Discussion: Error-Correcting Codes and the Core Property

Nathan

2023

A recap of the story

A recap of the story

Theorem

*For any d and σ, there are constants C, κ such that for any **natural** rank function rk and any d-tensor T,*

$$\Pr_{I_1\sim[n_1]_\sigma,\ldots,I_d\sim[n_d]_\sigma}\left[\mathrm{rk}(T_{|I_{[d]}} \geq \kappa\,\mathrm{rk}(T)\right] \geq 1 - Ce^{-\kappa\,\mathrm{rk}(T)}$$

A recap of the story

Theorem

*For any d, σ, and ϵ, there's a constant κ such that for any **natural** rank function* rk *and any degree-d polynomial ϕ,*

$$\Pr_{I \sim [n]_\sigma} [\mathrm{rk}(\phi_{|I} \geq \kappa\, \mathrm{rk}(T)] \geq 1 - \epsilon$$

ERROR-CORRECTION CODE APPLICATION

NOISY DECODING BY SHALLOW CIRCUITS WITH PARITIES: CLASSICAL AND QUANTUM

JOP BRIËT, HARRY BUHRMAN, DAVI CASTRO-SILVA, AND NIELS M. P. NEUMANN

ABSTRACT. We consider the problem of decoding corrupted error correcting codes with $NC^0[\oplus]$ circuits in the classical and quantum settings. We show that any such classical circuit can correctly recover only a vanishingly small fraction of messages, if the codewords are sent over a noisy channel with positive error rate. Previously this was known only for linear codes with non-trivial dual distance, whereas our result applies to any code. By contrast, we give a simple quantum circuit that correctly decodes the Hadamard code with probability $\Omega(\varepsilon^2)$ even if a $(1/2-\varepsilon)$-fraction of a codeword is adversarially corrupted.

Our classical hardness result is based on an equidistribution phenomenon for multivariate polynomials over a finite field under biased input-distributions. This is proved using a structure-versus-randomness strategy based on a new notion of rank for high-dimensional polynomial maps that may be of independent interest.

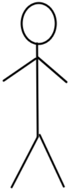
Our quantum circuit is inspired by a non-local version of the Bernstein-Vazirani problem, a technique to generate "poor man's cat states" by Watts et al., and a constant-depth quantum circuit for the OR function by Takahashi and Tani.

What are Error-Correcting Codes?

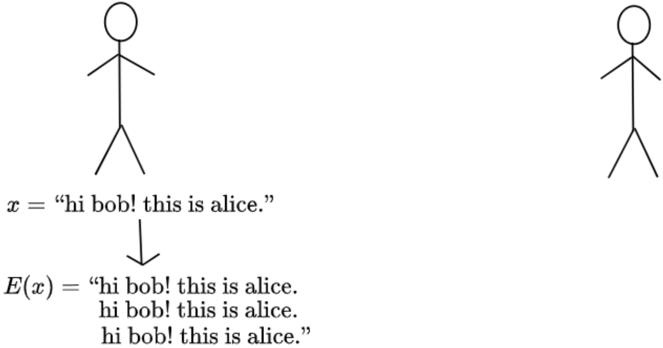
$x =$ "hi bob! this is alice."

What are Error-Correcting Codes?

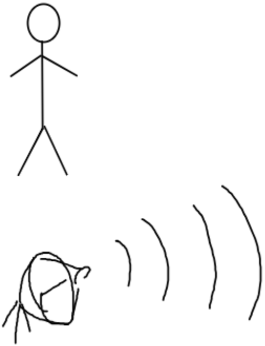
$x + \mathcal{N} =$ "oi bwb! thipuis al36e."



What are Error-Correcting Codes?



WHAT ARE ERROR-CORRECTING CODES?



$E(x) + \mathcal{N} =$ “hwtbou! tris ps alici.
ii 4obp ph?s is xlike.
hi brb! thin iv aaiceq

What are Error-Correcting Codes?

$E(x) + \mathcal{N} =$ "hwtbou! tris ps alici.
ii 4obp ph?s is xlike.
hi brb! thin iv aaiceq

$D(E(x + \mathcal{N})) =$ "hi bob! this is alice."

What are Error-Correcting Codes?

Error model:

$$\mathcal{N}_\rho = \begin{cases} 0 \text{ with probability } \rho \\ \text{random field element with probability } 1-\rho \end{cases}$$

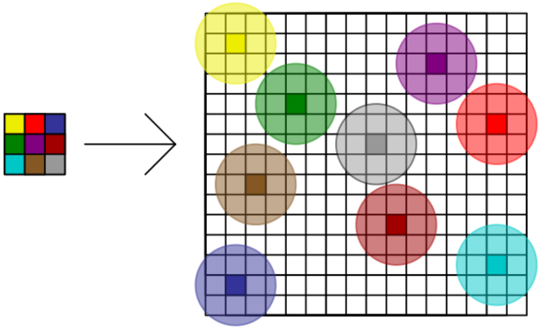
What are Error-Correcting Codes?

Error model:

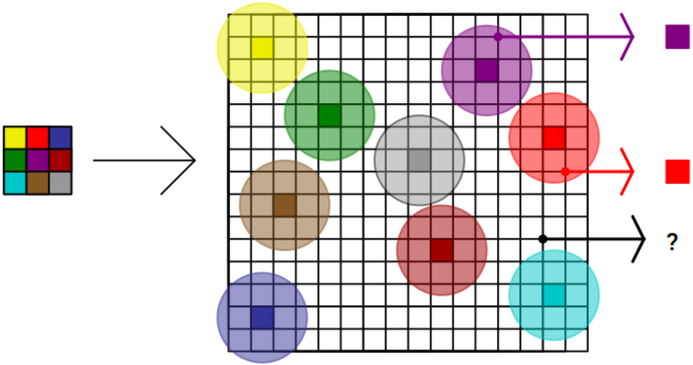
$$\mathcal{N}_\rho = \begin{cases} 0 \text{ with probability } \rho \\ \text{random field element with probability } 1-\rho \end{cases}$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9
$\mathcal{N}_{2/3} =$	0	r	0	0	0	r	0	0	r
	x_1	r	x_3	x_4	x_5	r	x_7	x_8	r

What are Error-Correcting Codes?



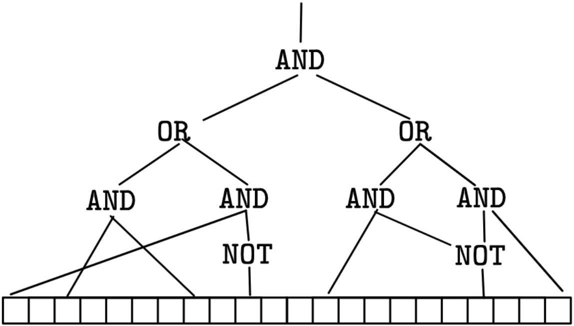
What are Error-Correcting Codes?



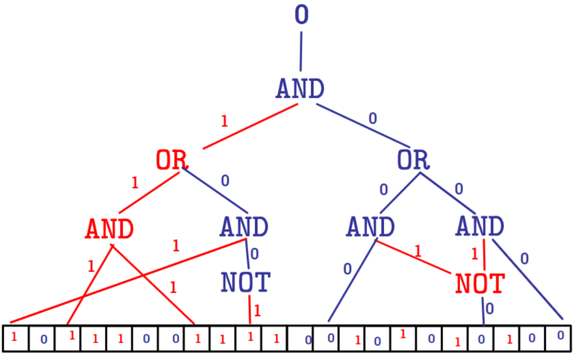
Example: Walsh-Hadamard Code

$$\text{WH} : \{0,1\}^n \to \{0,1\}^{2^n}$$
$$\text{WH}(x)_i = \langle x, i \rangle$$

WHAT IS $\mathsf{NC}^0[\oplus]$?



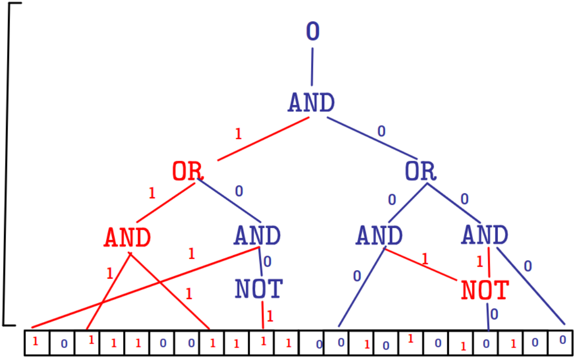
WHAT IS $\mathsf{NC}^0[\oplus]$?



WHAT IS $\mathsf{NC}^0[\oplus]$?

NC^0 :

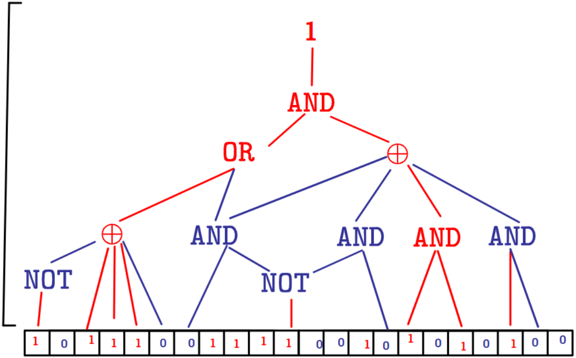
- constant depth
- fan-in 2



WHAT IS $\mathsf{NC}^0[\oplus]$?

$NC^0[\oplus]$:

- constant depth
- fan-in 2
- except for arbitrary fan-in parity gates

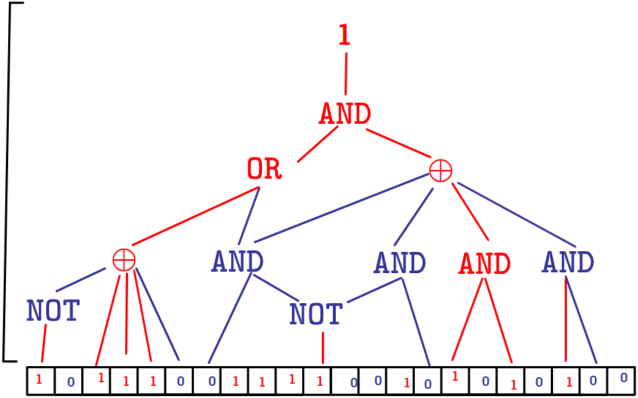


WHAT IS $NC^0[\oplus]$?

$NC^0[\oplus]$:

- constant depth
- fan-in 2
- except for arbitrary fan-in parity gates

compute constant-degree polynomials



[BBCSN22] Main Theorem

Theorem

For any $p, d \in \mathbb{N}$, $\rho, \epsilon \in (0,1)$ *there exists* $k_0(p, d, \rho, \epsilon)$ *such that, for any integers* $k \geq k_0$, n, *any function (i.e. error-correcting code)* $E : \mathbb{F}_p^k \to \mathbb{F}_p^n$, *and any degree-*$d$ *polynomial (i.e.* $\mathsf{NC}^0[\oplus]$ *circuit)* ϕ,

$$\Pr_{x \in \mathbb{F}_p^k,\ Z \sim \mathcal{N}_\rho} [\phi(E(x) + Z) = x] \leq \epsilon.$$

Intuition

Goal: $\Pr_{x \in \mathbb{F}_p^k,\, Z \sim \mathcal{N}_\rho}[\phi(E(x) + Z) = x] \leq \epsilon.$

Intuition

Goal: $\Pr_{x \in \mathbb{F}_p^k,\, Z \sim \mathcal{N}_\rho}[\phi(E(x) + Z) = x] \leq \epsilon.$

Idea: either ϕ has small rank (in which case the output space will be too small to hit most x), or ϕ has large rank (in which case it's too sensitive to the errors).

Intuition: Linear Case

$$\text{Goal: } \Pr_{x \in \mathbb{F}_p^k,\ Z \sim \mathcal{N}_\rho}[U(E(x) + Z) + v = x] \leq \epsilon.$$

- Suppose ϕ is degree-1; i.e., can be written as $y \mapsto Uy + v$.

INTUITION: LINEAR CASE

$$\text{Goal: } \Pr_{x \in \mathbb{F}_p^k,\ Z \sim \mathcal{N}_\rho}[U(E(x) + Z) + v = x] \leq \epsilon.$$

- Suppose ϕ is degree-1; i.e., can be written as $y \mapsto Uy + v$.
- If $\mathrm{rk}(U) \leq k/2$, $\mathrm{im}(U + v)$ is affine space of size at most $p^{k/2}$, so decoding probability $\leq p^{k/2}/p^k = p^{-k/2}$.

Intuition: Linear Case

$$\text{Goal: } \Pr_{x \in \mathbb{F}_p^k,\ Z \sim \mathcal{N}_\rho}[U(E(x) + Z) + v = x] \leq \epsilon.$$

- Suppose $\mathrm{rk}(U) > k/2$. Note it suffices to bound $\Pr_{Z \sim \mathcal{N}_\rho}[UZ = x - v - UE(x)]$ for every fixed x.

INTUITION: LINEAR CASE

$$\text{Goal: } \Pr_{Z \sim \mathcal{N}_\rho}[UZ = x - v - UE(x)] \leq 2^{-\Omega(k)}$$

- Suppose $\mathrm{rk}(U) > k/2$.
- To choose Z, first choose corrupted indices, then set values. Equivalently, first take random restriction of U, then feed random input.

Intuition: Linear Case

$$\text{Goal: } \Pr_{Z \sim \mathcal{N}_\rho}[UZ = x - v - UE(x)] \leq 2^{-\Omega(k)}$$

- Suppose $\mathrm{rk}(U) > k/2$.
- To choose Z, first choose corrupted indices, then set values. Equivalently, first take random restriction of U, then feed random input.
- w.h.p. random restriction has rank at least $(1-\rho)k/4$, so probability of being in the kernel is less than $p^{-(1-\rho)k/4}$.

Analytic Rank for degree-d polynomials

Definition

$$\operatorname{arank}_d(\phi) = -\log_p \left(\max_{\psi:\mathbb{F}_p^n \to \mathbb{F}_p^k,\ \deg(\psi) \leq d-1} \Pr[\phi(x) = \psi(x)] \right)$$

(why same if linear?)

ANALYTIC RANK FOR DEGREE-d POLYNOMIALS

Definition

$$\operatorname{arank}_d(\phi) = -\log_p \left(\max_{\psi:\mathbb{F}_p^n \to \mathbb{F}_p^k,\ \deg(\psi) \le d-1} \Pr[\phi(x) = \psi(x)] \right)$$

Equivalently,

$$\operatorname{arank}_d(\phi) = \min_{\psi:\mathbb{F}_p^n \to \mathbb{F}_p^k,\ \deg(\psi) \le d-1} -\log_p \mathbb{E}_{v \in \mathbb{F}_p^k,\ x \in \mathbb{F}_p^n} \omega^{\langle v, \phi(x) - \psi(x) \rangle}.$$

Main Theorem Proof Outline

- If high analytic rank:
  - suffices to show equidistribution of $\phi(Z)$
  - can be thought of in terms of rank of the restriction; arank is natural so we apply the theorem from the other paper
- If low analytic rank:
  - Equivalent to saying a related polynomial has high bias
  - Functions with high bias have some coherent structure in terms of their derivatives
  - Exploiting that structure and doing some Fourier analysis, can write the claim in terms of a lower-degree instance
  - $\implies$ win by induction

Some Terminology

Definition

Letting $\omega = e^{2i\pi/p}$, for a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$, we define

$$\mathrm{bias}(f) = |\mathbb{E}_{x \in \mathbb{F}_p^n} \omega^{f(x)}|$$

Some Terminology

Definition

Letting $\omega = e^{2i\pi/p}$, for a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$, we define

$$\text{bias}(f) = |\mathbb{E}_{x \in \mathbb{F}_p^n} \omega^{f(x)}|$$

Definition

For a polynomial $P \in \mathbb{F}_p[x_1, \ldots, x_n]$ and a vector $h \in \mathbb{F}_p^n$, we define the "derivative"

$$\Delta_h P(x) = P(x+h) - P(x)$$

Derivative Fact 1

$$\mathrm{bias}(f) = |\mathbb{E}_{x \in \mathbb{F}_p^n} \omega^{f(x)}|$$

$$\Delta_h P(x) = P(x+h) - P(x)$$

Fact

For any P, h, we always have

$$\deg(\Delta_h P) < \deg(P).$$

Derivative Fact 2

$$\text{bias}(f) = |\mathbb{E}_{x \in \mathbb{F}_p^n} \omega^{f(x)}|$$

$$\Delta_h P(x) = P(x+h) - P(x)$$

Theorem (Kaufman, Lovett)

There exists $s(p, d, \epsilon)$ such that, if $P \in \mathbb{F}_p[x_1, \ldots, x_n]$ has degree at most d and bias at least ϵ, then there exist $h_1, \ldots, h_r \in \mathbb{F}_p^n$, $\Gamma : \mathbb{F}_p^s \to \mathbb{F}_p$, such that

$$P(x) \equiv \Gamma\big(\Delta_{h_1} P(x), \ldots, \Delta_{h_s} P(x)\big)$$

Main Theorem Proof Outline

- **If high analytic rank:**
  - suffices to show equidistribution of $\phi(Z)$
  - can be thought of in terms of rank of the restriction; arank is natural so we apply the theorem from the other paper
- If low analytic rank:
  - Equivalent to saying a related polynomial has high bias
  - Functions with high bias have some coherent structure in terms of their derivatives
  - Exploiting that structure and doing some Fourier analysis, can write the claim in terms of a lower-degree instance
  - $\implies$ win by induction

High Analytic Rank

Lemma

There exists $R(d, \rho, \epsilon)$ *such that, if* $\deg(\phi) \leq d$ *and* $\operatorname{arank}_d(\phi) \geq R$*,*

$$\Pr_{Z \sim \mathcal{N}_p}[\phi(y + Z) = w] \leq \epsilon \text{ for all } y \in \mathbb{F}_p^n, w \in \mathbb{F}_p^k.$$

High Analytic Rank

Lemma

There exists $R(d, \rho, \epsilon)$ *such that, if* $\deg(\phi) \leq d$ *and* $\mathrm{arank}_d(\phi) \geq R$*,*

$$\Pr_{Z \sim \mathcal{N}_p}[\phi(y + Z) = w] \leq \epsilon \textit{ for all } y \in \mathbb{F}_p^n, w \in \mathbb{F}_p^k.$$

Proof:

- Since $x \mapsto \phi(y + x) - w$ has the same degree and analytic rank as ϕ, wlog $y = w = 0$.

High Analytic Rank

Lemma

There exists $R(d, \rho, \epsilon)$ *such that, if* $\deg(\phi) \leq d$ *and* $\operatorname{arank}_d(\phi) \geq R$*,*

$$\Pr_{Z \sim \mathcal{N}_p}[\phi(y + Z) = w] \leq \epsilon \text{ for all } y \in \mathbb{F}_p^n, w \in \mathbb{F}_p^k.$$

Proof:

- GOAL: $\Pr_{Z \sim \mathcal{N}_p}[\phi(Z) = 0] \leq \epsilon$.
- First, sample $I \sim [n]_{1-\rho}$ to be the corrupted coordinates, then choose the noise values.

High Analytic Rank

Lemma

There exists $R(d, \rho, \epsilon)$ *such that, if* $\deg(\phi) \leq d$ *and* $\operatorname{arank}_d(\phi) \geq R$*,*

$$\Pr_{Z \sim \mathcal{N}_p}[\phi(y + Z) = w] \leq \epsilon \text{ for all } y \in \mathbb{F}_p^n, w \in \mathbb{F}_p^k.$$

Proof:

- GOAL: $\Pr_{Z \sim \mathcal{N}_p}[\phi(Z) = 0] \leq \epsilon$.
- First, sample $I \sim [n]_{1-\rho}$, then choose the noise.
- Equivalently, randomly restrict ϕ, then give random input.

High Analytic Rank

Lemma

There exists $R(d, \rho, \epsilon)$ *such that, if* $\deg(\phi) \leq d$ *and* $\operatorname{arank}_d(\phi) \geq R$*,*

$$\Pr_{Z \sim \mathcal{N}_p} [\phi(y + Z) = w] \leq \epsilon \text{ for all } y \in \mathbb{F}_p^n, w \in \mathbb{F}_p^k.$$

Proof:

- GOAL: $\mathbb{E}_{I \sim [n]_{1-\rho}} \Pr_{z \in \mathbb{F}_p^I} [\phi_{|I}(z) = 0] \leq \epsilon$.
- Since the 0 polynomial has degree $< d$,

$$\mathbb{E}_{I \sim [n]_{1-\rho}} \Pr_{z \in \mathbb{F}_p^I} [\phi_{|I}(z) = 0] \leq \mathbb{E}_{I \sim [n]_{1-\rho}} p^{-\operatorname{arank}_d(\phi_{|I}}$$

High Analytic Rank

Lemma

There exists $R(d, \rho, \epsilon)$ *such that, if* $\deg(\phi) \leq d$ *and* $\operatorname{arank}_d(\phi) \geq R$*,*

$$\Pr_{Z \sim \mathcal{N}_p}[\phi(y + Z) = w] \leq \epsilon \text{ for all } y \in \mathbb{F}_p^n, w \in \mathbb{F}_p^k.$$

Proof:

- GOAL: $\mathbb{E}_{I \sim [n]_{1-\rho}} p^{-\operatorname{arank}_d(\phi_{|I}} \leq \epsilon$.
- Now, if we knew that analytic rank was natural, we could just apply the random restriction theorem.

Analytic Rank Is Natural

- Symmetry
- Sub-additivity
- Monotonicity under restrictions
- Lipschitz

Main Theorem Proof Outline

- If high analytic rank:
  - suffices to show equidistribution of $\phi(Z)$
  - can be thought of in terms of rank of the restriction; arank is natural so we apply the theorem from the other paper
- **If low analytic rank:**
  - Equivalent to saying a related polynomial has high bias
  - Functions with high bias have some coherent structure in terms of their derivatives
  - Exploiting that structure and doing some Fourier analysis, can write the claim in terms of a lower-degree instance
  - $\implies$ win by induction

SMALL ANALYTIC RANK

$$\text{Given: } \deg(\phi) \le d, \operatorname{arank}(\phi) < R$$
$$\text{Goal: } \Pr_{x\in\mathbb{F}_p^k,\ Z\sim\mathcal{N}_\rho}[\phi(E(x)+Z) = x] \le \epsilon.$$

$$\operatorname{arank}(\phi) < R$$

is equivalent to

$$\exists\psi, \deg(\psi) \le d-1, \Pr_{x\in\mathbb{F}_p^n}[\phi(x) = \psi(x)] \ge p^{-R}.$$

Small Analytic Rank

$$\text{Given: } \deg(\phi) \le d, \deg(\psi) \le d-1$$
$$\Pr_{x \in \mathbb{F}_p^n}[\phi(x) = \psi(x)] \ge p^{-R}.$$

$$\text{Goal: } \Pr_{x \in \mathbb{F}_p^k,\, Z \sim \mathcal{N}_\rho}[\phi(E(x) + Z) = x] \le \epsilon.$$

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

Small Analytic Rank

$$\text{Given: } \deg(\phi) \le d, \deg(\psi) \le d-1$$
$$\Pr_{x \in \mathbb{F}_p^n}[\phi(x) = \psi(x)] \ge p^{-R}.$$
$$\text{Goal: } \Pr_{x \in \mathbb{F}_p^k,\ Z \sim \mathcal{N}_\rho}[\phi(E(x) + Z) = x] \le \epsilon.$$

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

We have $\mathrm{bias}(P) = \mathbb{E}_y \, \mathbb{E}_v \, \omega^{\langle v, \tilde{\phi}(y) \rangle} = \Pr[\tilde{\phi}(y) = 0] \ge p^{-R}$.

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

We have $\mathrm{bias}(P) = \mathbb{E}_y \, \mathbb{E}_v \, \omega^{\langle v, \tilde{\phi}(y) \rangle} = \Pr[\tilde{\phi}(y) = 0] \geq p^{-R}$.

By Kaufman-Lovett, there exist s, $(h_1, w_1), \ldots, (h_s, w_s)$, Γ such that

$$P(y, v) = \Gamma(\Delta_{(h_1, w_1)} P(y, v), \ldots, \Delta_{(h_s, w_s)} P(y, v)).$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$P(y, v) = \Gamma(\Delta_{(h_1, w_1)} P(y, v), \ldots, \Delta_{(h_s, w_s)} P(y, v))$.

$$\Delta_{(h,w)} P(y, v) = P(y + h, v + w) - P(y, v)$$

$$= P(y + h, w) + P(y + h, v) - P(y, v)$$

$$= \langle w, \tilde{\phi}(y + h) \rangle + \langle v, \Delta_h \tilde{\phi}(y) \rangle$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$P(y, v) = \Gamma(\Delta_{(h_1,w_1)} P(y, v), \ldots, \Delta_{(h_s,w_s)} P(y, v))$.

$$\Delta_{(h,w)} P(y, v) = P(y + h, v + w) - P(y, v)$$

$$= P(y + h, w) + P(y + h, v) - P(y, v)$$

$$= \langle w, \tilde{\phi}(y + h) \rangle + \langle v, \Delta_h \tilde{\phi}(y) \rangle$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$P(y,v) = \Gamma\Bigg(\Big(\langle w_1, \tilde{\phi}(y + h_1) \rangle + \langle v, \Delta_{h_1} \tilde{\phi}(y) \rangle \Big) P(y,v),$$

$$\ldots, \Big(\langle w_s, \tilde{\phi}(y + h_s) \rangle + \langle v, \Delta_{h_1} \tilde{\phi}(y) \rangle \Big) P(y,v) \Bigg).$$

Letting $f(x) = \omega^{\Gamma(x)}$ and applying Fourier inversion,

$$\omega^{P(y,v)} = f(P(y,v)) = \sum_{\alpha \in \mathbb{F}_p^s} \widehat{f}(\alpha) \omega^{\langle \alpha, \ldots \rangle} = \sum_{\alpha \in \mathbb{F}_p^s} \widehat{f}(\alpha) \omega^{Q_\alpha(y) + \langle v, \gamma_\alpha(y) \rangle}$$

Where we define

$$Q_\alpha(y) = \sum_{i=1}^{s} \langle \alpha_i w_i, \tilde{\phi}(y + h_i) \rangle,$$

$$\gamma_\alpha(y) = \sum_{i=1}^{s} \alpha_i \Delta_{h_i} \tilde{\phi}(y).$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \dots, y_n, v_1, \dots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$P(y, v) = \Gamma\Bigg(\Big(\langle w_1, \tilde{\phi}(y + h_1) \rangle + \langle v, \Delta_{h_1} \tilde{\phi}(y) \rangle \Big) P(y, v),$$

$$\dots, \Big(\langle w_s, \tilde{\phi}(y + h_s) \rangle + \langle v, \Delta_{h_1} \tilde{\phi}(y) \rangle \Big) P(y, v) \Bigg).$$

Letting $f(x) = \omega^x$ and applying Fourier inversion,

$$\omega^{P(y,v)} = f(P(y, v)) = \sum_{\alpha \in \mathbb{F}_p^s} \widehat{f}(\alpha) \omega^{\langle \alpha, \dots \rangle} = \sum_{\alpha \in \mathbb{F}_p^s} \widehat{f}(\alpha) \omega^{Q_\alpha(y) + \langle v, \gamma_\alpha(y) \rangle}$$

Where we define

$$Q_\alpha(y) = \sum_{i=1}^{s} \langle \alpha_i w_i, \tilde{\phi}(y + h_i) \rangle,$$

$$\gamma_\alpha(y) = \sum_{i=1}^{s} \alpha_i \Delta_{h_i} \tilde{\phi}(y). \leftarrow \deg < d$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$\omega^{P(y,v)} = \sum_{\alpha \in \mathbb{F}_p^s} \widehat{f}(\alpha) \omega^{Q_\alpha(y) + \langle v, \gamma_\alpha(y) \rangle}$$

$$\deg(\gamma_\alpha(y)) < d$$

Now, note that

$$\mathbf{1}[\phi(y) = x] = \mathbb{E}_{v \in \mathbb{F}_p^k} \, \omega^{\langle v, \phi(y) - x \rangle}$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$\omega^{P(y,v)} = \sum_{\alpha \in \mathbb{F}_p^s} \widehat{f}(\alpha) \omega^{Q_\alpha(y) + \langle v, \gamma_\alpha(y) \rangle}$$

$$\deg(\gamma_\alpha(y)) < d$$

Now, note that

$$\mathbf{1}[\phi(y) = x] = \mathbb{E}_{v \in \mathbb{F}_p^k} \, \omega^{\langle v, \phi(y) - x \rangle}$$

$$= \mathbb{E}_{v \in \mathbb{F}_p^k} \, \omega^{\langle v, \phi(y) - x \rangle}$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$\omega^{P(y,v)} = \sum_{\alpha \in \mathbb{F}_p^s} \widehat{f}(\alpha) \omega^{Q_\alpha(y) + \langle v, \gamma_\alpha(y) \rangle}$$

$$\deg(\gamma_\alpha(y)) < d$$

Now, note that

$$\mathbf{1}[\phi(y) = x] = \mathbb{E}_{v \in \mathbb{F}_p^k} \, \omega^{\langle v, \phi(y) - x \rangle}$$

$$= \mathbb{E}_{v \in \mathbb{F}_p^k} \, \omega^{\langle v, \phi(y) - x \rangle} = \mathbb{E}_{v \in \mathbb{F}_p^k} \, \omega^{P(y,v) + \langle v, -\psi(y) - x \rangle}$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$\omega^{P(y,v)} = \sum_{\alpha \in \mathbb{F}_p^s} \widehat{f}(\alpha) \omega^{Q_\alpha(y) + \langle v, \gamma_\alpha(y) \rangle}$$

$$\deg(\gamma_\alpha(y)) < d$$

Now, note that

$$\mathbf{1}[\phi(y) = x] = \mathbb{E}_{v \in \mathbb{F}_p^k} \omega^{\langle v, \phi(y) - x \rangle}$$

$$= \mathbb{E}_{v \in \mathbb{F}_p^k} \omega^{\langle v, \phi(y) - x \rangle} = \mathbb{E}_{v \in \mathbb{F}_p^k} \omega^{P(y,v) + \langle v, -\psi(y) - x \rangle}$$

$$= \sum_{\alpha \in \mathbb{F}_p^s} \widehat{f}(\alpha) \omega^{Q_\alpha(y)} \mathbb{E}_{v \in \mathbb{F}_p^k} \omega^{\langle v, (\gamma_\alpha - \psi)(y) \rangle}$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$\deg(\gamma_\alpha(y)) < d$$

$$\Pr[\phi(E(x) + Z) = x] = \mathbb{E}_{x,Z}\, \mathbf{1}[\phi(E(x) + Z) = x]$$
$$= \mathbb{E}_{x,Z} \sum_{\alpha \in \mathbb{F}_p^s} \widehat{f}(\alpha) \omega^{Q_\alpha(y)}\, \mathbb{E}_{v \in \mathbb{F}_p^k}\, \omega^{\langle v, (\gamma_\alpha - \psi)(E(x)+Z) \rangle}$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$\deg(\gamma_\alpha(y)) < d$$

$$\Pr[\phi(E(x) + Z) = x] \leq$$

$$\sum_{\alpha \in \mathbb{F}_p^s} \left(|\widehat{f}(\alpha)| \, \mathbb{E}_{x,Z} \left| \omega^{Q_\alpha(y)} \, \mathbb{E}_{v \in \mathbb{F}_p^k} \, \omega^{\langle v, (\gamma_\alpha - \psi)(E(x)+Z) \rangle} \right| \right)$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$\deg(\gamma_\alpha(y)) < d$$

$$\Pr[\phi(E(x) + Z) = x] \leq$$

$$\left(\sum_{\alpha \in \mathbb{F}_p^s} |\widehat{f}(\alpha)| \right) \max_{\alpha \in \mathbb{F}_p^s} \mathbb{E}_{x,Z} \left| \omega^{Q_\alpha(y)} \, \mathbb{E}_{v \in \mathbb{F}_p^k} \, \omega^{\langle v, (\gamma_\alpha - \psi)(E(x)+Z) \rangle} \right|$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$\deg(\gamma_\alpha(y)) < d$$

$$\Pr[\phi(E(x) + Z) = x] \leq$$

$$p^{s/2} \max_{\alpha \in \mathbb{F}_p^s} \mathbb{E}_{x,Z} \left| \omega^{Q_\alpha(y)} \, \mathbb{E}_{v \in \mathbb{F}_p^k} \, \omega^{\langle v, (\gamma_\alpha - \psi)(E(x)+Z) \rangle} \right|$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$\deg(\gamma_\alpha(y)) < d$$

$$\Pr[\phi(E(x) + Z) = x] \leq$$

$$p^{s/2} \max_{\alpha \in \mathbb{F}_p^s} \mathbb{E}_{x,Z} \mathbf{1}[(\gamma_\alpha - \psi)(E(x) + Z) = x]$$

Small Analytic Rank

Define $\tilde{\phi} = \phi - \psi$, $P(y_1, \ldots, y_n, v_1, \ldots, v_k) = \langle v, \tilde{\phi}(y) \rangle$.

$$\deg(\gamma_\alpha(y)) < d$$

$$\Pr[\phi(E(x) + Z) = x] \leq$$

$$p^{s/2} \max_{\alpha \in \mathbb{F}_p^s} \Pr[(\gamma_\alpha - \psi)(E(x) + Z) = x]$$

$$\leq \epsilon$$

We're now looking at $(\gamma_\alpha - \psi)$, which is a polynomial of degree $d - 1$ – by the induction hypothesis, beyond some k the above will always hold.

Main Theorem Proof Outline

- If high analytic rank:
  - suffices to show equidistribution of $\phi(Z)$
  - can be thought of in terms of rank of the restriction; arank is natural so we apply the theorem from the other paper
- If low analytic rank:
  - Equivalent to saying a related polynomial has high bias
  - Functions with high bias have some coherent structure in terms of their derivatives
  - Exploiting that structure and doing some Fourier analysis, can write the claim in terms of a lower-degree instance
  - $\implies$ win by induction

Core Property

Definition

A notion of rank satisfies the (A, B)**-core property** if, for every (sufficiently high-rank) d-tensor T, there exist $J_1, \ldots, J_d \subset$ of size at most $A(\mathrm{rk}(T))$ such that $\mathrm{rk}(T_{|J_{[d]}} \geq B(\mathrm{rk}(T))$.

Core Property

Definition

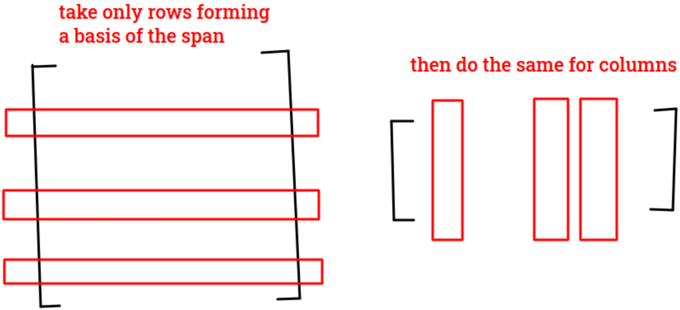
A notion of rank satisfies the (A, B)**-core property** if, for every (sufficiently high-rank) d-tensor T, there exist $J_1, \ldots, J_d \subset$ of size at most $A(\mathrm{rk}(T))$ such that $\mathrm{rk}(T_{|J_{[d]}} \geq B(\mathrm{rk}(T))$.

Definition

rk satisfies the **linear core property** if A and B are linear functions.

Matrix Rank Satisfies Core Property

For matrix rank, we can set both A and B to be $x \mapsto x$ (perfect linear core property).



Why Linear Core Property is Strong

Theorem

If a natural rank rk *satisfies the linear core property, for every* σ *there exist* $C, \kappa > 0$ *such that, for every d-tensor* T*,*

$$\Pr_{I \sim [n_1]_\sigma, \ldots, I_d \sim [n_d]_\sigma} [\operatorname{rk}(T_{|I_{[d]}}) > \kappa \operatorname{rk}(T)] \geq 1 - Ce^{-\kappa \operatorname{rk}(T)}.$$

Why Linear Core Property is Strong

Theorem

If a natural rank rk *satisfies the linear core property, for every* σ *there exist* $C, \kappa > 0$ *such that, for every d-tensor* T*,*

$$\Pr_{I \sim [n_1]_\sigma, \ldots, I_d \sim [n_d]_\sigma} [\mathrm{rk}(T_{|I_{[d]}}) > \kappa \,\mathrm{rk}(T)] \geq 1 - Ce^{-\kappa \,\mathrm{rk}(T)}.$$

Proof: Fix some sets $J_1, \ldots, J_d$ of size $a\,\mathrm{rk}(T)$ such that $\mathrm{rk}(T_{J_{[d]}} \geq b\,\mathrm{rk}(T)$. Choose $\lambda = b/(3da)$. By Chernoff bound, if we do a $(1-\lambda)$-restriction, w.h.p. all J_is have at least $(1-2\lambda)$ fraction remaining.

WHY LINEAR CORE PROPERTY IS STRONG

Theorem

If a natural rank rk *satisfies the linear core property, for every* σ *there exist* $C, \kappa > 0$ *such that, for every d-tensor* T*,*

$$\Pr_{I \sim [n_1]_\sigma, \ldots, I_d \sim [n_d]_\sigma} [\mathrm{rk}(T_{|I_{[d]}}) > \kappa\, \mathrm{rk}(T)] \geq 1 - Ce^{-\kappa\, \mathrm{rk}(T)}.$$

Proof: Fix some sets $J_1, \ldots, J_d$ of size $a\, \mathrm{rk}(T)$ such that $\mathrm{rk}(T_{J_{[d]}} \geq b\, \mathrm{rk}(T)$. Choose $\lambda = b/(3da)$. By Chernoff bound, if we do a $(1-\lambda)$-restriction, w.h.p. all J_is have at least $(1-2\lambda)$ fraction remaining.

$$\Pr_{I \sim [n_1]_{1-\lambda}, \ldots, I_d \sim [n_d]_{1-\lambda}} [\mathrm{rk}(T_{|I_{[d]}}) \geq \frac{c}{3}\, \mathrm{rk}(T)] \geq 1 - Ce^{-\kappa\, \mathrm{rk}(T)}.$$

WHY LINEAR CORE PROPERTY IS STRONG

Theorem

If a natural rank rk *satisfies the linear core property, for every* σ *there exist* $C, \kappa > 0$ *such that, for every d-tensor* T*,*

$$\Pr_{I \sim [n_1]_\sigma, \ldots, I_d \sim [n_d]_\sigma} [\operatorname{rk}(T_{|I_{[d]}}) > \kappa \operatorname{rk}(T)] \geq 1 - Ce^{-\kappa \operatorname{rk}(T)}.$$

$$\Pr_{I \sim [n_1]_{1-\lambda}, \ldots, I_d \sim [n_d]_{1-\lambda}} [\operatorname{rk}(T_{|I_{[d]}}) \geq \frac{c}{3} \operatorname{rk}(T)] \geq 1 - Ce^{-\kappa \operatorname{rk}(T)}.$$

Now, just iterate this argument t times until $(1-\lambda)^t < \sigma$.

Conclusion / Lingering Questions