Decoding Ta-Shma's Binary Codes

Fernando Granha Jeronimo
(UChicago)

based on joint work with

Vedat Levi Alev (UWaterloo),
Dylan Quintana (UChicago),
Shashank Srivastava (TTIC) and
Madhur Tulsiani (TTIC)

Junior Theorists Workshop 2020
Northwestern

Goal of the Talk

Goal

Present two efficient decoding algorithms for Ta-Shma's codes

Goal of the Talk

Goal

Present two efficient decoding algorithms for Ta-Shma's codes

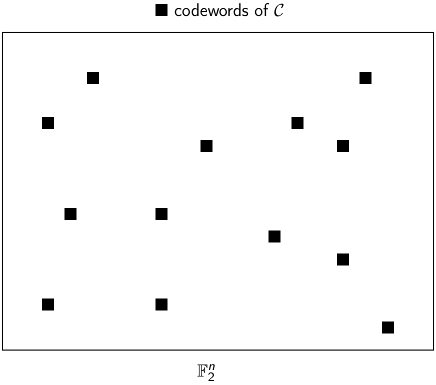
While highlighting connections among:

- Approximation and Optimization
- Pseudorandomness and Expansion
- Coding Theory

Coding Theory Concepts

Code

A binary code is a subset $\mathcal{C} \subseteq \mathbb{F}_2^n$



Coding Theory Concepts

Two fundamental parameters

Distance

The distance $\Delta(\mathcal{C})$ of $\mathcal{C}$ is $\Delta(\mathcal{C}) := \min_{z,z' \in \mathcal{C}\colon z \neq z'} \Delta(z, z')$

Coding Theory Concepts

Two fundamental parameters

Distance

The distance $\Delta(\mathcal{C})$ of $\mathcal{C}$ is $\Delta(\mathcal{C}) := \min_{z,z' \in \mathcal{C}\,:\, z \neq z'} \Delta(z, z')$

Rate

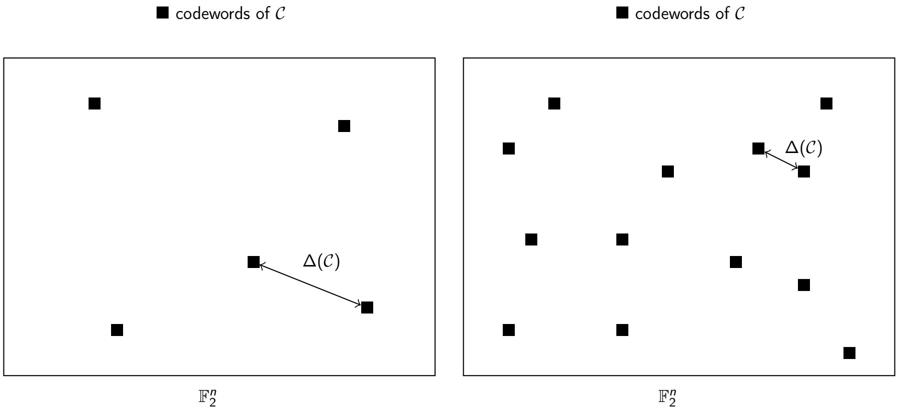
The rate $r(\mathcal{C})$ of $\mathcal{C}$ is $\frac{\log_2(|\mathcal{C}|)}{n}$ (the fraction of information symbols)

Tension between Rate and Distance of a Code

Tension

- Higher rate $r(\mathcal{C})$, lower distance $\Delta(\mathcal{C})$
- Higher distance $\Delta(\mathcal{C})$, lower rate $r(\mathcal{C})$

Tension between Rate and Distance of a Code



Lower rate $r(\mathcal{C})$

Higher rate $r(\mathcal{C})$

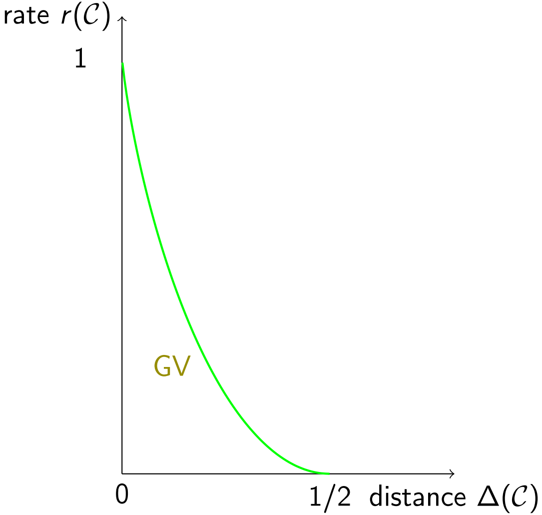
Coding Theory Concepts

Question

What is the best trade-off between rate $r(\mathcal{C})$ and distance $\Delta(\mathcal{C})$?

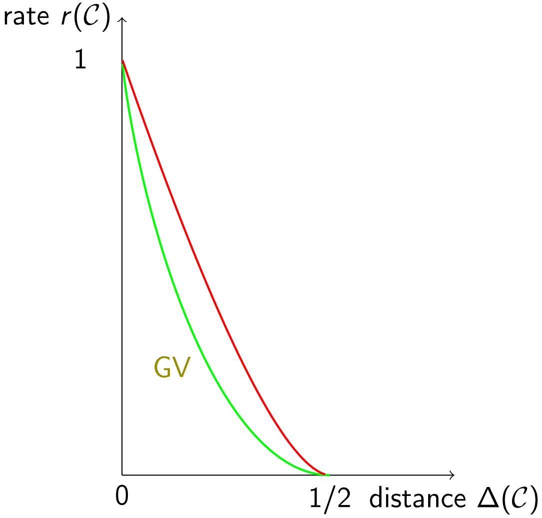
Coding Theory Concepts

Gilbert–Varshamov existential bound (Gilbert'52,Varshamov'57)

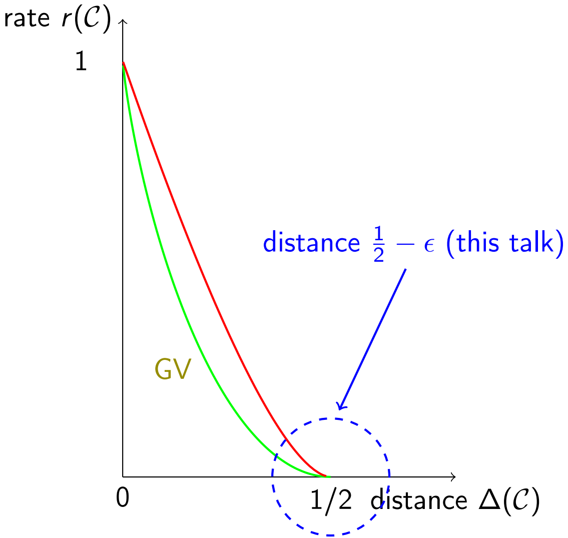


Coding Theory Concepts

McEliece–Rodemich–Rumsey–Welch'77 impossibility bound



Coding Theory Concepts



Coding Theory Concepts

Why is the Gilbert–Varshamov bound interesting?

The Gilbert–Varshamov (GV) bound is *"nearly"* optimal

For distance $1/2 - \epsilon$

- rate $\Omega(\epsilon^2)$ is achievable (Gilbert–Varshamov bound)
- rate better than $O(\epsilon^2 \log(1/\epsilon))$ is impossible (McEliece *et al.*)

Coding Theory Concepts

For distance $1/2 - \epsilon$

- rate $\Omega(\epsilon^2)$ is achievable (Gilbert–Varshamov bound)
- rate better than $O(\epsilon^2 \log(1/\epsilon))$ is impossible (McEliece *et al.*)

Ta-Shma's Codes (60 years later!)

First **explicit** binary codes near the GV bound are due to Ta-Shma'17 with

- distance $1/2 - \epsilon/2$ (actually ϵ-balanced), and
- rate $\Omega(\epsilon^{2+o(1)})$.

Coding Theory Concepts

Ta-Shma's Codes (60 years later!)

First **explicit** binary codes near the GV bound are due to Ta-Shma'17 with

- distance $1/2 - \epsilon/2$ (actually ϵ-balanced), and
- rate $\Omega(\epsilon^{2+o(1)})$.

Open at the time

It was an open question whether Ta-Shma's codes admit efficient decoding

Coding Theory Concepts

Open at the time

It was an open question whether Ta-Shma's codes admit efficient decoding

Theorem (this talk)

Ta-Shma's codes are polynomial (even near-linear) time unique decodable

Our Contribution

Theorem (Near-linear Time Decoding)

For every $\epsilon > 0$, $\exists$ *explicit binary linear Ta-Shma codes* $\mathcal{C}_{N,\epsilon} \subseteq \mathbb{F}_2^N$ *with*

1. *distance at least* $1/2 - \epsilon/2$ *(actually* ϵ*-balanced),*
2. *rate* $\Omega(\epsilon^{2+o(1)})$*, and*
3. *a unique decoding algorithm with running time* $\widetilde{O}_\epsilon(N)$.

Our Contribution

Pseudorandomness approach

Theorem (Near-linear Time Decoding)

For every $\epsilon > 0$, $\exists$ explicit binary linear Ta-Shma codes $\mathcal{C}_{N,\epsilon} \subseteq \mathbb{F}_2^N$ with

1. *distance at least $1/2 - \epsilon/2$ (actually ϵ-balanced),*
2. *rate $\Omega(\epsilon^{2+o(1)})$, and*
3. *a unique decoding algorithm with running time $\widetilde{O}_\epsilon(N)$.*

Our Contribution

Sum-of-Squares SDP hierarchy approach (SOS approach)

Theorem (J-Quintana-Srivastava-Tulsiani'20)

Ta-Shma's codes are unique decodable in $N^{O_\epsilon(1)}$ *time*

Related Work (a Sample)

Theorem (Guruswami–Indyk'04)

*Efficiently decodable **non-explicit** binary codes at the GV bound*

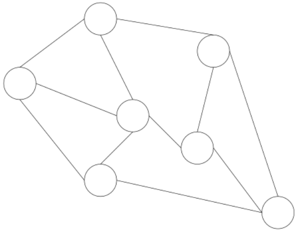
Theorem (Hemenway–Ron-Zewi–Wootters'17)

*Near-linear time decodable **non-explicit** binary codes at the GV bound*

Towards Ta-Shma's Codes

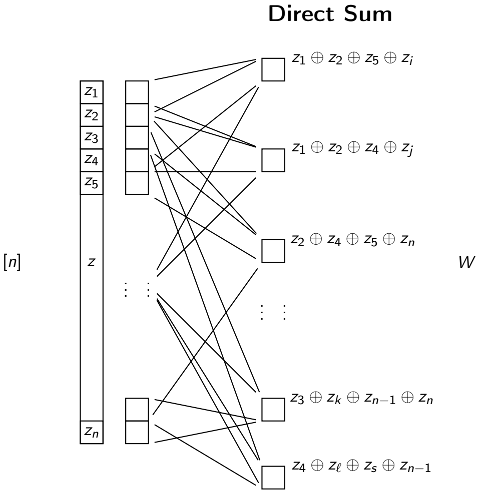
Expander Graphs and Codes

Expanders can amplify the distance of a not so great base code $\mathcal{C}_0$



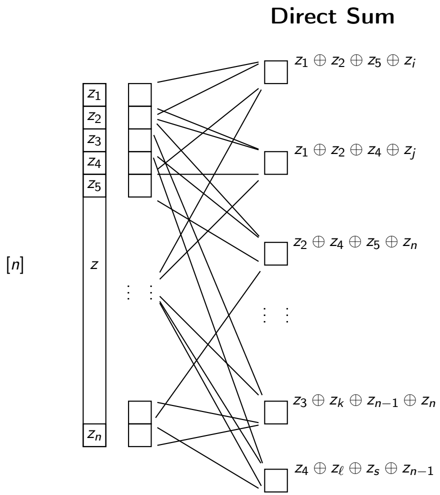
Expansion and Distance Amplification

Fix a bipartite graph between $[n]$ and $W \subseteq [n]^k$. Let $z \in \mathbb{F}_2^n$.



Expansion and Distance Amplification

Fix a bipartite graph between $[n]$ and $W \subseteq [n]^k$. Let $z \in \mathbb{F}_2^n$.



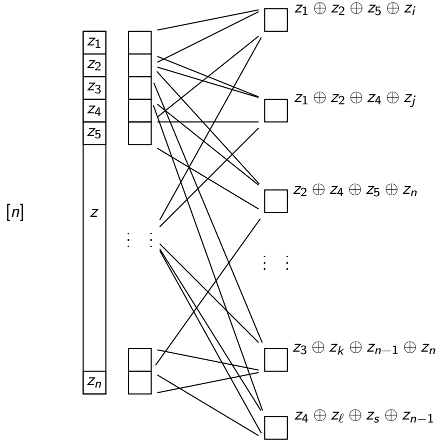
rate loss factor $n/|W|$

distance amplification needs to be worth this loss

Expansion and Distance Amplification

Fix a bipartite graph between $[n]$ and $W \subseteq [n]^k$. Let $z \in \mathbb{F}_2^n$.

Direct Sum



W

rate loss factor $n/|W|$

distance amplification needs to be worth this loss

Alon–Brooks–Naor–Naor–Roth & Alon–Edmonds–Luby *style* distance amplification

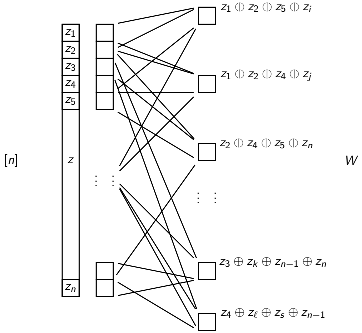
Expansion and Distance Amplification

Direct Sum

Let $z \in \mathbb{F}_2^n$ and $W \subseteq [n]^k$. The *direct sum* of z is $y \in \mathbb{F}_2^{W}$ defined as

$$y_{(i_1,\ldots,i_k)} = z_{i_1} \oplus \cdots \oplus z_{i_k},$$

for every $(i_1, \ldots, i_k) \in W$. We denote $y = \text{dsum}_W(z)$.



Expansion and Distance Amplification

Bias

- Let $z \in \mathbb{F}_2^n$. Define $\text{bias}(z) := \left| \mathbf{E}_{i \in [n]} (-1)^{z_i} \right|$
- $\text{bias}(\mathcal{C}) = \max_{z \in \mathcal{C} \setminus 0} \text{bias}(z)$
- If $\text{bias}(\mathcal{C}) \leq \epsilon$, then $\Delta(\mathcal{C}) \geq 1/2 - \epsilon/2$ (assuming $\mathcal{C}$ linear)

Expansion and Distance Amplification

Bias

- Let $z \in \mathbb{F}_2^n$. Define $\text{bias}(z) := |\mathbf{E}_{i \in [n]} (-1)^{z_i}|$
- $\text{bias}(\mathcal{C}) = \max_{z \in \mathcal{C} \setminus 0} \text{bias}(z)$
- If $\text{bias}(\mathcal{C}) \leq \epsilon$, then $\Delta(\mathcal{C}) \geq 1/2 - \epsilon/2$ (assuming $\mathcal{C}$ linear)

$$\text{bias}(\underbrace{00\ldots0}_{n}) = \text{bias}(\underbrace{11\ldots1}_{n}) = 1$$

$$\text{bias}(\underbrace{0\ldots0}_{n/2}\underbrace{1\ldots1}_{n/2}) = 0$$

Expansion and Distance Amplification

Bias

- Let $z \in \mathbb{F}_2^n$. Define $\text{bias}(z) := \left| \mathbf{E}_{i \in [n]} (-1)^{z_i} \right|$
- $\text{bias}(\mathcal{C}) = \max_{z \in \mathcal{C} \setminus 0} \text{bias}(z)$
- If $\text{bias}(\mathcal{C}) \leq \epsilon$, then $\Delta(\mathcal{C}) \geq 1/2 - \epsilon/2$ (assuming $\mathcal{C}$ linear)

Definition (Parity Sampler, c.f. Ta-Shma'17)

Let $W \subseteq [n]^k$. We say that dsum_W is (ϵ_0, ϵ)-**parity sampler** iff

$$(\forall z \in \mathbb{F}_2^n) \left(\text{bias}(z) \leq \epsilon_0 \implies \text{bias}(\text{dsum}_W(z)) \leq \epsilon \right).$$

Expanders and Distance Amplification

Parity Samplers

Where to look for good parity samplers $W \subseteq [n]^k$?

Expanders and Distance Amplification

A Dream Parity Sampler

Let $z \in \mathbb{F}_2^n$ with $\text{bias}(z) = \epsilon_0$. Let $W = [n]^k$. Then

$$\text{bias}\left(\text{dsum}_W(z)\right) \leq \left|\mathbf{E}_{i \in [n]}(-1)^{z_i}\right|^k \leq \epsilon_0^k,$$

implying that W is a $(\epsilon_0, \epsilon_0^k)$-parity sampler (for every ϵ_0).

Expanders and Distance Amplification

A Dream Parity Sampler

Let $z \in \mathbb{F}_2^n$ with $\text{bias}(z) = \epsilon_0$. Let $W = [n]^k$. Then

$$\text{bias}\left(\text{dsum}_W(z)\right) \leq \left|\mathbf{E}_{i \in [n]}(-1)^{z_i}\right|^k \leq \epsilon_0^k,$$

implying that W is a $(\epsilon_0, \epsilon_0^k)$-parity sampler (for every ϵ_0).

Issue: Vanishing Rate

W is **"too dense"** so distance amplified code has rate $\leq 1/n^{k-1}$

Expanders and Distance Amplification

Another Dream Parity Sampler

Sample a uniformly random $W \subseteq [n]^k$ of size $\Theta_{\epsilon_0}(n/\epsilon^2)$.
Then w.h.p. dsum_W is (ϵ_0, ϵ)-parity sampler.

Expanders and Distance Amplification

Another Dream Parity Sampler

Sample a uniformly random $W \subseteq [n]^k$ of size $\Theta_{\epsilon_0}(n/\epsilon^2)$.
Then w.h.p. dsum_W is (ϵ_0, ϵ)-parity sampler.

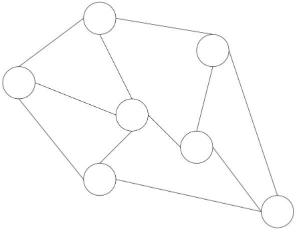
Issue: Non-explicit

Now W has near optimal size but it is non-explicit

Explicit Constructions of Parity Samplers

Solution (Alon and Rozenman–Wigderson)

Take $W \subseteq [n]^k$ to be the collection of **all** length-$(k-1)$ walks on a sparse expander graph $G = (V = [n], E)$



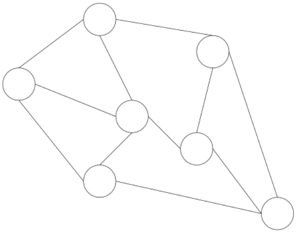
Explicit Constructions of Parity Samplers

Solution (Alon and Rozenman–Wigderson)

Take $W \subseteq [n]^k$ to be the collection of **all** length-$(k-1)$ walks on a sparse expander graph $G = (V = [n], E)$

Solution (good but not near optimal)

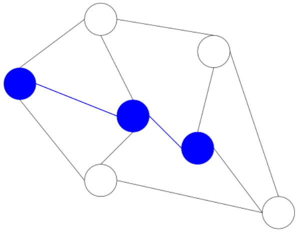
This yields codes of distance $1/2 - \epsilon$ and rate $\Omega(\epsilon^{4+o(1)})$



Explicit Constructions of Parity Samplers

Solution of Ta-Shma'17

Take $W \subseteq [n]^k$ to be a **carefully chosen** collection of length-$(k-1)$ walks on a structured sparse expander graph $G = (V = [n], E)$



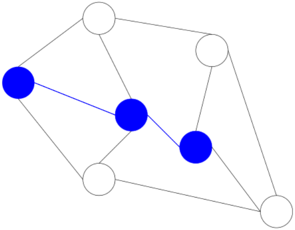
Explicit Constructions of Parity Samplers

Solution of Ta-Shma'17

Take $W \subseteq [n]^k$ to be a **carefully chosen** collection of length-$(k-1)$ walks on a structured sparse expander graph $G = (V = [n], E)$

Solution (near optimal)

This yields codes of distance $1/2 - \epsilon$ and rate $\Omega(\epsilon^{2+o(1)})$



General Techniques for Decoding

Decoding Direct Sum

What does decoding look like for direct sum?

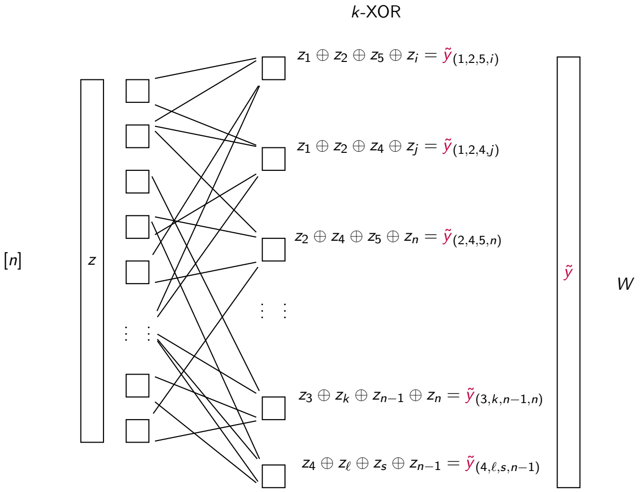
Decoding by Solving a k-CSP

Setup (informal)

- $\mathcal{C}_0 \subseteq \mathbb{F}_2^n$ is a code of small distance
- $W \subseteq [n]^k$ for direct sum
- $\mathcal{C} = \text{dsum}_W(\mathcal{C}_0)$ is a code of large distance

Decoding by Solving a k-CSP

Suppose $y^* \in \mathcal{C}$ is corrupted into some $\tilde{y} \in \mathbb{F}_2^W$ in the unique decoding ball centered at y^*.



Decoding by Solving a k-CSP

Unique Decoding Scenario: k-XOR like

Unique decoding $\tilde{y}$ amounts to solving

$$\arg\max_{z \in \mathcal{C}_0} \mathbf{E}_{(i_1,\ldots,i_k)\in W} \mathbf{1}[z_{i_1} \oplus \cdots \oplus z_{i_k} = \tilde{y}_{(i_1,\ldots,i_k)}].$$

Decoding by Solving a k-CSP

Unique Decoding Scenario: k-XOR like

Unique decoding $\tilde{y}$ amounts to solving

$$\arg\max_{z \in \mathcal{C}_0} \mathbf{E}_{(i_1,\ldots,i_k)\in W} \mathbf{1}[z_{i_1} \oplus \cdots \oplus z_{i_k} = \tilde{y}_{(i_1,\ldots,i_k)}].$$

A Relaxation

Suppose that we can find $\tilde{z} \in \mathbb{F}_2^n$ (rather than in $\mathcal{C}_0$) satisfying

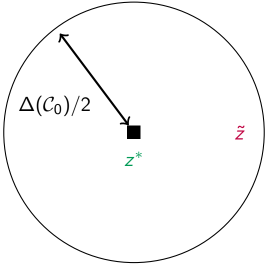
$$\mathbf{E}_{(i_1,\ldots,i_k)\in W} \mathbf{1}[\tilde{z}_{i_1} \oplus \cdots \oplus \tilde{z}_{i_k} = \tilde{y}_{(i_1,\ldots,i_k)}] \approx \mathsf{OPT}.$$

Decoding by Solving a k-CSP

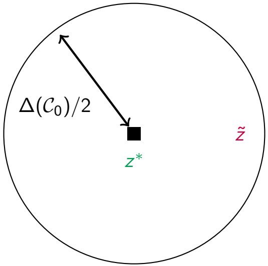
Say $y^* = \text{dsum}(z^*)$ for some $z^* \in \mathcal{C}_0$

Claim (Informal)

If the parity sampler is *strong enough*, then $\tilde{z}$ lies in the unique decoding ball centered at $z^* \in \mathcal{C}_0$.



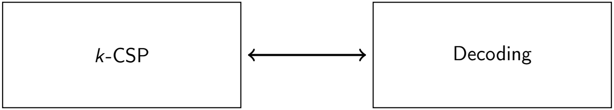
Decoding by Solving a k-CSP



Moral

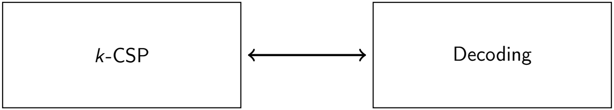
- Find approx. optimal solution $\tilde{z} \in \mathbb{F}_2^n$ (rather than in $\mathcal{C}_0$) is enough
- Use unique decoder of $\mathcal{C}_0$ to correct $\tilde{z}$ into z^*

What do we have so far?



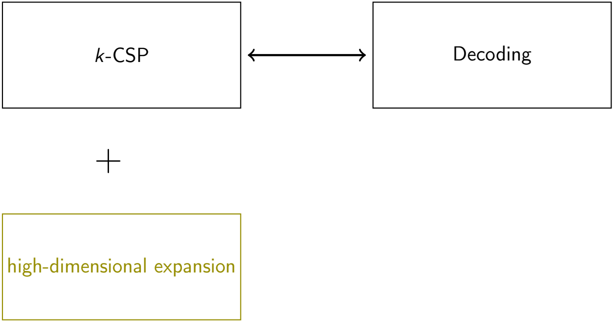
What do we have so far?

Why can we efficiently approximate these k-CSPs?



What do we have so far?

Why can we efficiently approximate these k-CSPs?

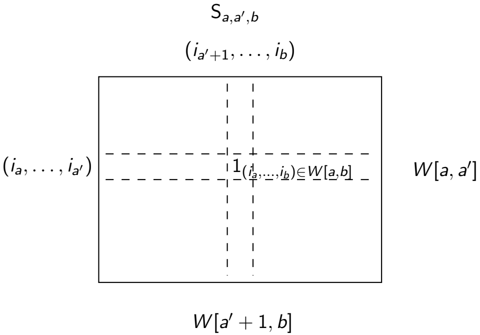


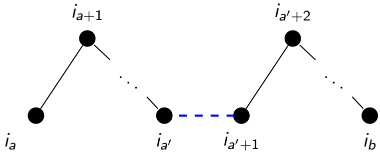
A Notion of High-dimensional Expansion

Let $W \subseteq [n]^k$. Define $W[a,b]$ for $1 \leq a \leq b \leq k$ as

$$W[a,b] = \{(i_a, \ldots, i_b) \mid (i_1, \ldots, i_k) \in W\}.$$

A Notion of High-dimensional Expansion





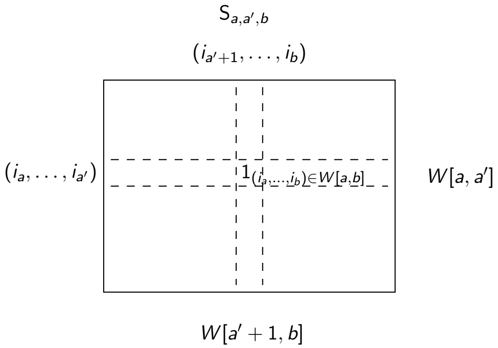
$$W[a, b] = \{(i_a, \ldots, i_b) \mid (i_1, \ldots, i_k) \in W\}$$

A Notion of High-dimensional Expansion

Definition (Splittability (informal))

A collection $W \subseteq [n]^k$ is said to be τ-splittable, if $k = 1$ or for every $1 \leq a \leq a' < b \leq k$:

1. The (normalized) matrix $\mathsf{S}_{a,a',b} \in \mathbb{R}^{W[a,a'] \times W[a'+1,b]}$ defined as $\mathsf{S}_{a,a',b}(w, w') = 1_{ww' \in W[a,b]}$ satisfy $\sigma_2(\mathsf{S}_{a,a',b}) \leq \tau$

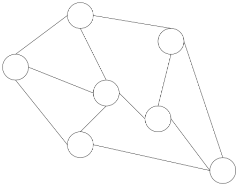


A Notion of High-dimensional Expansion

Example of τ-splittable structures

Lemma (Alev–J–Quintana–Srivastava–Tulsiani'20)

*The collection $W \subseteq [n]^k$ of **all** walks on τ-two-sided spectral expander graph $G = (V = [n], E)$ is τ-splittable*

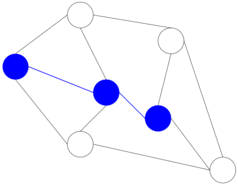


A Notion of High-dimensional Expansion

Example of τ-splittable structures

Lemma (J–Quintana–Srivastava–Tulsiani'20)

A simple modification of Ta-Shma's parity sampler $W \subseteq [n]^k$ is τ-splittable

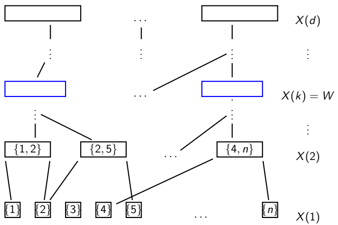


A Notion of High-dimensional Expansion

Example of τ-splittable structures

Theorem (Alev–J–Tulsiani'19 and Dikstein–Dinur'19)

The collection W of hyperedges of sufficiently expanding high-dimensional expander (link spectral HDX [Dinur–Kaufman]) is τ-splittabe



Sum-of-Squares Approach

Sum-of-Squares

k-CSP ⟷ Decoding

$+$

high-dimensional expansion

Sum-of-Squares Approach

Using the Sum-of-Squares (SOS) semi-definite programming hierarchy:

Theorem (Alev–J–Tulsiani'19 (informal))

Instances of k-XOR supported on expanding (τ-splittable) tuples $W \subseteq [n]^k$ can be efficiently approximated

(building on Barak–Raghavendra–Steurer'11)

Sum-of-Squares Approach

Using the Sum-of-Squares (SOS) semi-definite programming hierarchy:

Theorem (Alev–J–Tulsiani'19)

Let $W \subseteq [n]^k$ be τ-splittable. Suppose $\mathfrak{I}$ is a k-XOR instance on W. If $\tau \leq \text{poly}(\delta/2^k)$, then we can find a solution $z \in \mathbb{F}_2^n$ satisfying

$$\text{OPT}(\mathfrak{I}) - \delta,$$

fraction of the constraints of $\mathfrak{I}$ in time $n^{\text{poly}(2^k/\delta)}$.

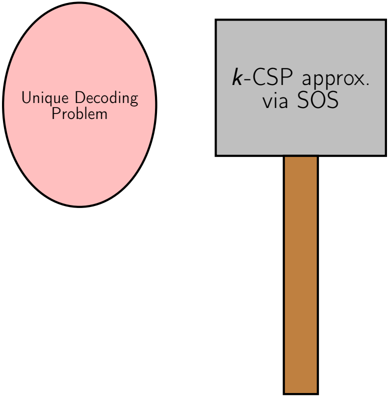
(building on Barak–Raghavendra–Steurer'11)

Sum-of-Squares Approach

What are the techniques?

We will just mention the techniques at a very high-level

Sum-of-Squares Approach



Sum-of-Squares Approach

Well... Our parameters...

We can only decode codes $\mathcal{C}$ satisfying

- $\Delta(\mathcal{C}) \geq 1/2 - \epsilon$, and
- rate $r(\mathcal{C}) = 2^{-\text{polylog}(1/\epsilon)} \ll \epsilon^{2+o(1)}$ (not even polynomial rate)

Sum-of-Squares Approach

Leveraging Unique Decoding to List Decoding AJQST'20

Maximizing an entropic function Ψ while "solving" the Sum-of-Squares program of unique decoding yields a list decoding algorithm

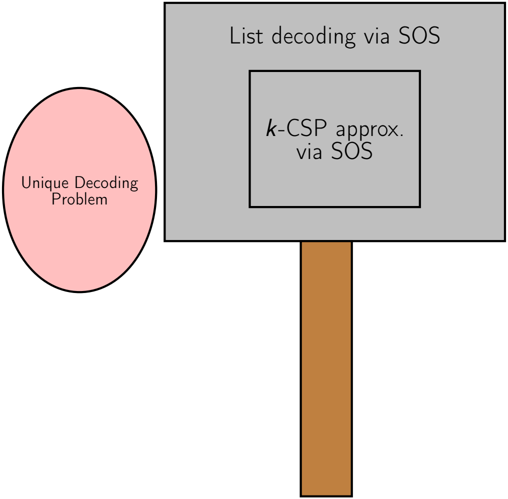
Sum-of-Squares Approach

Leveraging Unique Decoding to List Decoding AJQST'20

Maximizing an entropic function Ψ while "solving" the Sum-of-Squares program of unique decoding yields a list decoding algorithm

Several independent applications in robust statistics:
Raghavendra–Yau & Karmalkar–Klivans–Kothari to regression
by Raghavendra–Yau & Bakshi–Kothari to subspace recovery
by Bakshi–Kothari to clustering mixtures of Gaussians

Sum-of-Squares Approach



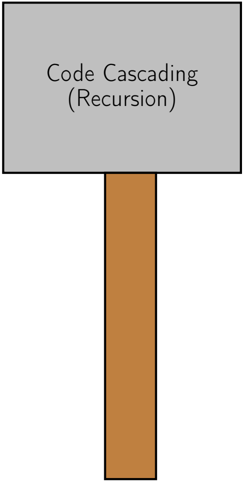
Sum-of-Squares Approach

Second Hammer Effect

We can only decode codes $\mathcal{C}$ satisfying

- $\Delta(\mathcal{C}) \geq 1/2 - \epsilon$, and
- rate $r(\mathcal{C}) = 2^{-\mathsf{polylog}(1/\epsilon)} \ll \epsilon^{2+o(1)}$ (not even polynomial rate)

Sum-of-Squares Approach



Sum-of-Squares Approach

Ta-Shma's walks admit a recursive structure

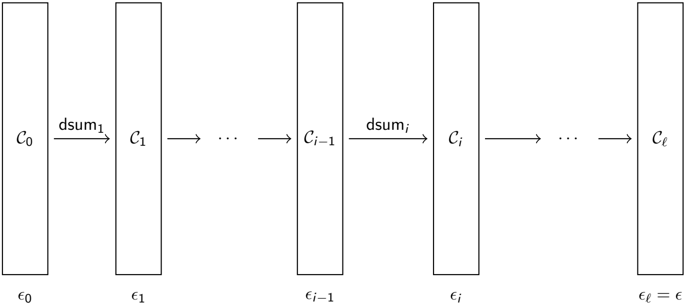
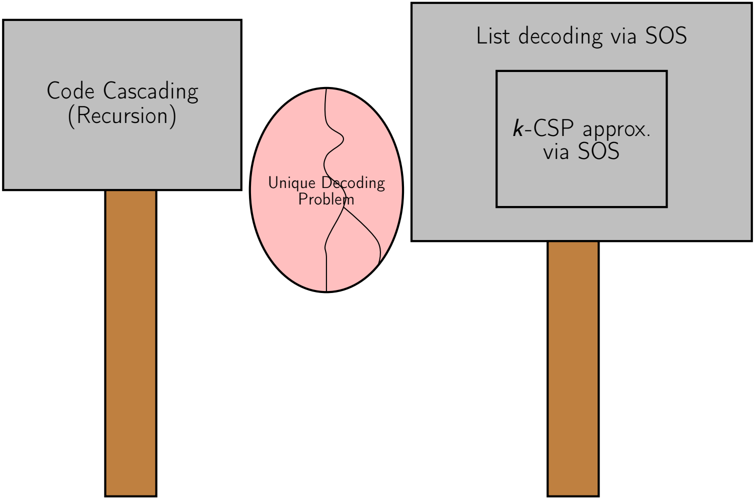
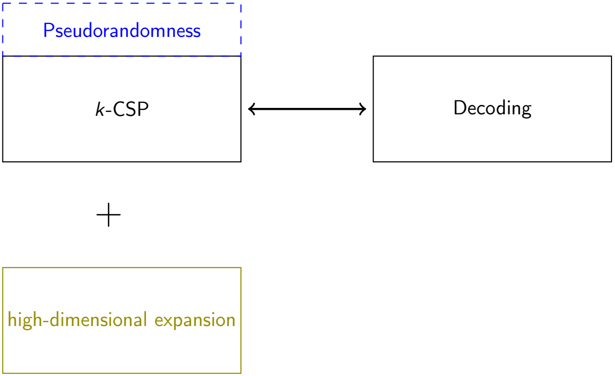


Figure: Code cascading: recursive construction of codes.

Sum-of-Squares Approach



Pseudorandomness Approach



Pseudorandomness Approach

Using pseudorandomness techniques (weak regularity decompositions):

Theorem (J–Srivastava–Tulsiani'20)

Let $W \subseteq [n]^k$ be τ-splittable. Suppose $\mathfrak{I}$ is a k-XOR instance on W. If $\tau \leq \text{poly}(\delta/k)$, then we can find a solution $z \in \mathbb{F}_2^n$ satisfying

$$\text{OPT}(\mathfrak{I}) - \delta,$$

fraction of the constraints of $\mathfrak{I}$ in time $\widetilde{O}_\delta(|W|)$.

Weak Regularity Decomposition: Dense Graphs

We recall Frieze and Kannan'96 approach.
Let A be the adjacency matrix of a **dense** graph $G = ([n], E)$. Suppose we have $A \approx \sum_{\ell=1}^{L} c_i \cdot 1_{S_1^i} \otimes 1_{S_2^i}$ such that

$$\max_{S,T \subseteq [n]} \left| \langle A - \sum_{\ell=1}^{L} c_i \cdot 1_{S_1^i} \otimes 1_{S_2^i}, 1_S \otimes 1_T \rangle \right| \leq \delta \cdot n^2,$$

and $L = O(1/\delta^2)$.

Weak Regularity Decomposition: Dense Graphs

Frieze and Kannan use $\sum_{\ell=1}^{L} c_i \cdot 1_{S_1^i} \otimes 1_{S_2^i}$ to approximate the **maximum cut** value of G within additive error $\delta \cdot n^2$

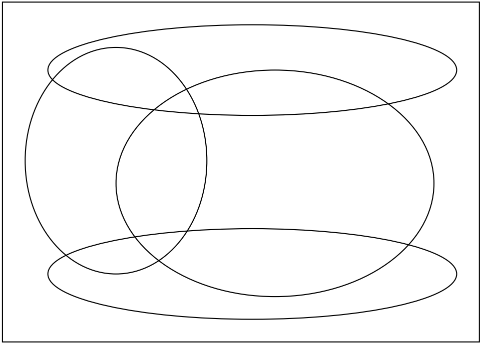
$$|E(S, \overline{S})| = \langle A, 1_S \otimes 1_{\overline{S}} \rangle \approx \langle \sum_{\ell=1}^{L} c_i \cdot 1_{S_1^i} \otimes 1_{S_2^i}, 1_S \otimes 1_{\overline{S}} \rangle,$$

$$= \sum_{\ell=1}^{L} c_i \cdot |S_1^i \cap S||S_2^i \cap \overline{S}|,$$

Weak Regularity Decomposition: Dense Graphs

$$|E(S,\overline{S})| \approx \sum_{\ell=1}^{L} c_i \cdot |S_1^i \cap S||S_2^i \cap \overline{S}|$$

Venn diagram of sets S_1^i, S_2^i for $i \in [L]$

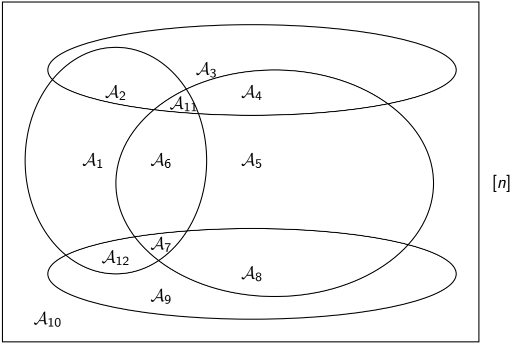


$[n]$

Weak Regularity Decomposition: Dense Graphs

$$|E(S, \overline{S})| \approx \sum_{\ell=1}^{L} c_i \cdot |S_1^i \cap S||S_2^i \cap \overline{S}|$$

Venn diagram of sets S_1^i, S_2^i for $i \in [L]$

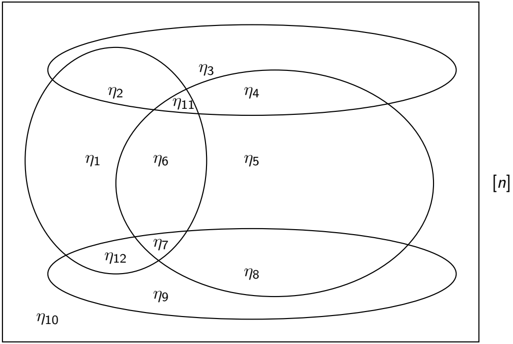


$\exp(L) = \exp(1/\delta^2)$ atoms $\mathcal{A}_1, \mathcal{A}_2, \ldots$

Weak Regularity Decomposition: Dense Graphs

$$|E(S,\overline{S})| \approx \sum_{\ell=1}^{L} c_i \cdot |S_1^i \cap S||S_2^i \cap \overline{S}|$$

Venn diagram of sets S_1^i, S_2^i for $i \in [L]$



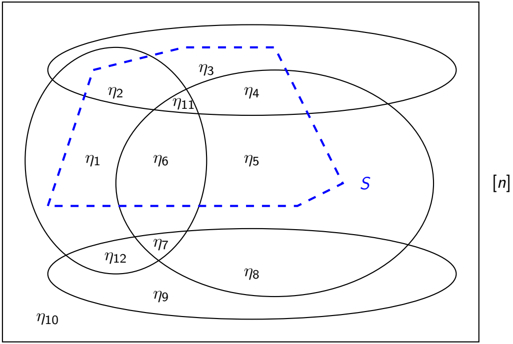
$\exp(L) = \exp(1/\delta^2)$ atoms $\mathcal{A}_1, \mathcal{A}_2, \ldots$

$$\eta_j = \frac{|\mathcal{A}_j \cap S|}{|\mathcal{A}_j|} \text{ for atom } \mathcal{A}_j$$

Weak Regularity Decomposition: Dense Graphs

$$|E(S,\overline{S})| \approx \sum_{\ell=1}^{L} c_i \cdot |S_1^i \cap S||S_2^i \cap \overline{S}|$$

Venn diagram of sets S_1^i, S_2^i for $i \in [L]$



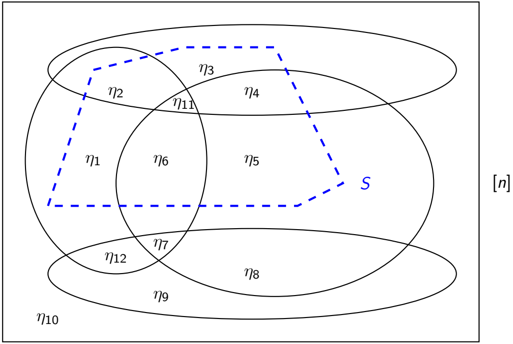
$\exp(L) = \exp(1/\delta^2)$ atoms $\mathcal{A}_1, \mathcal{A}_2, \ldots$

$\eta_j = \frac{|\mathcal{A}_j \cap S|}{|\mathcal{A}_j|}$ for atom $\mathcal{A}_j$

Weak Regularity Decomposition: Dense Graphs

$|E(S, \overline{S})| \approx \sum_{\ell=1}^{L} c_i \cdot |S_1^i \cap S||S_2^i \cap \overline{S}|$

Venn diagram of sets S_1^i, S_2^i for $i \in [L]$



$\exp(L) = \exp(1/\delta^2)$ atoms $\mathcal{A}_1, \mathcal{A}_2, \ldots$

$\eta_j = \frac{|\mathcal{A}_j \cap S|}{|\mathcal{A}_j|}$ for atom $\mathcal{A}_j$

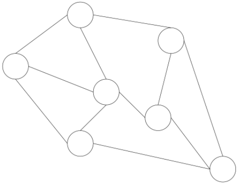
To find best S brute-force over a fine enough discretization of η_j's

Weak Regularity Decomposition: Sparse Graphs

Theorem (Oveis Gharan and Trevisan'13)

Expander graphs admit efficient weak regularity decompositions, so MaxCut can be approximated on them

(their result also holds for low threshold rank graphs)



Weak Regularity Decomposition: Sparse Tensors

Sparse Tensors on Splittable Structures

Let $W \subseteq [n]^k$ and $g\colon W \to [-1,1]$. We want to find $g \approx \sum_{\ell=1}^{L} c_i \cdot 1_{S_1^i} \otimes \cdots \otimes 1_{S_k^i}$ such that

$$\max_{S_1,\ldots,S_k \subseteq [n]} \left| \langle g - \sum_{\ell=1}^{L} c_i \cdot 1_{S_1^i} \otimes \cdots \otimes 1_{S_k^i}, 1_{S_1} \otimes \cdots \otimes 1_{S_k} \rangle \right| \leq \delta \cdot |W|,$$

and $L = O(1/\delta^2)$.

Weak Regularity Decomposition: Sparse Tensors

Sparse Tensors on Splittable Structures

Let $W \subseteq [n]^k$ τ-splittable and $g \colon W \to [-1,1]$. If $\tau \leq \text{poly}(\delta/k)$, there exists $\sum_{\ell=1}^{L} c_i \cdot 1_{S_1^i} \otimes \cdots \otimes 1_{S_k^i}$ such that

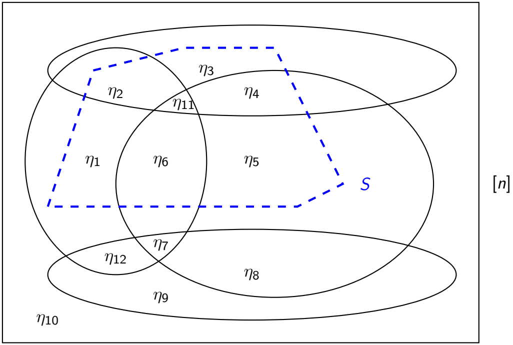
$$\max_{S_1,\ldots,S_k \subseteq [n]} \left| \left\langle g - \sum_{\ell=1}^{L} c_i \cdot 1_{S_1^i} \otimes \cdots \otimes 1_{S_k^i}, 1_{S_1} \otimes \cdots \otimes 1_{S_k} \right\rangle \right| \leq \delta \cdot |W|,$$

and $L = O(1/\delta^2)$.

Weak Regularity Decomposition: Sparse Tensors

Similar strategy works for k-CSPs (and even to list decoding)

Venn diagram of sets $S_1^i, \ldots, S_k^i$ for $i \in [L]$



$\exp(kL) = \exp(k/\delta^2)$ atoms $\mathcal{A}_1, \mathcal{A}_2, \ldots$

$$\eta_j = \frac{|\mathcal{A}_j \cap S|}{|\mathcal{A}_j|} \text{ for atom } \mathcal{A}_j$$

Weak Regularity Decomposition: Sparse Tensors

Existential regularity decomposition for splittable tensors

Showing the existence of $\sum_{\ell=1}^{L} c_i \cdot 1_{S_1^i} \otimes \cdots \otimes 1_{S_k^i} \approx g$ is not too hard

Weak Regularity Decomposition: Sparse Tensors

$\mathrm{CUT}^{\otimes k} = \{\pm 1_{S_1} \otimes \cdots \otimes 1_{S_k} \mid S_1, \ldots, S_k \subseteq [n]\}$
Let μ be a probability measure on W

---

function ExistentialWeakRegularityDecomposition($g \colon W \to [-1, 1]$)
    $h \leftarrow 0$
    while $\exists f \in \mathrm{CUT}^{\otimes k} \colon \langle g - h, f \rangle_\mu \geq \delta$ **do**
        $h \leftarrow h + \delta \cdot f$
    end while
    return h
end function

Weak Regularity Decomposition: Sparse Tensors

function ExistentialWeakRegularityDecomposition($g \colon W \to [-1, 1]$)
  $h \leftarrow 0$
  while $\exists f \in \mathrm{CUT}^{\otimes k} \colon \langle g - h, f \rangle_\mu \geq \delta$ **do**
    $h \leftarrow h + \delta \cdot f$
  end while
  return h
end function

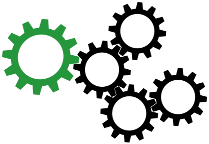
Claim: $\|g - h\|_\mu^2$ decreases by δ^2 at each iteration

$$\begin{aligned} \langle g - h - \delta \cdot f, g - h - \delta \cdot f \rangle_\mu &= \langle g - h, g - h \rangle_\mu - 2\delta \langle g - h, f \rangle_\mu + \delta^2 \langle f, f \rangle_\mu \\ &\leq \langle g - h, g - h \rangle_\mu - \delta^2 \end{aligned}$$

Weak Regularity Decomposition: Sparse Tensors

Near-linear time regularity decomposition for splittable tensors

The more challenging steps are related to algorithmically finding a decomposition $\sum_{\ell=1}^{L} c_i \cdot 1_{S_1^i} \otimes \cdots \otimes 1_{S_k^i} \approx g$ in time $\widetilde{O}_\delta(|W|)$ (and also proving list decoding)

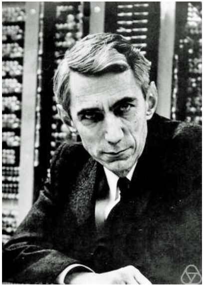


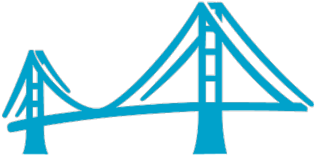
Towards List Decoding Capacity

Major Open Problem in the adversarial (Hamming) model

Find explicit efficient list decodable binary codes from radius $1/2 - \epsilon$ having rate $\Omega(\epsilon^2)$

(pointed by Guruswami and Sudan)





Towards List Decoding Capacity

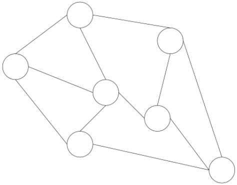
Open Problem: Near List Decoding Capacity

Find explicit efficient list decodable binary codes from radius $1/2 - \epsilon$ having rate $\Omega(\epsilon^{2+o(1)})$

Can any of our approaches help resolve this problem?

Towards List Decoding Capacity

More broadly, where else can these techniques be applied?



That's all.

Thank you!

Questions?