzero for inputs with Hamming weight up to $\Omega(N)$

$\Rightarrow \Psi_{\text{AND-OR}}$ nonzero up to Hamming weight $\Omega(RN)$

1. $\Psi_{\text{AND-OR}}$ has L_1-norm 1 ✓
2. $\Psi_{\text{AND-OR}}$ has pure high degree $\Omega(R^{1/2}N^{1/2}) = \Omega(R)$ ✓
3. $\Psi_{\text{AND-OR}}$ has high correlation with $\text{AND}_R \circ \text{OR}_N$ ✓
4. $\Psi_{\text{AND-OR}}$ is supported on inputs with $|x| \leq N$ ✗

Fixing the AND-OR Dual Polynomial

$$\Psi_{\text{AND-OR}}(x) = 2^R \Psi_{\text{AND}}(\operatorname{sgn}\Psi_{\text{OR}}(x_1), \ldots, \operatorname{sgn}\Psi_{\text{OR}}(x_R)) \prod_{i=1}^{R} |\Psi_{\text{OR}}(x_i)|$$

Ψ_{OR} *must* be nonzero for inputs with Hamming weight up to $\Omega(N)$

$\Rightarrow \Psi_{\text{AND-OR}}$ nonzero up to Hamming weight $\Omega(RN)$

Fix 1: Trade pure high degree of Ψ_{OR} for "support" size

Fix 2: Zero out high Hamming weight inputs to $\Psi_{\text{AND-OR}}$

Fix 1: Trading PHD for Support Size

For every integer $1 \leq k \leq N$, there is a dual polynomial Ψ^k_{OR} for OR_N which

- has pure high degree $\Omega(k^{1/2})$
- is supported on inputs of Hamming weight $\leq k$

$$\Psi^k_{\text{AND-OR}}(x) = 2^R \Psi_{\mathrm{AND}}(\operatorname{sgn}\Psi^k_{\mathrm{OR}}(x_1), \ldots, \operatorname{sgn}\Psi^k_{\mathrm{OR}}(x_R)) \prod_{i=1}^{R} |\Psi^k_{\mathrm{OR}}(x_i)|$$

Dual polynomial $\Psi^k_{\text{AND-OR}}$

- has pure high degree $\Omega(R^{1/2}\, k^{1/2})$
- is supported on inputs of Hamming weight $\leq kN$

Fix 2: Zeroing Out High Hamming Weight Inputs

Dual polynomial $\Psi^k_{\text{AND-OR}}$
- has pure high degree $\Omega(R^{1/2}\, k^{1/2})$
- is supported on inputs of Hamming weight $\leq kN$

Suppose further that $$\sum_{|x|>N} |\Psi^k_{\text{AND-OR}}(x)| \ll \text{negl}(R)$$

Can we post-process $\Psi^k_{\text{AND-OR}}$ to zero out inputs with Hamming weight $N < |x| \leq kN$...

...without ruining
- pure high degree of $\Psi^k_{\text{AND-OR}}$
- correlation between $\Psi^k_{\text{AND-OR}}$ and $\text{AND}_R \circ \text{OR}_N$?

YES (Follows from [Razborov-Sherstov-08])

Fix 2: Zeroing Out High Hamming Weight Inputs

Technical Lemma (follows from [Razborov-Sherstov08])

If $0 < D < N$ and

$$\sum_{|x|>N} |\Psi^k_{\text{AND-OR}}(x)| \ll 2^{-D},$$

then there exists a "correction term" Ψ^k_{corr} that

1. Agrees with $\Psi^k_{\text{AND-OR}}$ inputs of Hamming weight $> N$
2. Has L_1-norm 0.01
3. Has pure high degree D

Fix 2: Zeroing Out High Hamming Weight Inputs

<u>Claim:</u> For $1 \leq k \leq N$, $$\sum_{|x|>N} |\Psi^k_{\text{AND-OR}}(x)| \ll 2^{-R/k}$$

<u>Proof idea:</u>

Ψ^k_{OR} can be made "weakly biased" toward low Hamming weight inputs: For all $t > 0$, $\sum_{|x|=t} |\Psi^k_{\text{OR}}(t)| \lesssim \frac{1}{t^2}$

$\Rightarrow$ "Worst" high Hamming weight inputs look like

$|x_1| = k, \ldots, |x_{R/k}| = k, |x_{(R/k)+1}| = 0, \ldots, |x_R| = 0$

$$\Psi^k_{\text{AND-OR}}(x) = 2^R \Psi_{\text{AND}}(\operatorname{sgn} \Psi^k_{\text{OR}}(x_1), \ldots, \operatorname{sgn} \Psi^k_{\text{OR}}(x_R)) \boxed{\prod_{i=1}^{R} |\Psi^k_{\text{OR}}(x_i)|}$$

Weight on such inputs looks like $k^{-R/k}$

Putting the Pieces Together

Dual polynomial $\Psi^k_{\text{AND-OR}}$ Fix 1

- has pure high degree $\Omega(R^{1/2}\, k^{1/2})$
- satisfies $\sum_{|x|>N} |\Psi^k_{\text{AND-OR}}(x)| \ll 2^{-R/k}$

Balanced at $k = R^{1/3}$
$\Rightarrow$ PHD $\Omega(R^{2/3})$

Correction term Ψ^k_{corr}

- has pure high degree $\Omega(R/k)$
- agrees with $\Psi^k_{\text{AND-OR}}$ inputs of Hamm weight $> N$

$\Rightarrow \Psi_{\text{AND-OR}} = \boxed{\Psi^k_{\text{AND-OR}} - \Psi^k_{\text{corr}}}$ has

1. L_1-norm ≈ 1
2. high correlation with $\text{AND}_R \circ \text{OR}_N$
3. pure high degree $\Omega(\min\{R^{1/2}k^{1/2},\ R/k\})$
4. support on inputs with $|x| \leq N$

Recap of SURJECTIVITY Lower Bound

Theorem: For some $N = \mathrm{O}(R)$,

$$\widetilde{\deg}(\text{SURJ}_{N,R}) = \Omega(R^{2/3}) = \Omega(\widetilde{\deg}(\text{AND}_R)^{2/3} \cdot R^{1/3})$$

(New proof of result of [Aaronson-Shi01, Ambainis03])

Stage 1: Apply *symmetrization* to reduce to ✓

Builds on [Ambainis03]

Claim: $\widetilde{\deg}(\text{AND}_R \circ \text{OR}_N) = \Omega(R^{2/3})$ *even under the promise* that $|x| \leq N$

Stage 2: Prove Claim via *method of dual polynomials* ✓

Refines AND-OR dual polynomial w/ techniques of [Razborov-Sherstov08]

Conclusions I: Upcoming Work

This work: New degree amplification theorem

$\Rightarrow$ almost optimal approx. degree lower bound for AC^0

Upcoming work [B.-Thaler-Kothari]: Quantitative refinement to hardness amplification theorem, with applications

- $\widetilde{\deg}(\mathrm{SURJ}_{N,R}) = \Omega(R^{3/4})$

  Matches upper bound of Sherstov

- Nearly tight approx. degree / quantum query lower bounds for k-distinctness, junta testing, statistical distance, entropy comparison

Conclusions II: Open Problems

- Is there an AC^0 function with approximate degree $\Omega(n)$? A *polynomial* size DNF?

- Can we obtain similar bounds for ε close to 1?

  Conjecture: There exists $f \in AC^0$ with $\deg_\varepsilon(f) = \Omega(n^{1\text{-}\delta})$ even for $\varepsilon = 1 - 2^{-n^{1\text{-}\delta}}$

- What is the approx. degree of $\mathrm{APPROX\text{-}MAJ}$?

  [Srinivasan]

Thank you!