Polynomial bounds for decoupling, with applications

Ryan O'Donnell, Yu Zhao
Carnegie Mellon University

Block-multilinearity

A homogeneous polynomial function f with degree k is *Block-multilinear*

Block-multilinearity

A homogeneous polynomial function f with degree k is *Block-multilinear* if we can partition the input variables into k blocks $S_1, \dots, S_k$

Block-multilinearity

A homogeneous polynomial function f with degree k is *Block-multilinear* if we can partition the input variables into k blocks $S_1, \dots, S_k$ such that each monomial in f contains exactly 1 variable in each block.

$$f(x_1, x_2, x_3, x_4) = \frac{1}{2}x_1x_2 + \frac{1}{2}x_2x_3 + \frac{1}{2}x_3x_4 - \frac{1}{2}x_1x_4$$

$$S_1 = \{x_1, x_3\}, S_2 = \{x_2, x_4\}$$

Anti-concentrations of Gaussian polynomial

Max-E3-Lin-2

[Khot Naor 08, Lovett 10, Kane Meka13, Aaronson Ambainis15]

PRG for Liptschitz functions of polynomials

Classical simulation for quantum query algorithm

AA Conjecture

Let $f:\{-1,1\}^n \to [-1,1]$ be a bounded Boolean polynomial with degree at most k. Then

$$\mathrm{MaxInf}[f] \geq \mathrm{poly}(\mathrm{Var}[f]/k).$$

Def: $f(x) = \sum_{S\subseteq[n]} \hat{f}(S) \prod_{i\in S} x_i$ $\quad f(x_1,x_2,x_3,x_4) = \frac{1}{2}x_1x_2 + \frac{1}{2}x_2x_3 + \frac{1}{2}x_3x_4 - \frac{1}{2}x_1x_4$

$$\mathrm{Var}[f] = \sum_{S\neq\emptyset} \hat{f}(S)^2 \qquad \mathrm{Var}[f] = 1$$

$$\mathrm{Inf}_i[f] = \sum_{S\ni i} \hat{f}(S)^2 \qquad \mathrm{Inf}_1[f] = \frac{1}{2}$$

$$\mathrm{MaxInf}[f] = \max_{i\in[n]}\{\mathrm{Inf}_i[f]\} \qquad \mathrm{MaxInf}[f] = \frac{1}{2}$$

AA Conjecture

Let $f:\{-1,1\}^n \to [-1,1]$ be a bounded Boolean polynomial with degree at most k. Then

$$\mathrm{MaxInf}[f] \geq \mathrm{poly}(\mathrm{Var}[f]/k).$$

Suppose AA Conjecture holds:

1. There exists some deterministic simulation of a quantum algorithm;
2. $\mathrm{P} = \mathrm{P}^{\#\mathrm{P}}$ implies $\mathrm{BQP}^A \subset \mathrm{AvgP}^A$ with probability 1 for a random oracle A.

AA Conjecture, weak version

Let $f:\{-1,1\}^n \to [-1,1]$ be a Boolean polynomial with degree at most k. Then

$$\mathrm{MaxInf}[f] \geq \mathrm{Var}[f]^2/\exp(k).$$

AA Conjecture, weak version

Let $f:\{-1,1\}^n \to [-1,1]$ be a Boolean polynomial with degree at most k. Then

$$\mathrm{MaxInf}[f] \geq \mathrm{Var}[f]^2/\exp(k).$$

There exists an easy proof for block-multilinear function!!

$$f(y,z) = \sum_i y_i g_i(z)$$

First block

Rest variables

Then use hypercontractivity and Cauchy-Schwartz

AA Conjecture, weak version

Let $f:\{-1,1\}^n \to [-1,1]$ be a Boolean polynomial with degree at most k. Then

$$\mathrm{MaxInf}[f] \geq \mathrm{Var}[f]^2/\exp(k).$$

There exists an easy proof for block-multilinear function!!

Can we extend this proof to arbitrary Boolean polynomials?

Yes, via decoupling!

Decoupling

f —decoupling→ $\tilde{f}$

general polynomial
degree k
n variables

block-multilinear
degree k
kn variables
(k blocks of n variables)

1. $f(x) = \tilde{f}(\overbrace{x, x, \dots, x}^{k \text{ copies of } x})$
2. $\tilde{f}$ and f has similar properties

Examples of decoupling

$$f(x_1, x_2, x_3) = x_1 x_2 x_3$$

$$\tilde{f}(y_1, y_2, y_3, z_1, z_2, z_3, w_1, w_2, w_3)$$

$$= \frac{1}{6} y_1 z_2 w_3$$

Examples of decoupling

$$f(x_1, x_2, x_3) = x_1 x_2 x_3$$

$$\tilde{f}(y_1, y_2, y_3, z_1, z_2, z_3, w_1, w_2, w_3)$$

$$= \frac{1}{6} y_1 z_2 w_3 + \frac{1}{6} y_1 w_2 z_3$$

Examples of decoupling

$$f(x_1, x_2, x_3) = x_1 x_2 x_3$$

$$\tilde{f}(y_1, y_2, y_3, z_1, z_2, z_3, w_1, w_2, w_3)$$

$$= \tfrac{1}{6} y_1 z_2 w_3 + \tfrac{1}{6} y_1 w_2 z_3 + \tfrac{1}{6} z_1 y_2 w_3 + \tfrac{1}{6} z_1 w_2 y_3 + \tfrac{1}{6} w_1 y_2 z_3 + \tfrac{1}{6} w_1 z_2 y_3$$

$$\mathrm{Var}[\tilde{f}] = \frac{1}{k!}\mathrm{Var}[f] \qquad \mathrm{Inf}_{y_i}[\tilde{f}] = \frac{1}{k! \cdot k}\mathrm{Inf}_{x_i}[f]$$

AA Conjecture, weak version

Let $f:\{-1,1\}^n \to [-1,1]$ be a Boolean function with degree at most k. Then

$$\mathrm{MaxInf}[f] \geq \mathrm{Var}[f]^2/\exp(k).$$

$$f \xrightarrow{\text{decoupling}} \tilde{f}$$

$$\mathrm{Var}[\tilde{f}] = \frac{1}{k!}\mathrm{Var}[f]$$

$$\mathrm{MaxInf}[\tilde{f}] = \frac{1}{k! \cdot k}\mathrm{MaxInf}[f]$$

Decoupling inequality

(k is the degree of f)

Theorem 1. Let $\Phi\colon \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ be convex and non-decreasing.

$$\mathrm{E}\left[\Phi\left(\left|\tilde{f}\left(x^{(1)}, \ldots, x^{(k)}\right)\right|\right)\right] \leq \mathrm{E}[\Phi(C_k|f(x)|)]$$

[de la Peña 92]

Theorem 2. For all $t > 0$,

$$\Pr\left[\left|\tilde{f}\left(x^{(1)}, \ldots, x^{(k)}\right)\right| > C_k t\right] \leq D_k \Pr[|f(x)| > t]$$

[Peña Montgomery-Smith 95, Giné 98]

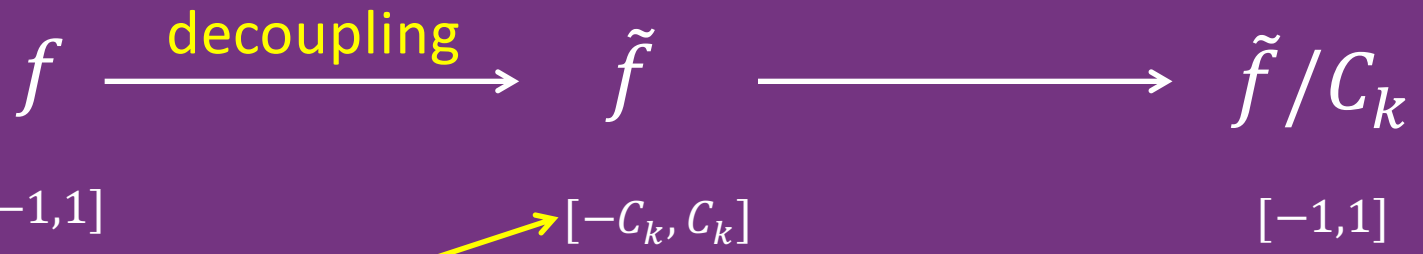
Comments:

1. $C_k, D_k = \exp(k \log k)$
2. The inputs can be any independent random variables with all moments finite.
3. The reverse inequality also holds with some worse constants.
4. f does not need to be multilinear neccesarily

AA Conjecture, weak version

Let $f:\{-1,1\}^n \to [-1,1]$ be a Boolean function with degree at most k. Then

$$\mathrm{MaxInf}[f] \geq \mathrm{Var}[f]^2/\exp(k).$$



$C_k = \exp(k \log k)$ from decoupling inequality

$$\mathrm{Var}[\tilde{f}] = \frac{1}{k!}\mathrm{Var}[f]$$

$$\mathrm{MaxInf}[\tilde{f}] = \frac{1}{k! \cdot k}\mathrm{MaxInf}[f]$$

$$\mathrm{Var}[\tilde{f}/C_k] = \frac{1}{C_k^2}\mathrm{Var}[\tilde{f}]$$

$$\mathrm{MaxInf}[\tilde{f}/C_k] = \frac{1}{C_k^2}\mathrm{MaxInf}[\tilde{f}]$$

Summary of classical decoupling

Advantage:

Transfer a general function f to a block-multilinear function.

Disadvantage:

Introduce an exponential factor on k in decoupling inequality. ☹

Summary of classical decoupling

Sometimes we don't need the function to be all-blocks-multilinear.

We only need f to be a linear map on y.

$$f(y,z) = \sum_i y_i g_i(z)$$

First block

Rest variables

Then use hypercontractivity and Cauchy-Schwartz

One-block-multilinear

A polynomial function f with degree k is *one-block-multilinear* if there exists a subset of the input variables S such that each monomial (except the constant term) in f contains exactly 1 variable in S.

$$f(y,z) = \sum_i y_i g_i(z)$$

Partial decoupling, with polynomial bounds

Our result:

f —Partial decoupling→ $\breve{f}$

general function
degree k
n variables

One-block-multilinear function
degree k
$2n$ variables
(2 blocks of n variables)

Examples of partial decoupling

$f(x_1, x_2, x_3) = x_1 x_2 x_3$

$\check{f}(y_1, y_2, y_3, z_1, z_2, z_3)$

$= \frac{1}{3} y_1 z_2 z_3 + \frac{1}{3} z_1 y_2 z_3 + \frac{1}{3} z_1 z_2 y_3$

$$\mathrm{Var}[\check{f}] = \frac{1}{k}\mathrm{Var}[f] \qquad \mathrm{Inf}_{y_i}[\check{f}] = \frac{1}{k^2}\mathrm{Inf}_{x_i}[f]$$

$$\mathrm{Inf}_{z_i}[\check{f}] = \frac{k-1}{k^2}\mathrm{Inf}_{x_i}[f]$$

Partial decoupling, with polynomial bounds

Our result:

Theorem 1. Let $\Phi\colon \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ be convex and non-decreasing.

$$\mathrm{E}\left[\Phi\left(\left|\check{f}(y,z)\right|\right)\right] \leq \mathrm{E}[\Phi(C_k|f(x)|)]$$

Theorem 2. For all $t > 0$,

$$\Pr\left[\left|\check{f}(y,z)\right| > C_k t\right] \leq D_k \Pr[|f(x)| > t]$$

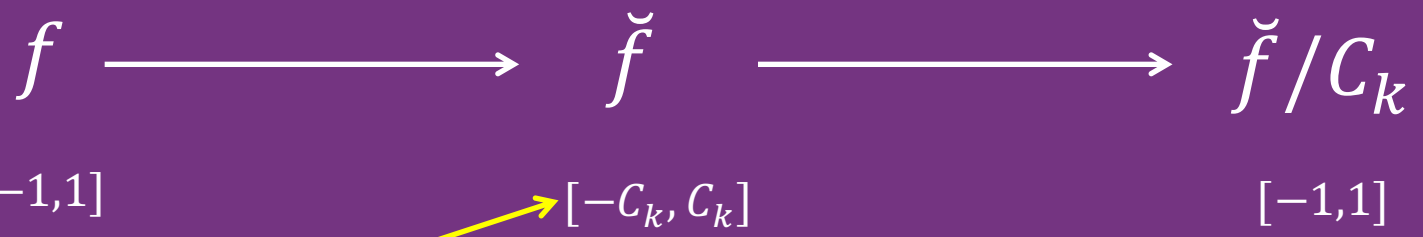
With constants: $\mathrm{poly}(k)$

$$D_k = \exp(k \log k) \qquad C_k = \begin{cases} O(k^2) & \text{Boolean} \\ O(k^{3/2}) & \text{Boolean, homogeneous} \\ O(k) & \text{standard Gaussian} \end{cases}$$

AA Conjecture, weak version

Let $f:\{-1,1\}^n \to [-1,1]$ be a Boolean function with degree at most k. Then

$$\mathrm{MaxInf}[f] \geq \mathrm{Var}[f]^2/\exp(k).$$



$C_k = \mathrm{poly}(k)$
from new decoupling inequality

$$\mathrm{Var}[\check{f}] = \frac{1}{k}\mathrm{Var}[f]$$

$$\mathrm{MaxInf}[\check{f}] \geq \frac{1}{k^2}\mathrm{MaxInf}[f]$$

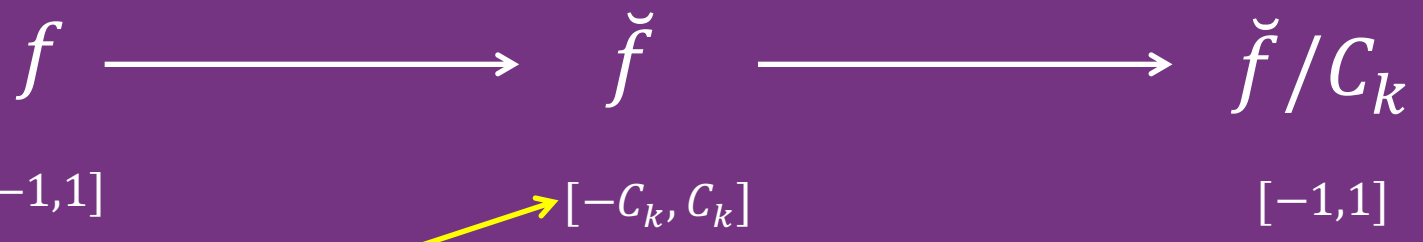
$$\mathrm{Var}[\check{f}/C_k] = \frac{1}{C_k^2}\mathrm{Var}[\check{f}]$$

$$\mathrm{MaxInf}[\check{f}/C_k] = \frac{1}{C_k^2}\mathrm{MaxInf}[\check{f}]$$

AA Conjecture

Let $f:\{-1,1\}^n \to [-1,1]$ be a Boolean function with degree at most k. Then

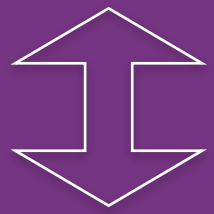
$$\mathrm{MaxInf}[f] \geq \mathrm{Var}[f]^2/\mathrm{poly}(k).$$



AA Conjecture

Let $f:\{-1,1\}^n \to [-1,1]$ be a Boolean function with degree at most k. Then

$$\mathrm{MaxInf}[f] \geq \mathrm{Var}[f]^2/\mathrm{poly}(k).$$



The conjecture holds for one-block-multilinear functions.

$$f(y,z) = \sum_i y_i g_i(z)$$

Comparisons

Full decoupling	Partial decoupling
Block-multilinear	One-block-multilinear
$C_k = \exp(k \log k)$	$C_k = \mathrm{poly}(k)$
General inputs with all finite moments	Boolean or Gaussian

Decoupling with polynomial bounds

Main result:

Prove the decoupling inequalities for one-block decoupling with polynomial bounds.

Applications:

1. Give an easy proof for the weak version of AA Conjecture. Show that AA Conjecture holds iff it holds for all one-block-multilinear functions;
2. Generalize a randomized algorithm to arbitrary Boolean functions with the same query complexity;
3. Prove the tight bounds for DFKO Theorems.

Application 2

Theorem in [AA15] Let $f:\{-1,1\}^n \to [-1,1]$ be any bounded block-multilinear Boolean function with degree k.

Then there exists a randomized algorithm that,

on input $x \in \{-1,1\}^n$, non-adaptively queries $2^{O(k)}(n/\varepsilon^2)^{1-1/k}$ bits of x, and then estimate the output of f within error ε with high probability.

$$f \xrightarrow{f(x)=\tilde{f}(x,\ldots,x)} \tilde{f} \xrightarrow[C_k = 2^{O(k)}]{\varepsilon' = \varepsilon / C_k} \tilde{f} / C_k$$

$$[-1,1] \qquad [-C_k, C_k] \qquad [-1,1]$$

Application 2

Theorem in [AA15] Let $f:\{-1,1\}^n \to [-1,1]$ be any bounded ~~block-multilinear~~ Boolean function with degree k.

Then there exists a randomized algorithm that,

on input $x \in \{-1,1\}^n$, non-adaptively queries $2^{O(k)}(n/\varepsilon^2)^{1-1/k}$ bits of x, and then estimate the output of f within error ε with high probability.

$$f \xrightarrow{f(x)=\tilde{f}(x,\ldots,x)} \tilde{f} \xrightarrow[C_k = 2^{O(k)}]{\varepsilon' = \varepsilon / C_k} \tilde{f} / C_k$$

$$[-1,1] \qquad [-C_k, C_k] \qquad [-1,1]$$

Application 3: Tight bounds for DFKO Theorems

DFKO Inequality: [Dinur Friedgut Kindler O'Donnell 07]

$f : R^n \to R$ a polynomial with degree k
Standard Gaussian/Boolean inputs (for Boolean, MaxInf[f] is small)
$\mathrm{Var}[f] \geq 1$

$$\Pr[|f| > t] \geq \exp(-O(t^2 k^2 \log k))$$

$\Pr[|f| > t] \leq \exp(-O(t^2))$

A gap of log k

There exists some function f such that

$$\Pr[|f| > t] \leq \exp(-O(t^2 k^2))$$

Future direction

Our result:

Theorem 1. Let $\Phi\colon \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ be convex and non-decreasing.

$$\mathrm{E}\left[\Phi\left(\left|\check{f}(y,z)\right|\right)\right] \leq \mathrm{E}[\Phi(C_k|f(x)|)]$$

Theorem 2. For all $t > 0$,

$$\Pr\left[\left|\check{f}(y,z)\right| > C_k t\right] \leq D_k \Pr[|f(x)| > t]$$

With constants:

$\mathrm{poly}(k)$

$$D_k = \exp(k \log k) \qquad C_k = \begin{cases} O(k^2) & \text{Boolean} \\ O(k^{3/2}) & \text{Boolean, homogeneous} \\ O(k) & \text{standard Gaussian} \end{cases}$$

Future direction

1. One-block decoupling inequalities are tight with Gaussian inputs. What about Boolean case?
2. Can we generalize them to arbitrary inputs with all moments finite?
3. Do the reverse inequalities hold?
4. Prove (or disprove) AA Conjecture for one-block-multilinear functions.

Thank you!