

Unique Decoding of Explicit ϵ -balanced Codes near the Gilbert–Varshamov Bound

Fernando Granha Jeronimo

joint work with

Dylan Quintana, Shashank Srivastava and

Madhur Tulsiani

FOCS 2020

Goal of the Talk

Goal

Present an efficient **unique decoding algorithm** for Ta-Shma's binary codes

Goal of the Talk

Outline

- Notation and Context ($\approx 25\%$)
- Direct Sum and Ta-Shma's Codes ($\approx 25\%$)
- Our Decoding Techniques ($\approx 50\%$)

Coding Theory Concepts

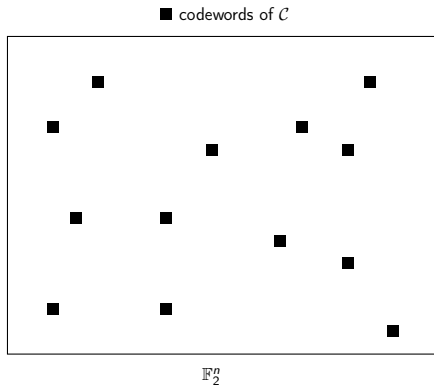
Code

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

Coding Theory Concepts

Code

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



Coding Theory Concepts

Two Fundamental Properties

Distance

The distance $\Delta(\mathcal{C})$ of \mathcal{C} is

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

where $\Delta(z, z')$ is the (normalized) Hamming distance.

Coding Theory Concepts

Two Fundamental Properties

Distance

The distance $\Delta(\mathcal{C})$ of \mathcal{C} is

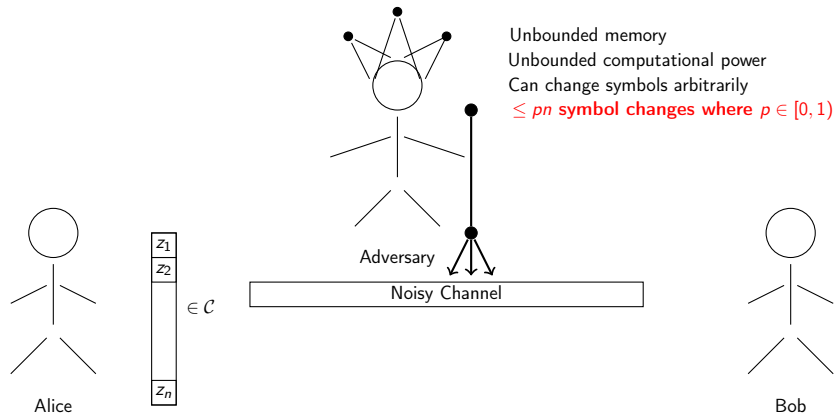
$$\Delta(\mathcal{C}) := \min_{z, z' \in \mathcal{C}: z \neq z'} \Delta(z, z'),$$

where $\Delta(z, z')$ is the (normalized) Hamming distance.

Rate

Fraction of information symbols $\frac{\log_2(|\mathcal{C}|)}{n}$ aka the rate $r(\mathcal{C})$ of \mathcal{C}

Error Model



Error Model

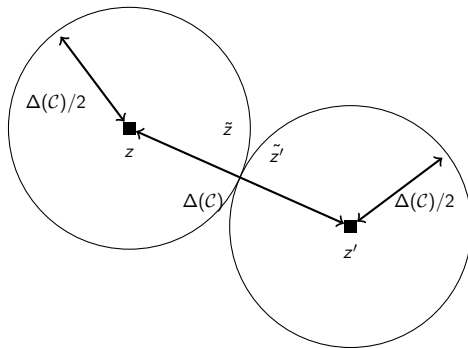
Question

How large can we take $p \in [0, 1)$?

Error Model

Question

How large can we take $p \in [0, 1)$? Information theoretically, any $p \in [0, \Delta(\mathcal{C})/2)$ is valid for unique decoding



Error Model

Error Model

This adversarial error model was introduced by Hamming in 1950



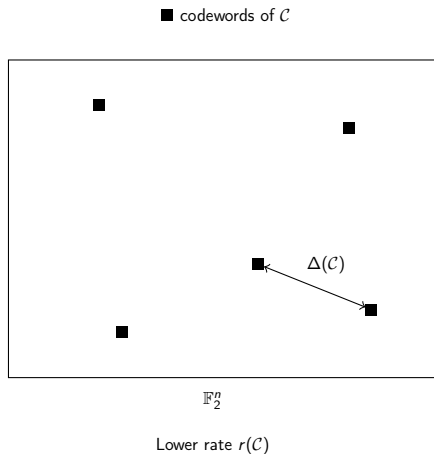
Figure: Richard W. Hamming (source: mathshistory.st-andrews.ac.uk).

Tension between Rate and Distance of a Code

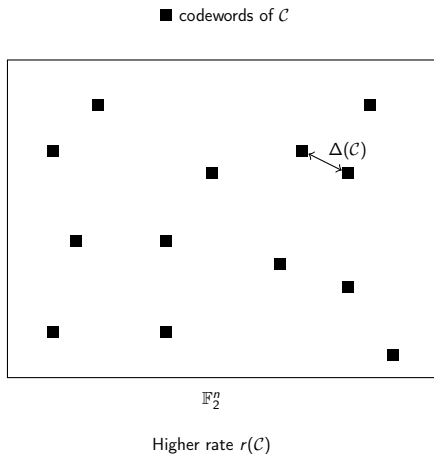
Tension

- Increasing the rate $r(\mathcal{C})$ may reduce the distance $\Delta(\mathcal{C})$
- Increasing the distance $\Delta(\mathcal{C})$ may reduce the rate $r(\mathcal{C})$

Tension between Rate and Distance of a Code

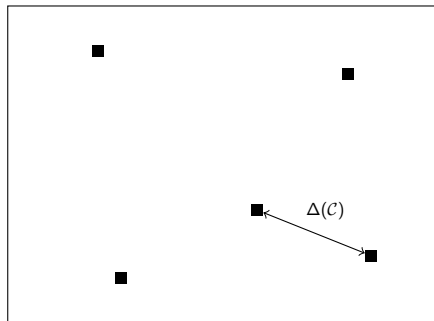


Tension between Rate and Distance of a Code



Tension between Rate and Distance of a Code

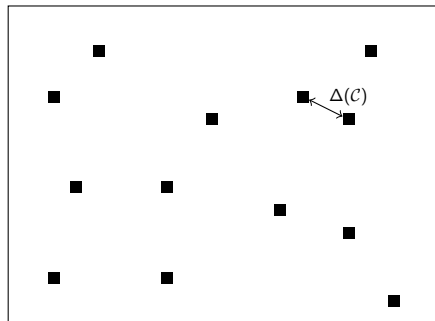
■ codewords of \mathcal{C}



\mathbb{F}_2^n

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

■ codewords of \mathcal{C}



\mathbb{F}_2^n

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

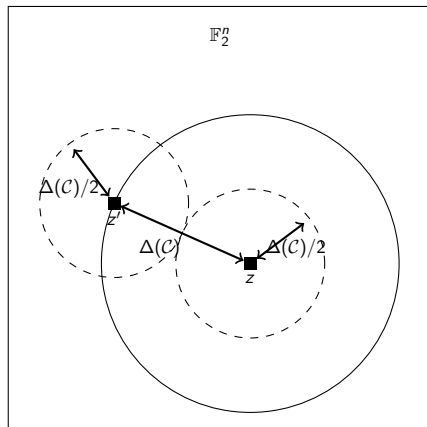
Gilbert'52, Varshamov'57 (abridged)

For every distance $\rho \in (0, 1/2)$, there exists \mathcal{C} of size $2^n/\text{Vol}(\text{Ball}(\rho))$, or equivalently $r(\mathcal{C}) \approx 1 - H_2(\rho)$

Coding Theory Concepts

Gilbert'52, Varshamov'57 (abridged)

For every distance $\rho \in (0, 1/2)$, there exists \mathcal{C} of size $2^n / \text{Vol}(\text{Ball}(\rho))$, or equivalently $r(\mathcal{C}) \approx 1 - H_2(\rho)$



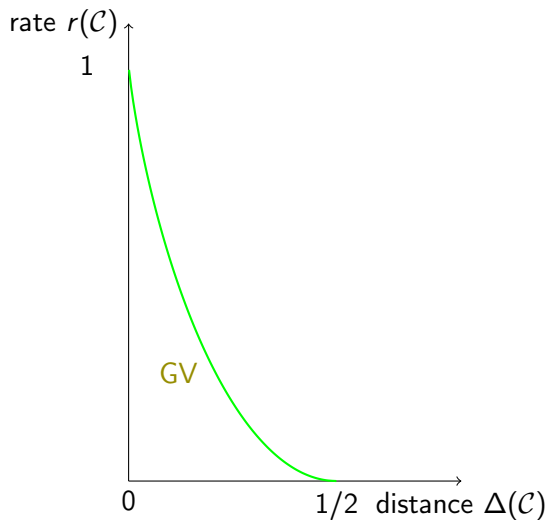
Coding Theory Concepts

Why is the Gilbert–Varshamov bound interesting?

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

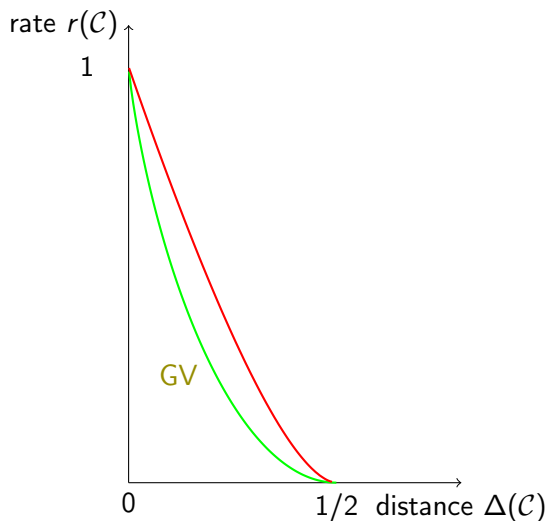
Coding Theory Concepts

Gilbert–Varshamov existential bound

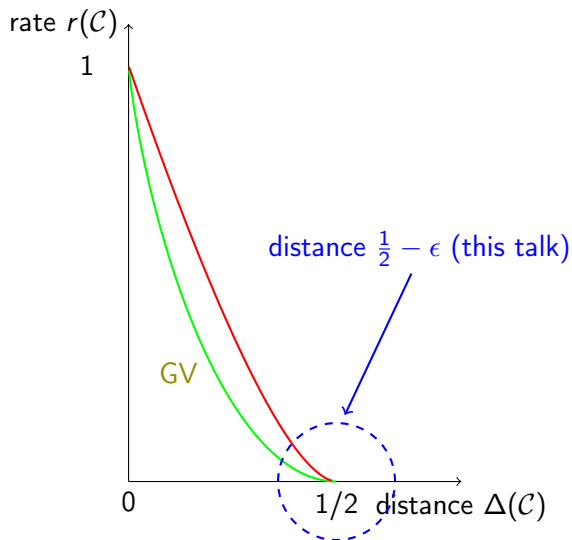


Coding Theory Concepts

McEliece–Rodemich–Rumsey–Welch'77 impossibility bound



Coding Theory Concepts



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.*)

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 are due to Ta-Shma'17

- these codes have 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 are due to Ta-Shma'17

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

Issue

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

Coding Theory Concepts

Issue

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

Theorem (this work)

Ta-Shma's codes are polynomial time unique decodable

Our Contribution

Theorem (Unique Decoding)

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

- ① distance at least $1/2 - \epsilon/2$ (actually ϵ -balanced),
- ② rate $\Omega(\epsilon^{2+\beta})$ where $\beta = O(1/(\log_2(1/\epsilon))^{1/6})$, and
- ③ a unique decoding algorithm with running time $N^{O_{\epsilon,\beta}(1)}$.

Our Contribution

Theorem (Unique Decoding)

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

- ❶ distance at least $1/2 - \epsilon/2$ (actually ϵ -balanced),
- ❷ rate $\Omega(\epsilon^{2+\beta})$ where $\beta = O(1/(\log_2(1/\epsilon))^{1/6})$, and
- ❸ a unique decoding algorithm with running time $N^{O_{\epsilon,\beta}(1)}$.

Furthermore, if instead we take $\beta > 0$ to be an arbitrary constant, the running time becomes $(\log(1/\epsilon))^{O(1)} \cdot N^{O_{\beta}(1)}$ (fixed polynomial time).

Our Contribution

Theorem (Gentle List Decoding)

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

- ① distance at least $1/2 - \epsilon/2$ (actually ϵ -balanced),
- ② rate $\Omega(\epsilon^{2+\beta})$ where $\beta = O(1/(\log_2(1/\epsilon))^{1/6})$, and
- ③ a list decoding algorithm that decodes within radius $1/2 - 2^{-\Theta((\log_2(1/\epsilon))^{1/6})}$ in time $N^{O_{\epsilon,\beta}(1)}$.

Related Work

All based on code **concatenation** starting from larger alphabet codes

Theorem (Guruswami–Indyk'04)

*Efficiently decodable **non-explicit** binary codes at the Gilbert–Varshamov bound*

Related Work

All based on code **concatenation** starting from larger alphabet codes

Theorem (Guruswami–Indyk'04)

*Efficiently decodable **non-explicit** binary codes at the Gilbert–Varshamov bound*

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

*Near-linear time decodable **non-explicit** binary codes at the Gilbert–Varshamov bound*

Related Work

All based on code **concatenation** starting from larger alphabet codes

Theorem (Guruswami–Rudra'06)

There are explicit binary codes list decodable from radius $1/2 - \epsilon$ and rate $\Omega(\epsilon^3)$ (Zyablov bound)

Related Work

All based on code **concatenation** starting from larger alphabet codes

Theorem (Guruswami–Rudra'06)

There are explicit binary codes list decodable from radius $1/2 - \epsilon$ and rate $\Omega(\epsilon^3)$ (Zyablov bound)

GR'06 results can now also be obtained from some later capacity achieving codes

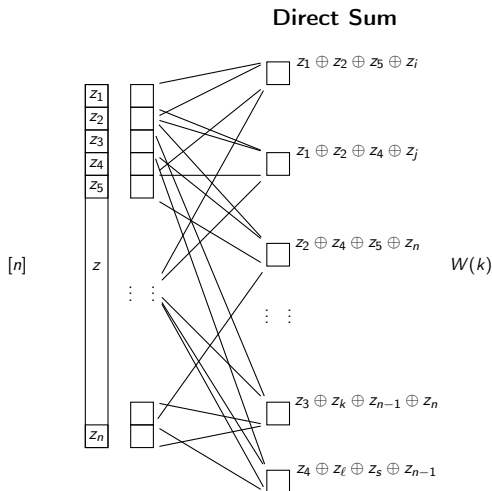
Towards Ta-Shma's Codes

Expander Graphs and Codes

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

Expansion and Distance Amplification

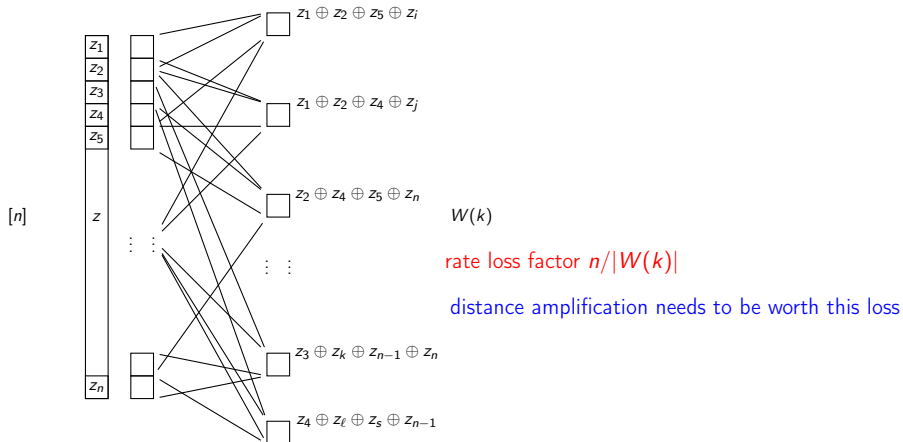
Fix a bipartite graph between $[n]$ and $W(k) \subseteq [n]^k$. Let $z \in \mathcal{C}_0 \subseteq \mathbb{F}_2^n$.



Expansion and Distance Amplification

Fix a bipartite graph between $[n]$ and $W(k) \subseteq [n]^k$. Let $z \in \mathcal{C}_0 \subseteq \mathbb{F}_2^n$.

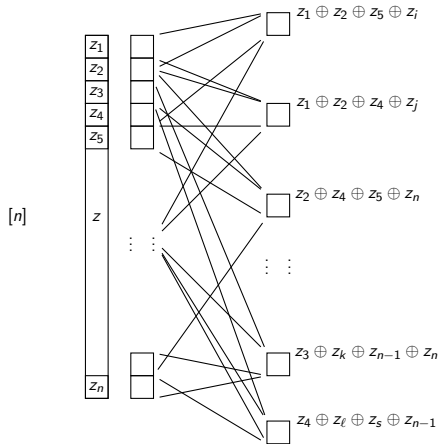
Direct Sum



Expansion and Distance Amplification

Fix a bipartite graph between $[n]$ and $W(k) \subseteq [n]^k$. Let $z \in \mathcal{C}_0 \subseteq \mathbb{F}_2^n$.

Direct Sum



$W(k)$

rate loss factor $n/|W(k)|$

distance amplification needs to be worth this loss

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

Expansion and Distance Amplification

Direct Sum

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

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

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

Expansion and Distance Amplification

Bias

- Let $z \in \mathbb{F}_2^n$. Define $\text{bias}(z) := |\mathbf{E}_{i \in [n]} (-1)^{z_i}|$.
- Let $\mathcal{C} \subseteq \mathbb{F}_2^n$. Define $\text{bias}(\mathcal{C}) := \max_{z \in \mathcal{C} \setminus \{0\}} \text{bias}(z)$.

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

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

Expanders and Distance Amplification

Parity Samplers

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

Expanders and Distance Amplification

A Dream Parity Sampler

Let $z \in \mathbb{F}_2^n$ with $\text{bias}(z) \leq \beta_0 < 1$. Let $W(k) = [n]^k$. Then

$$\text{bias}(\text{dsum}_{W(k)}(z)) \leq |\mathbf{E}_{i \in [n]} (-1)^{z_i}|^k \leq \beta_0^k.$$

Expanders and Distance Amplification

A Dream Parity Sampler

Let $z \in \mathbb{F}_2^n$ with $\text{bias}(z) \leq \beta_0 < 1$. Let $W(k) = [n]^k$. Then

$$\text{bias}(\text{dsum}_{W(k)}(z)) \leq |\mathbf{E}_{i \in [n]} (-1)^{z_i}|^k \leq \beta_0^k.$$

Issue: Vanishing Rate

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

Issue: Non-explicit

Now $W(k)$ has near optimal size but it is non-explicit

Expanders and Distance Amplification

Solution 1 (good but not near optimal)

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

Expanders and Distance Amplification

Solution 1 (good but not near optimal)

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

Solution 1 (good but not near optimal)

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

Expanders and Distance Amplification

Solution 1 (good but not near optimal)

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

(suggested by Rozenman–Wigderson and analyzed by Ta-Shma'17)

Solution 1 (good but not near optimal)

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

Expanders and Distance Amplification

Solution 2 (near optimal) Ta-Shma'17

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

Expanders and Distance Amplification

Solution 2 (near optimal) Ta-Shma'17

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

Solution 2 (near optimal) Ta-Shma'17

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

Expanders and Distance Amplification

Solution 2 (near optimal) Ta-Shma'17

Take $W(k) \subseteq [n]^k$ to be a **carefully chosen** collection of length- $(k - 1)$ walks on a sparse expander graph $G = (V = [n], E)$
(beautiful breakthrough of Ta-Shma'17 based on generalizations of the Zig-Zag product Reingold–Vadhan–Wigderson)

Solution 2 (near optimal) Ta-Shma'17

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

Bird's-eye view of Unique Decoding

Decoding Direct Sum

What does decoding look like for direct sum?

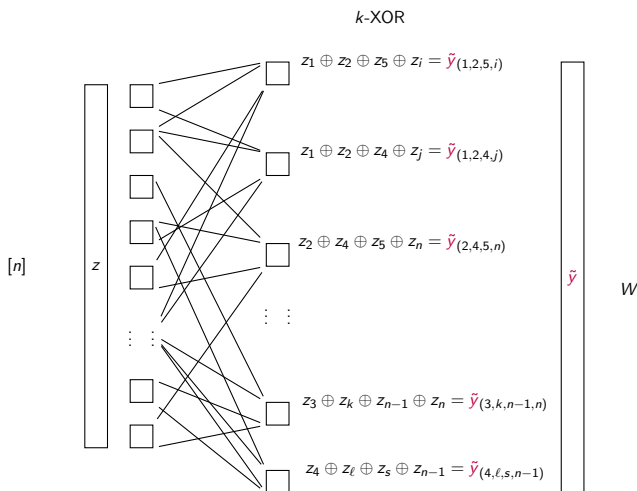
Bird's-eye view of Unique Decoding

Setup

- $\mathcal{C}_0 \subseteq \mathbb{F}_2^n$ an ϵ_0 -balanced code with $\Delta(\mathcal{C}_0) = 1/2 - \epsilon_0/2$
- $W = W(k) \subseteq [n]^k$ for direct sum
- $\mathcal{C} = \text{dsum}_W(\mathcal{C}_0)$ an ϵ -balanced code with $\Delta(\mathcal{C}) = 1/2 - \epsilon/2$

Bird's-eye view of Unique Decoding

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



Bird's-eye view of Unique Decoding

Unique Decoding Scenario: k -XOR

Unique decoding \tilde{y} amounts to solving

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

which is a MAX k -XOR instance \mathfrak{J} with the additional constraint that the solution z must lie in \mathcal{C}_0 .

Bird's-eye view of Unique Decoding

Let $z^* \in \mathcal{C}_0$ be s.t. $y^* = \text{dsum}_W(z^*)$.

Optimal Value

Since \tilde{y} is in the unique decoding ball centered at y^* , we have

$$\mathbb{E}_{(i_1, \dots, i_k) \in W} \mathbf{1}[z^*_{i_1} \oplus \dots \oplus z^*_{i_k} \neq \tilde{y}_{(i_1, \dots, i_k)}] = \Delta(y^*, \tilde{y}) < \Delta(\mathcal{C})/2$$

Thus,

$$\text{OPT}(\mathfrak{J}) \geq \mathbb{E}_{(i_1, \dots, i_k) \in W} \mathbf{1}[z^*_{i_1} \oplus \dots \oplus z^*_{i_k} = \tilde{y}_{(i_1, \dots, i_k)}] > 1 - \Delta(\mathcal{C})/2$$

Bird's-eye view of Unique Decoding

Optimal Solution

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

$$\mathbb{E}_{(i_1, \dots, i_k) \in W} \mathbf{1}[\tilde{z}_{i_1} \oplus \dots \oplus \tilde{z}_{i_k} = \tilde{y}_{(i_1, \dots, i_k)}] = \text{OPT}(\mathfrak{J}) > 1 - \Delta(\mathcal{C})/2$$

Thus, $\Delta(\text{dsum}_W(\tilde{z}), \tilde{y}) < \Delta(\mathcal{C})/2$

Bird's-eye view of Unique Decoding

By triangle inequality,

$$\begin{aligned}\Delta(\text{dsum}_W(\tilde{z}), \text{dsum}_W(z^*)) &\leq \Delta(\text{dsum}_W(\tilde{z}), \tilde{y}) + \\ &\quad \Delta(\tilde{y}, \text{dsum}_W(z^*)) < \Delta(\mathcal{C}) = 1/2 - \epsilon/2,\end{aligned}$$

implying

$$\text{bias}(\text{dsum}_W(\tilde{z}) \oplus \text{dsum}_W(z^*)) = \text{bias}(\text{dsum}_W(\tilde{z} \oplus z^*)) > \epsilon$$

“Nontrivial bias”

Bird's-eye view of Unique Decoding

Claim

If dsum_W is a “strong enough” parity sampler, then either \tilde{z} or $\tilde{z} \oplus 1$ lie in the unique decoding ball of \mathcal{C}_0 centered at z^* .

Bird's-eye view of Unique Decoding

Claim

If dsum_W is a $(1/2 + \epsilon_0/2, \epsilon)$ -parity sampler, then either \tilde{z} or $\tilde{z} \oplus 1$ lie in the unique decoding ball of \mathcal{C}_0 centered at z^* .

Bird's-eye view of Unique Decoding

Moral

- Find 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^*

Bird's-eye view of Unique Decoding

Need to resolve the following assumption.

Optimal Solution

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

$$\mathbb{E}_{(i_1, \dots, i_k) \in \mathcal{W}} \mathbf{1}[\tilde{\mathbf{z}}_{i_1} \oplus \dots \oplus \tilde{\mathbf{z}}_{i_k} = \tilde{\mathbf{y}}_{(i_1, \dots, i_k)}] = \text{OPT}(\mathcal{J})$$

Bird's-eye view of Unique Decoding

Need to resolve the following assumption.

Optimal Solution

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

$$\mathbb{E}_{(i_1, \dots, i_k) \in W} \mathbf{1}[\tilde{z}_{i_1} \oplus \dots \oplus \tilde{z}_{i_k} = \tilde{y}_{(i_1, \dots, i_k)}] = \text{OPT}(\mathfrak{J})$$

Possible issue?

MAX k-XOR is NP-hard, right?

Bird's-eye view of Unique Decoding

Possible issue?

MAX k-XOR is NP-hard, right?

Not an issue

Right, it can be NP-hard in general. However, for some **expanding** instances we can find an **approximate** solution (and that is enough).

Bird's-eye view of Unique Decoding

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

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

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

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

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

(building on Alev–J–Tulsiani'19 which builds on Barak–Raghavendra–Steurer'11)

Bird's-eye view of Unique Decoding

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

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

Bird's-eye view of Unique Decoding

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

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

Definition (Splittability (informal))

A collection $W(k) \subseteq [n]^k$ is said to be σ -splittable, if $k = 1$ (base case) or there exists $k' \in [k - 1]$ such that:

- 1 The matrix $S \in \mathbb{R}^{W[1, k'] \times W[k' + 1, k]}$ defined by $S(w, w') = \mathbb{1}_{ww' \in W}$ has normalized second singular value at most σ (where ww' denotes the concatenated tuple).
- 2 The collections $W[1, k']$ and $W[k' + 1, k]$ are σ -splittable.

Bird's-eye view of Unique Decoding

Lemma (AJQST'20)

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

Bird's-eye view of Unique Decoding

What about the code parameters?

What parameters do we get putting these pieces together?

Bird's-eye view of Unique Decoding

Well... Our parameters in AJQST'20...

With this approach we obtain binary codes with

- distance $1/2 - \epsilon$
- rate $\Theta(2^{-(\log(1/\epsilon))^2}) \ll \text{poly}(\epsilon)$
- polynomial time unique decoding algorithm

Bird's-eye view of Unique Decoding

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

(independently used by Raghavendra–Yau & Karmalkar–Klivans–Kothari to ML)

Bird's-eye view of Unique Decoding

Well... Again our parameters in AJQST'20...

With this entropic approach we obtain binary codes with

- list decoding radius $1/2 - \epsilon$
- rate $\Theta(2^{-(\log(1/\epsilon))^2}) \ll \text{poly}(\epsilon)$
- polynomial time list decoding algorithm

Bird's-eye view of Unique Decoding

On one side

There is this refined near optimal code construction of Ta-Shma

On the other side

There is this far from optimal parameter hungry decoding machinery

Bird's-eye view of Unique Decoding

What are the techniques?

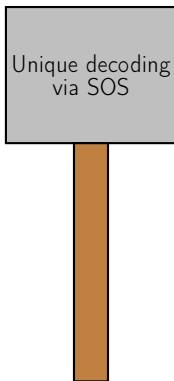
We will just mention the techniques at a very high-level

Bird's-eye view of Unique Decoding

Splittability

First, we modify Ta-Shma's direct sum construction $W(k)$ to make it *splittable* so that our decoding tools can be used

Techniques



Techniques

A few extra words about SOS

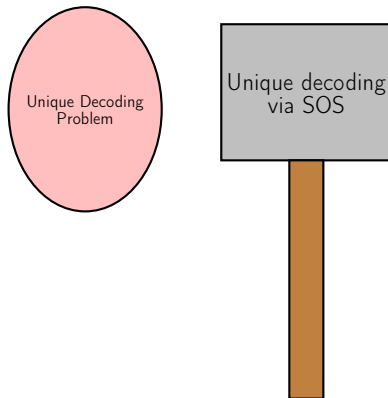
Sum-of-Squares (SOS)

Sum-of-Squares is a semi-definite programming hierarchy

- It generalizes linear programming
- It captures the state-of-the-art approximation guarantees for many problems (MAX-CUT and other CSPs)
- Roughly speaking, level d of SOS runs in time $n^{O(d)}$ where n is the number of variables



Techniques



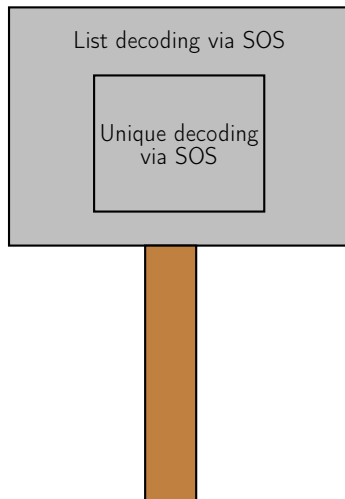
Techniques

First Hammer Effect

As in AJQST'20, we can only decode explicit binary 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)

Bird's-eye view of Unique Decoding



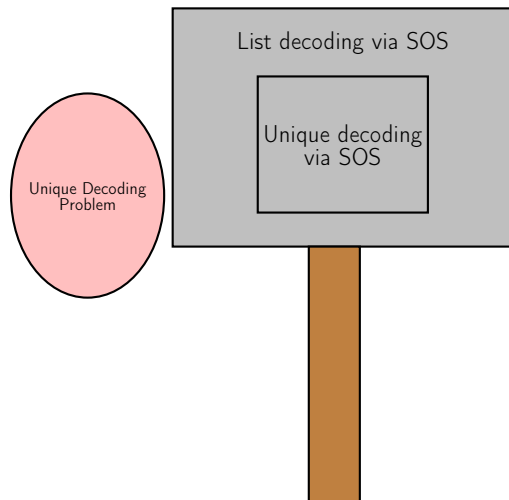
Bird's-eye view of Unique Decoding

Killing a Fly With a Bazooka

Use list decoding to perform unique decoding!

Also considered in some previous work (e.g. Guruswami–Indyk'04).

Bird's-eye view of Unique Decoding

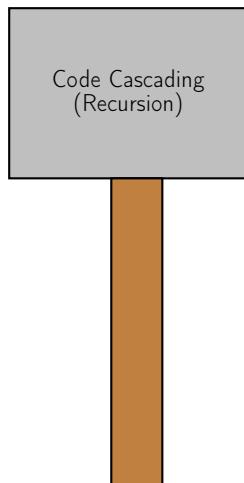


Bird's-eye view of Unique Decoding

Second Hammer Effect

Some parameters are better but $r(\mathcal{C})$ still not even polynomial

Bird's-eye view of Unique Decoding



Bird's-eye view of Unique Decoding

Ta-Shma's walks admit a recursive structure. In short,

- walks over walks are larger walks,
- walks over larger walks are even larger walks,
- walks over even larger walks are...
- and so on...

Bird's-eye view of Unique Decoding

Taking advantage of this recursive structure we can define a sequence of codes. Decoding takes places between consecutive levels and requires much weaker parameters now.

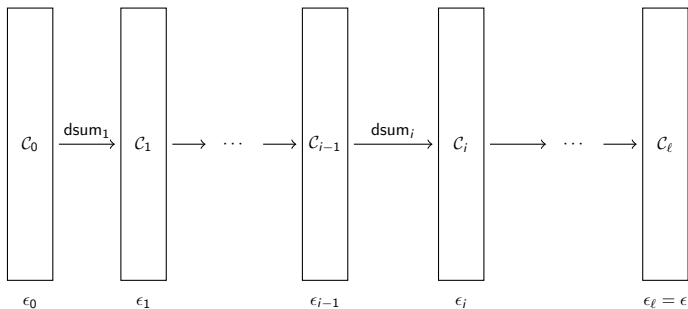


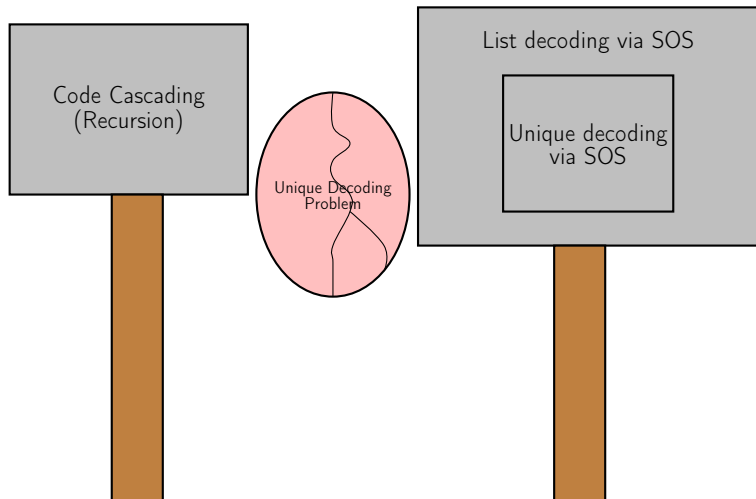
Figure: Code cascading: recursive construction of codes.

Bird's-eye view of Unique Decoding

Remark

Some form of cascading was present in the work of Guruswami–Indyk'01 to the so-called *direct product*. The details here and in their setting are quite different.

Bird's-eye view of Unique Decoding



Bird's-eye view of Unique Decoding

Second and Third Hammers Effect

Decode Ta-Shma's codes with nearly optimal rate

That's all.

Thank you!