Polynomial bounds for decoupling, with applications

Ryan O'Donnell, Yu Zhao
Carnegie Mellon University

Boolean functions

$$f : \{-1, 1\}^n \to \mathbb{R}$$

$$\mathrm{Maj}_3(x_1, x_2, x_3) = \begin{cases} 1 & \text{if at least two inputs are 1} \\ -1 & \text{if at least two inputs are -1} \end{cases}$$

x_1	x_2	x_3	**Output**
1	1	1	1
1	1	-1	1
1	-1	1	1
1	-1	-1	-1
-1	1	1	1
-1	1	-1	-1
-1	-1	1	-1
-1	-1	-1	-1

$$\mathrm{Maj}_3(x_1, x_2, x_3) = \frac{1}{2}x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3 - \frac{1}{2}x_1x_2x_3$$

Boolean functions

$x_i^2 = 1$

Fourier expansion: the unique multilinear polynomial representation of a Boolean function

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

$$\mathrm{Maj}_3(x_1, x_2, x_3) = \frac{1}{2}x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3 - \frac{1}{2}x_1 x_2 x_3$$

Properties of Boolean functions

Low circuit complexity

Monotonicity

Linear threshold

Bounded

Block-multilinearity

Low degree

Small influence

Small variance

Homogeneity

Block-multilinearity

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

Block-multilinearity

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

Block-multilinearity

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

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

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

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

Block-multilinearity

Theorem in [AA15] Let $f:\{-1,1\}^n \rightarrow [-1,1]$ 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 $2^{O(k)}(n/\varepsilon^2)^{1\text{-}1/k}$ bits of x, and then estimate the output of f within error ε with high probability.

$n^{1-1/k}$

Conjecture: This theorem works for arbitrary polynomials

Yes, via decoupling!

Block-multilinearity

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.

Quantum algorithm makes t queries to $x \in \{-1,1\}^n$

The probability that the algorithm accepts can be expressed as a Boolean function with degree at most $2t$.

The algorithm can be simulated by a classical algorithm with $O(n^{1-1/(2t)})$ queries.

Block-multilinearity

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.

Can we extend this algorithm to arbitrary Boolean functions?

Yes, via decoupling!

Decoupling

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

general function
degree k
n variables

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

1. $f(x) = \tilde{f}(\underbrace{x,\ldots,x}_{k \text{ copies of } x})$
2. $\tilde{f}$ and f has similar properties

Examples of decoupling

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

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

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

Examples of decoupling

$$\mathrm{Maj}_3(x_1,x_2,x_3)=\tfrac{1}{2}x_1+\tfrac{1}{2}x_2+\tfrac{1}{2}x_3-\tfrac{1}{2}x_1x_2x_3$$

$$\widetilde{\mathrm{Maj}_3}(y_1,y_2,y_3,z_1,z_2,z_3,w_1,w_2,w_3)$$

$$=\tfrac{1}{6}y_1+\tfrac{1}{6}z_1+\tfrac{1}{6}w_1$$

$$+\tfrac{1}{6}y_2+\tfrac{1}{6}z_2+\tfrac{1}{6}w_2$$

$$+\tfrac{1}{6}y_3+\tfrac{1}{6}z_3+\tfrac{1}{6}w_3$$

$$-\tfrac{1}{12}y_1z_2w_3-\tfrac{1}{12}y_1w_2z_3-\tfrac{1}{12}z_1y_2w_3-\tfrac{1}{12}z_1w_2y_3-\tfrac{1}{12}w_1y_2z_3-\tfrac{1}{12}w_1z_2y_3$$

Block-multilinearity

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

[KN08, Lov10, KM13, AA15]

Block-multilinearity

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

[KN08, Lov10, KM13, AA15]

Block-multilinearity

A ~~homogeneous~~ Boolean function f with degree k is *Block-multilinear* if we can partition the input variables into k blocks S_1, …, S_k such that each monomial in the Fourier expansion of f contains at most 1 variable in each block.

[KN08, Lov10, KM13, AA15]

Block-multilinearity

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.

$$f(x) = \tilde{f}(x, \ldots, x)$$

Block-multilinearity

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.

$$f(x) = \tilde{f}(x,\ldots,x)$$

$$f:\{-1,1\}^n \to [-1,1] \longrightarrow \tilde{f}:\{-1,1\}^{kn} \to [-C,C]?$$

Decoupling inequality

(k is the degree of f)

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

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

[de la Peña 92]

Theorem 2. For all t > 0,

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

[Peña Montgomery-Smith 95, Giné 98]

Comments:

1. $C_k, D_k = k^{O(k)}$
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

Decoupling inequality

(k is the degree of f)

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

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

[de la Peña 92]

Theorem 2. For all t > 0,

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

[Peña Montgomery-Smith 95, Giné 98]

Comments:

5. If f is a homogeneous function with Boolean input, C_k can be improved to $2^{O(k)}$. [Kwapień 87]

6. $\Phi = |\cdot|^p$ $\longrightarrow$ $\|\tilde{f}\|_p \leq C_k \|f\|_p$

· $p \to \infty$ $\quad$ $\|\tilde{f}\|_\infty \leq C_k \|f\|_\infty$

Block-multilinearity

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.

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

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

Block-multilinearity

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.

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

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

Application 2: AA Conjecture

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

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

Def:

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

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

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

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

$$\mathrm{Maj}_3(x_1,x_2,x_3) = \tfrac{1}{2}x_1 + \tfrac{1}{2}x_2 + \tfrac{1}{2}x_3 - \tfrac{1}{2}x_1x_2x_3$$

$$\mathrm{Var}[\mathrm{Maj}_3] = 1$$

$$\mathrm{Inf}_i[\mathrm{Maj}_3] = \tfrac{1}{2}$$

$$\mathrm{MaxInf}[\mathrm{Maj}_3] = \tfrac{1}{2}$$

Application 2: AA Conjecture

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

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

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.

Application 2: AA Conjecture, weak version

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

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

Application 2: AA Conjecture, weak version

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

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

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

Examples of decoupling

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

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

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

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

Application 2: AA Conjecture, weak version

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

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

$$f \longrightarrow \tilde{f} \longrightarrow \tilde{f}/C_k$$

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

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

$$\mathrm{Inf}_i[\tilde{f}] = \frac{1}{k!\cdot k}\mathrm{Inf}_i[f] \qquad \mathrm{Inf}_i[\tilde{f}/C_k] = \frac{1}{C_k^2}\mathrm{Inf}_i[\tilde{f}]$$

Application 2: AA Conjecture, weak version

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

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

$$f \longrightarrow \tilde{f} \longrightarrow \tilde{f}/C_k$$

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

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

$$\mathrm{Inf}_i[\tilde{f}] = \frac{1}{k!\cdot k}\mathrm{Inf}_i[f] \qquad \mathrm{Inf}_i[\tilde{f}/C_k] = \frac{1}{C_k^2}\mathrm{Inf}_i[\tilde{f}]$$

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 Boolean 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 the Fourier expansion of f contains exactly 1 variable in S.

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

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

$$\mathrm{Maj}_3(x_1,x_2,x_3)=\frac{1}{2}x_1+\frac{1}{2}x_2+\frac{1}{2}x_3-\frac{1}{2}x_1x_2x_3$$

Partial decoupling, with polynomial bounds

Our result:

$$f \xrightarrow{\text{Partial decoupling}} \overset{\frown}{f}$$

general function
degree k
n variables

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

Examples of partial decoupling

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

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

$$= y_1 z_2 z_3 + z_1 y_2 z_3 + z_1 z_2 y_3$$

Examples of partial decoupling

$\mathrm{Maj}_3(x_1, x_2, x_3) = \frac{1}{2}x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3 - \frac{1}{2}x_1 x_2 x_3$

$\widetilde{\mathrm{Maj}_3}(y_1, y_2, y_3, z_1, z_2, z_3)$

$= \frac{1}{2}y_1 + \frac{1}{2}y_2 + \frac{1}{2}y_3$

Examples of partial decoupling

$$\mathrm{Maj}_3(x_1,x_2,x_3)=\tfrac{1}{2}x_1+\tfrac{1}{2}x_2+\tfrac{1}{2}x_3-\tfrac{1}{2}x_1x_2x_3$$

$$\widehat{\mathrm{Maj}_3}(y_1,y_2,y_3,z_1,z_2,z_3)$$
$$=\tfrac{1}{2}y_1+\tfrac{1}{2}y_2+\tfrac{1}{2}y_3-\tfrac{1}{2}y_1z_2z_3-\tfrac{1}{2}z_1y_2z_3-\tfrac{1}{2}z_1z_2y_3$$

$kf(x)=\widehat{f}(x,x)$ for homogeneous case only

$$\mathrm{Var}[f]\le\mathrm{Var}[\widehat{f}]\le k\mathrm{Var}[f]$$

$$\mathrm{Inf}_{y_i}[\widehat{f}]=\mathrm{Inf}_{x_i}[f] \qquad \mathrm{Inf}_{z_i}[\widehat{f}]\le(k-1)\mathrm{Inf}_{x_i}[f]$$

Partial decoupling, with polynomial bounds

Our result:

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

$$E[\Phi(|\overset{\frown}{f}(y,z)|)] \leq E[\Phi(C_k\,|f(x)|)]$$

Theorem 2. For all t > 0,

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

With constants:

poly(k)

.

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

Application 2: AA Conjecture, weak version

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

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

$$f \longrightarrow \overset{\frown}{f} \longrightarrow \overset{\frown}{f}/C_k$$

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

$$\mathrm{Var}[\overset{\frown}{f}] \geq \mathrm{Var}[f] \qquad \mathrm{Var}[\overset{\frown}{f}/C_k] = \frac{1}{C_k^2}\mathrm{Var}[\overset{\frown}{f}]$$

$$\mathrm{MaxInf}[\overset{\frown}{f}] \leq k\,\mathrm{MaxInf}[f] \qquad \mathrm{Inf}_i[\overset{\frown}{f}/C_k] = \frac{1}{C_k^2}\mathrm{Inf}_i[\overset{\frown}{f}]$$

Application 2: AA Conjecture

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

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

$$f \longrightarrow \overset{\frown}{f} \longrightarrow \overset{\frown}{f}/C_k$$

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

$$\text{Var}[\overset{\frown}{f}] \geq \text{Var}[f] \qquad \text{Var}[\overset{\frown}{f}/C_k] = \frac{1}{C_k^2}\text{Var}[\overset{\frown}{f}]$$

$$\text{MaxInf}[\overset{\frown}{f}] \leq k\text{MaxInf}[f] \qquad \text{Inf}_i[\overset{\frown}{f}/C_k] = \frac{1}{C_k^2}\text{Inf}_i[\overset{\frown}{f}]$$

Application 2: AA Conjecture

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

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

$$\Updownarrow$$

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
$C_k = \exp(k)$	$C_k = \mathrm{poly}(k)$
$\mathrm{Var}[\widetilde{f}] \approx \exp(-O(k))\mathrm{Var}[f]$	$\mathrm{Var}[f] \le \mathrm{Var}[\overset{\frown}{f}] \le k\mathrm{Var}[f]$
$f(x) = \widetilde{f}(x,\ldots,x)$	$kf(x) = \overset{\frown}{f}(x,x)$ for homogeneous case only
General inputs with all finite moments	Boolean or Gaussian

The rest of my talk

1. Application 3: Tight bounds for DFKO Theorems
2. Proof sketch for our decoupling inequalities

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, $\mathrm{MaxInf}[f]$ is small)

$\mathrm{Var}[f] \geq 1$

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

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

A gap of log k

There exists some function f such that

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

Application 3:
Tight bounds for DFKO Theorems

$$\Pr[|\hat{f}(y,z)|>t]\geq \exp(-O(k+t^2))$$

(by hypercontractivity)

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

Gaussian case: $C_k=O(k), D_k=k^{O(k)}=\exp(O(k\log k))$

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

Proof sketch for Gaussian case

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

$$E[\Phi(|\overset{\frown}{f}(y,z)|)] \leq E[\Phi(C_k\,|f(x)|)]$$

$$\overset{\frown}{f}(y,z) = \sum_i c_i f(a_i y + b_i z)$$

$$a_i^2 + b_i^2 = 1 \qquad a_i y + b_i z \sim N(0,1)^n$$

$$\sum_i |c_i| = C_k = O(k)$$

Proof sketch for Gaussian case

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

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

$$\mathrm{E}[\Phi(|\frown{f}(y,z)|)] = \mathrm{E}\left[\Phi\left(\left|\sum_i c_i f(a_i y + b_i z)\right|\right)\right]$$

$$\leq \sum_i \frac{|c_i|}{C_k} \mathrm{E}\left[\Phi\left(\left|C_k f(a_i y + b_i z)\right|\right)\right]$$

$$= \sum_i \frac{|c_i|}{C_k} \mathrm{E}\left[\Phi\left(C_k \left|f(x)\right|\right)\right]$$

$$= \mathrm{E}\left[\Phi\left(C_k \left|f(x)\right|\right)\right]$$

Proof sketch for Gaussian case

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

$$E[\Phi(|\overset{\frown}{f}(y,z)|)]\leq E[\Phi(C_k\,|f(x)|)]$$

$$\overset{\frown}{f}(y,z)=\sum_i c_i f(a_i y+b_i z)$$

$$a_i^2+b_i^2=1$$

$$\sum_i |c_i|=C_k=O(k)$$

$$f(x)=x_1x_2 \qquad \overset{\frown}{f}(y,z)=y_1z_2+y_2z_1$$

$$f(a_i y+b_i z)=(a_i y_1+b_i z_1)(a_i y_2+b_i z_2)$$

$$y_1z_2+y_2z_1=$$

$$\sum_i c_i a_i^2 y_1 y_2+\sum_i c_i a_i b_i(y_1z_2+y_2z_1)+\sum_i c_i b_i^2 z_1 z_2$$

$$\sum_i c_i a_i^2=0 \qquad \sum_i c_i a_i b_i=1 \qquad \sum_i c_i b_i^2=0$$

Best choice we got: $\dfrac{a_i}{b_i}=\dfrac{k}{i}$

Summary

Main result:

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

Applications:

1. Generalize a randomized algorithm to arbitrary Boolean functions with the same query complexity;
2. 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;
3. Prove the tight bounds for DFKO Theorems.

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!