Dual Lower Bounds for Approximate Degree and Markov-Bernstein Inequalities

Mark Bun and Justin Thaler

Harvard University

July 8, 2013

Boolean Functions

- Boolean function $f : \{-1,1\}^n \to \{-1,1\}$
- $$\mathrm{OR}_n(x) = \begin{cases} 1 \quad \text{(FALSE)} & \text{if } x = 1^n \\ -1 \quad \text{(TRUE)} & \text{otherwise} \end{cases}$$

Approximate Degree

- p a real polynomial ϵ-approximates f if

$$|p(x) - f(x)| < \epsilon \quad \forall x \in \{-1, 1\}^n$$

- $\deg_\epsilon(f)$ = minimum degree needed to ϵ-approximate f
- $\widetilde{\deg}(f) := \deg_{1/3}(f)$ is the approximate degree of f

Applications

Lower bounds on $\widetilde{\deg}$

- Quantum query complexity [BBCMW98] [AS01] [Amb03] [KSW04]
- Communication complexity [BVW07] [She07] [SZ07] [CA08] [LS08] [She12]
- Circuit complexity [MP69] [Bei93] [Bei94] [She08]

Upper bounds on $\widetilde{\deg}$

- Learning theory [KS03] [KKMS06]
- Data privacy [TUV12] [CTUW13]

Our Contributions

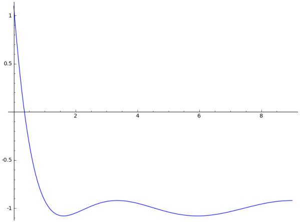
1. Tight lower bound on $\widetilde{\deg}\,\mathrm{AND\text{-}OR}$
   - Challenge problem in lower bounding approximate degree [Aar08]
   - Refines analysis of a "dual polynomial" due to [She09]
2. Explicit dual polynomials witnessing tight approximate degree lower bounds for <u>symmetric functions</u>
3. Dual proofs of Markov-type inequalities used to lower bound approximate degree

Lower Bounding Approximate Degree

[NS91] $\widetilde{\deg}\,\mathrm{OR}_n = \Theta(\sqrt{n})$, [Pat92] for symmetric functions

1. Symmetrize

   $p(x_1, \ldots, x_n) \approx \mathrm{OR}_n(x_1, \ldots, x_n) \Rightarrow P(y)$ with $\deg P \leq \deg p$



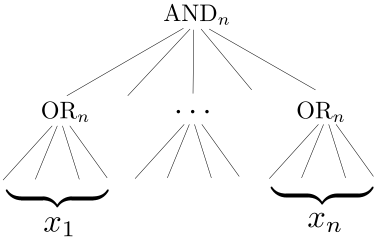
2. Markov-Bernstein inequality

   If $|P(y)| \leq 1$ for $y \in [-1, 1]$, then

$$|P'(y)| \leq \frac{\deg P}{\sqrt{1 - y^2}}$$

Lower Bounding Approximate Degree

- Symmetrization loses information
- Recent approaches focus on "moving beyond symmetrization"
- What is $\widetilde{\deg}\,\mathrm{AND\text{-}OR}_{n^2}$?



(Re-)posed by Aaronson at FOCS '08

Progress on the AND-OR Tree

Upper bounds

[HMW03] $\widetilde{\deg}\text{AND-OR}_{n^2} = O(n)$

Lower bounds

[NS91] $\Omega(\sqrt{n})$
[Shi01] $\Omega(\sqrt{n \log n})$
[Amb03] $\Omega(n^{2/3})$
[She09] $\Omega(n^{3/4})$

This work $\Omega(n)$
[She13] $\Omega(n)$, independently

Beyond Symmetrization via Dual Polynomials

Dual Characterization of Approximate Degree

Primal (Linear in ϵ and coefficients of p):

$$\begin{aligned} \min_{p,\epsilon} \quad & \epsilon \\ \text{s.t.} \quad & |p(x) - f(x)| \le \epsilon && \text{for all } x \in \{-1,1\}^n \\ & \deg p \le d \end{aligned}$$

Dual:

$$\begin{aligned} \max_{\psi} \quad & \sum_{x \in \{-1,1\}^n} \psi(x) f(x) \\ \text{s.t.} \quad & \sum_{x \in \{-1,1\}^n} |\psi(x)| = 1 \\ & \sum_{x \in \{-1,1\}^n} \psi(x) q(x) = 0 && \text{whenever } \deg q \le d \end{aligned}$$

Dual Characterization of Approximate Degree

Theorem: $\deg_\epsilon(f) > d$ iff there exists a "dual polynomial" ψ with

(1) $\sum_{x \in \{-1,1\}^n} \psi(x) f(x) > \epsilon$ "high correlation with f"

(2) $\sum_{x \in \{-1,1\}^n} |\psi(x)| = 1$ "L_1-norm 1"

(3) $\sum_{x \in \{-1,1\}^n} \psi(x) q(x) = 0, \deg q \leq d$ "pure high degree d"

Key technique in, e.g., [She07] [Lee09] [She09]

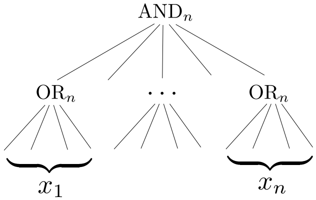
Goal: Construct an explicit dual polynomial $\psi_{\textsf{\textbf{AND-OR}}}$ for $\mathrm{AND\text{-}OR}$

Constructing a Dual Polynomial

- By [NS91], there are dual polynomials
  $\psi_{\textsf{\textbf{OUT}}}$ for $\widetilde{\deg}\,\mathrm{AND}_n = \Omega(\sqrt{n})$ and
  $\psi_{\textsf{\textbf{IN}}}$ for $\widetilde{\deg}\,\mathrm{OR}_n = \Omega(\sqrt{n})$

  We can construct these duals explicitly [Špa08]
- Goal: Combine $\psi_{\textsf{\textbf{OUT}}}$ and $\psi_{\textsf{\textbf{IN}}}$ to obtain a dual polynomial $\psi_{\textsf{\textbf{AND-OR}}}$ for $\mathrm{AND\text{-}OR}$
- Refines analysis of construction due to [Lee09] and [She09]

A First Attempt



$$\psi_{\textbf{AND-OR}}(x_1, \ldots, x_n) := \psi_{\textbf{OUT}}(\ldots, \psi_{\textbf{IN}}(x_i), \ldots)$$

A Dual Polynomial for $\mathrm{AND\text{-}OR}$

Combined dual polynomial [She09]

$$\psi_{\textsf{AND-OR}}(x_1, \ldots, x_n) := \cancel{\psi_{\textsf{OUT}}(\ldots, \psi_{\textsf{IN}}(x_i), \ldots)}$$

$$2^n \psi_{\textsf{OUT}}(\ldots, \operatorname{sgn} \psi_{\textsf{IN}}(x_i), \ldots) \prod_{i=1}^{n} |\psi_{\textsf{IN}}(x_i)|$$

Verify:

1. $\psi_{\textsf{AND-OR}}$ has high correlation with $\mathrm{AND\text{-}OR}$ Our contribution
2. $\psi_{\textsf{AND-OR}}$ has L_1-norm 1 ✓ [She09]
3. $\psi_{\textsf{AND-OR}}$ has pure high degree n ✓ [She09]

(Sub)Goal: Show $\psi_{\textbf{AND-OR}}$ has high correlation with AND-OR

Key Ideas for Correlation Analysis

1. If $\mathrm{AND}(y) =$ FALSE, one input bit witnesses this fact
   i.e. AND has "certificate complexity 1" on FALSE inputs

2. Dual polynomial $\psi_{\textsf{IN}}$ has "one-sided error" [GS10]
   - If $\operatorname{sgn}\psi_{\textsf{IN}}(y) =$ TRUE, then $\mathrm{OR}(y) =$ TRUE
   - Special property of the OR function

Correlation Analysis

$$\psi_{\textsf{AND-OR}}(x_1, \ldots, x_n) = 2^n \psi_{\textsf{OUT}}(\ldots, \operatorname{sgn} \psi_{\textsf{IN}}(x_i), \ldots) \prod_{i=1}^{n} |\psi_{\textsf{IN}}(x_i)|$$

$\psi_{\textsf{AND-OR}}(x)$ on random $x \overset{\text{i.d.}}{=} \psi_{\textsf{OUT}}(z)$ on random z

If $\mathrm{OR}(x_i) = \operatorname{sgn} \psi_{\textsf{IN}}(x_i)$ on every input,

$$\text{Correlation} = \sum_{z \in \{-1,1\}^n} \psi_{\textsf{OUT}}(z) \, \mathrm{AND}(z) > \epsilon$$

But $\operatorname{sgn} \psi_{\textsf{IN}}$ is only correlated with OR, so input to AND is noisy

Key ideas show that noise doesn't propagate

Main Result

1. $\psi_{\textsf{AND-OR}}$ has high correlation with $\mathrm{AND\text{-}OR}$ ✓
2. $\psi_{\textsf{AND-OR}}$ has L_1-norm 1 ✓
3. $\psi_{\textsf{AND-OR}}$ has pure high degree n ✓

Conclude $\widetilde{\deg}\,\mathrm{AND\text{-}OR}_{n^2} = \Omega(n)$

Explicit Dual Polynomials for Symmetric Functions

[Pat92] Symmetrization argument shows

$$\widetilde{\deg} f = \Omega(\sqrt{t(n-t)})$$

if f changes value between layers $t-1$ and t of the Hamming cube

This work: Explicit dual polynomials for this (tight) lower bound

- Elementary proof based only on LP-duality
- Dual polynomials have numerous applications in communication complexity (see survey [She08])
- Informs search for dual polynomials to prove new lower bounds

Dual Polynomials for Symmetric Functions

- [Špa08] gave a dual polynomial for OR considering layers $\{i^2 : 0 \le i \le \sqrt{n}\}$ of the Hamming cube

- A similar idea yields a dual polynomial for MAJ, considering layers $\{4i : 0 \le i \le n/4\}$

Our dual:

1. Interpolates between OR and MAJ

2. Exploits complementary slackness by weighting the extreme points of the optimal ϵ-approximation of [She08]

Future Directions

- Context for our work: Moving beyond symmetrization
- Can we prove more new $\widetilde{\deg}$ lower bounds by constructing dual polynomials?

  What is the approximate degree of AC^0?
- Importance of dual polynomials with one-sided error

  [GS10] Separation of multi-party communication versions of **NP** and **co-NP**

  [BT13] New threshold weight lower bounds for AC^0

Thank you!