Explicit Folded Reed–Solomon and Multiplicity Codes Achieve Near-Optimal List Decodability

Zihan Zhang

Department of Computer Science and Engineering
The Ohio State University

Talk at Peking University (Online)
March 18th, 2024

Joint Work With Yeyuan Chen at University of Michigan

Talk Overview

- Motivations of Error-Correcting Codes

Talk Overview

- Motivations of Error-Correcting Codes
- Basic Backgrounds on List Decoding

Talk Overview

- Motivations of Error-Correcting Codes
- Basic Backgrounds on List Decoding
- Central Topic in List Decoding: An Open Problem of Guruswami and Rudra (STOC'06)

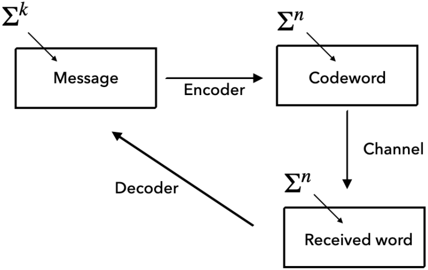
Talk Overview

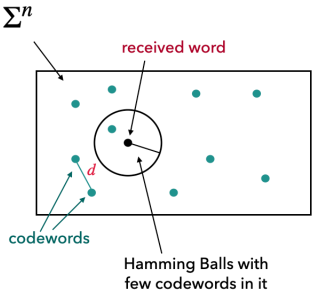
- Motivations of Error-Correcting Codes
- Basic Backgrounds on List Decoding
- Central Topic in List Decoding: An Open Problem of Guruswami and Rudra (STOC'06)
- Our Result and Proof Overview

Talk Overview

- Motivations of Error-Correcting Codes
- Basic Backgrounds on List Decoding
- Central Topic in List Decoding: An Open Problem of Guruswami and Rudra (STOC'06)
- Our Result and Proof Overview
- Future Directions

Motivations of Error-Correcting Codes





Definition (Linear codes)

A $[n, k]$ linear code $C \subset \mathbb{F}_q^n$ is a k-dimensional linear subspace of $\mathbb{F}_q^n$.

Linear Codes: Background

Definition (Linear codes)

A $[n, k]$ linear code $C \subset \mathbb{F}_q^n$ is a k-dimensional linear subspace of $\mathbb{F}_q^n$.

- Code rate $R := k/n$.

Linear Codes: Background

Definition (Linear codes)

A $[n, k]$ linear code $C \subset \mathbb{F}_q^n$ is a k-dimensional linear subspace of $\mathbb{F}_q^n$.

- Code rate $R := k/n$.
- Alphabet is the finite field $\mathbb{F}_q$.

Linear Codes: Background

Definition (Linear codes)

A $[n, k]$ linear code $C \subset \mathbb{F}_q^n$ is a k-dimensional linear subspace of $\mathbb{F}_q^n$.

- Code rate $R := k/n$.
- Alphabet is the finite field $\mathbb{F}_q$.
- Hamming distance $d(x, y) := |\{i : x[i] \neq y[i]\}| \in [n]$, where $[n] := \{1, 2, \ldots, n\}$.

Linear Codes: Background

Definition (Linear codes)

A $[n, k]$ linear code $C \subset \mathbb{F}_q^n$ is a k-dimensional linear subspace of $\mathbb{F}_q^n$.

- Code rate $R := k/n$.
- Alphabet is the finite field $\mathbb{F}_q$.
- Hamming distance $d(x, y) := |\{i : x[i] \neq y[i]\}| \in [n]$, where $[n] := \{1, 2, \dots, n\}$.
- Code distance is defined to be

$$d(C) := \min_{x \neq y \in C} d(x, y),$$

where $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N}$ is the Hamming distance.

Sublinear Codes: Background

Definition (Sublinear codes (informal))

A $[n, k]$ $\mathbb{F}_q$-sublinear code $C \subset (\mathbb{F}_q^s)^n$ is a k-dimensional $\mathbb{F}_q$-linear subspace of $(\mathbb{F}_q^s)^n$.

Sublinear Codes: Background

Definition (Sublinear codes (informal))

A $[n, k]$ $\mathbb{F}_q$-sublinear code $C \subset (\mathbb{F}_q^s)^n$ is a k-dimensional $\mathbb{F}_q$-linear subspace of $(\mathbb{F}_q^s)^n$.

- Code rate $R := k/sn$.

Sublinear Codes: Background

Definition (Sublinear codes (informal))

A $[n, k]$ $\mathbb{F}_q$-sublinear code $C \subset (\mathbb{F}_q^s)^n$ is a k-dimensional $\mathbb{F}_q$-linear subspace of $(\mathbb{F}_q^s)^n$.

- Code rate $R := k/sn$.
- Alphabet is the vector space $\mathbb{F}_q^s$.

Sublinear Codes: Background

Definition (Sublinear codes (informal))

A $[n, k]$ $\mathbb{F}_q$-sublinear code $C \subset (\mathbb{F}_q^s)^n$ is a k-dimensional $\mathbb{F}_q$-linear subspace of $(\mathbb{F}_q^s)^n$.

- Code rate $R := k/sn$.
- Alphabet is the vector space $\mathbb{F}_q^s$.
- Hamming distance $d(x, y) := |\{i : x[i] \neq y[i]\}| \in [n]$, where $[n] := \{1, 2, \ldots, n\}$.

Sublinear Codes: Background

Definition (Sublinear codes (informal))

A $[n, k]$ $\mathbb{F}_q$-sublinear code $C \subset (\mathbb{F}_q^s)^n$ is a k-dimensional $\mathbb{F}_q$-linear subspace of $(\mathbb{F}_q^s)^n$.

- Code rate $R := k/sn$.
- Alphabet is the vector space $\mathbb{F}_q^s$.
- Hamming distance $d(x, y) := |\{i : x[i] \neq y[i]\}| \in [n]$, where $[n] := \{1, 2, \ldots, n\}$.
- Code distance is defined to be

$$d(C) := \min_{x \neq y \in C} d(x, y),$$

where $d : (\mathbb{F}_q^s)^n \times (\mathbb{F}_q^s)^n \to \mathbb{N}$ is the Hamming distance.

- In the following content, the alphabet Σ can either be $\mathbb{F}_q$ or $\mathbb{F}_q^s$

Unique Decoding: Backgrounds

- In the following content, the alphabet Σ can either be $\mathbb{F}_q$ or $\mathbb{F}_q^s$
- For $r \in [n]$ and $y \in \Sigma^n$, Hamming ball of radius r and center y

$$B_r(y) = \{x \in \Sigma^n : d(x, y) \leq r\}.$$

Unique Decoding: Backgrounds

- In the following content, the alphabet Σ can either be $\mathbb{F}_q$ or $\mathbb{F}_q^s$

- For $r \in [n]$ and $y \in \Sigma^n$, Hamming ball of radius r and center y

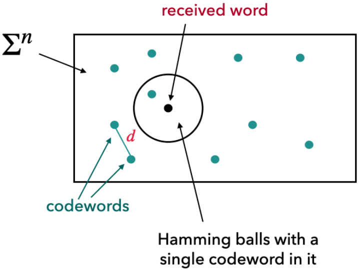
$$B_r(y) = \{x \in \Sigma^n : d(x, y) \leq r\}.$$

- $d(x, z) \leq d(x, y) + d(y, z) \longrightarrow$ for any $y \in \Sigma^n$, we have

$$\left| B_{\left\lfloor \frac{d(C)-1}{2} \right\rfloor}(y) \cap C \right| \leq 1.$$

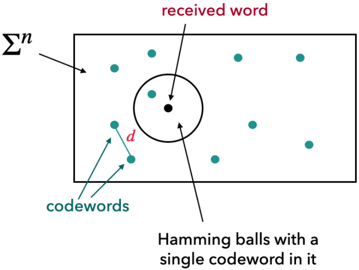
Unique Decoding: Backgrounds

Unique decoding: transmitted codeword $x \in C$ and received word $y \in \Sigma^n$, if $d(x,y) \le \left\lfloor \frac{\mathrm{d}(C)-1}{2} \right\rfloor$, then $x = B_{\left\lfloor \frac{d(C)-1}{2} \right\rfloor}(y) \cap C$



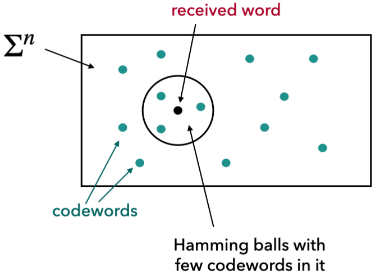
Unique Decoding: Backgrounds

Unique decoding: transmitted codeword $x \in C$ and received word $y \in \Sigma^n$, if $d(x, y) \le \left\lfloor \frac{\mathrm{d}(C)-1}{2} \right\rfloor$, then $x = B_{\left\lfloor \frac{d(C)-1}{2} \right\rfloor}(y) \cap C$



Question: More than $\left\lfloor \frac{\mathrm{d}(C)-1}{2} \right\rfloor$?

List decoding (introduced by Elias 1957, Wozencraft 1958): Given transmitted codeword $c \in C$ and received word $y \in \Sigma^n$, if $d(c, y) \leq \rho n$, then find an efficient algorithm to list all the $c \in B_{\rho n}(y) \cap C$, where $|B_{\rho n}(y) \cap C| = L$.



The power of List Decoding in Theoretical Computer Science: Few Examples

The power of List Decoding in Theoretical Computer Science: Few Examples

- The notion of local list decoding can be used to conditionally prove $\mathsf{P} = \mathsf{BPP}$ (Sudan–Trevisan–Vadhan STOC'99).

The power of List Decoding in Theoretical Computer Science: Few Examples

- The notion of local list decoding can be used to conditionally prove $\mathsf{P} = \mathsf{BPP}$ (Sudan–Trevisan–Vadhan STOC'99).
- Good list recoverable codes (e.g. folded RS codes, multiplicity codes) — a generalization of list decodable codes — can give explicit construction of "good" condensers and extractors (Guruswami–Umans–Vadhan JACM'09).

The power of List Decoding in Theoretical Computer Science: Few Examples

- The notion of local list decoding can be used to conditionally prove $\mathsf{P} = \mathsf{BPP}$ (Sudan–Trevisan–Vadhan STOC'99).
- Good list recoverable codes (e.g. folded RS codes, multiplicity codes) — a generalization of list decodable codes — can give explicit construction of "good" condensers and extractors (Guruswami–Umans–Vadhan JACM'09). Those constructions are the fundamental building blocks in the theory of pseudorandomness.

The power of List Decoding in Theoretical Computer Science: Few Examples

- The notion of local list decoding can be used to conditionally prove $\mathsf{P} = \mathsf{BPP}$ (Sudan–Trevisan–Vadhan STOC'99).
- Good list recoverable codes (e.g. folded RS codes, multiplicity codes) — a generalization of list decodable codes — can give explicit construction of "good" condensers and extractors (Guruswami–Umans–Vadhan JACM'09). Those constructions are the fundamental building blocks in the theory of pseudorandomness.
- Some current cryptographic protocols based on IOPPs (e.g. protocol STIR in CRYPTO'24) used the list decodability of Reed–Solomon and related codes, which are fundamental in the theory of zero-knowledge proofs.

List Decodability

Definition (Combinatorial list decodability)

For $\rho \in [0,1]$ and $L \geq 1$, a code $C \subseteq \Sigma^n$ is (ρ, L) list decodable if for all $y \in \Sigma^n$ and $L+1$ distinct codewords $c_0, c_1, \ldots, c_L \in C$, we have $\max_{0 \leq i \leq L} d(y, c_i) > \rho n$.

List Decodability

Definition (Combinatorial list decodability)

For $\rho \in [0,1]$ and $L \geq 1$, a code $C \subseteq \Sigma^n$ is (ρ, L) list decodable if for all $y \in \Sigma^n$ and $L+1$ distinct codewords $c_0, c_1, \ldots, c_L \in C$, we have $\max_{0 \leq i \leq L} d(y, c_i) > \rho n$.

Definition (Average-radius (combinatorial) list decodability)

A code $C \subset \Sigma^n$ is (ρ, L) average-radius list decodable if for every $y \in \Sigma^n$ and every $L+1$ distinct codewords $c_0, c_1, \ldots, c_L \in C$, we have $\frac{1}{L+1} \sum_{i=0}^{L} d(y, c_i) > \rho n$.

List Decodability

Definition (Combinatorial list decodability)

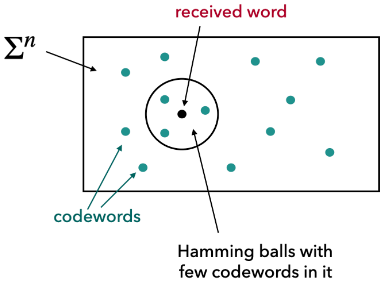
For $\rho \in [0,1]$ and $L \geq 1$, a code $C \subseteq \Sigma^n$ is (ρ, L) list decodable if for all $y \in \Sigma^n$ and $L+1$ distinct codewords $c_0, c_1, \ldots, c_L \in C$, we have $\max_{0 \leq i \leq L} d(y, c_i) > \rho n$.

Definition (Average-radius (combinatorial) list decodability)

A code $C \subset \Sigma^n$ is (ρ, L) average-radius list decodable if for every $y \in \Sigma^n$ and every $L+1$ distinct codewords $c_0, c_1, \ldots, c_L \in C$, we have $\frac{1}{L+1} \sum_{i=0}^{L} d(y, c_i) > \rho n$.

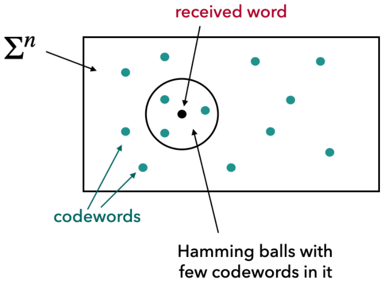
Remark (Algorithmic list decoding)

Given $y \in \Sigma^n$ s. t. $|B_{\rho n}(y) \cap C| \leq L$, find an efficient algorithm to list all the codewords $c \in B_{\rho n}(y) \cap C$.

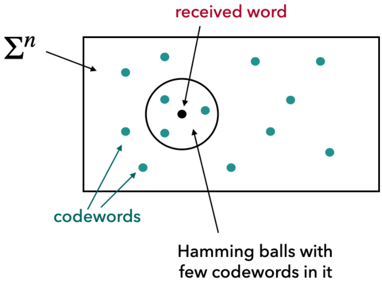


- large code rate R, large decoding radius ρ and list size small L

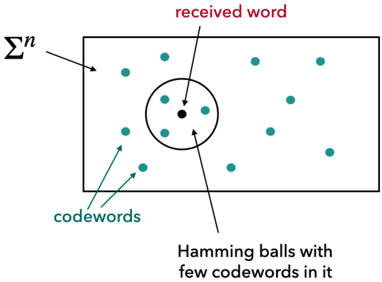
Combinatorics in List Decoding



- large code rate R, large decoding radius ρ and list size small L
- Fix R, larger $\rho \iff$ larger L

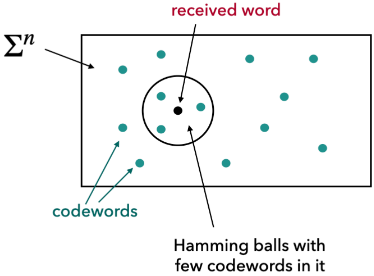


- large code rate R, large decoding radius ρ and list size small L
- Fix R, larger $\rho \Longleftrightarrow$ larger L
- Fix ρ, larger $R \Longleftrightarrow$ larger L



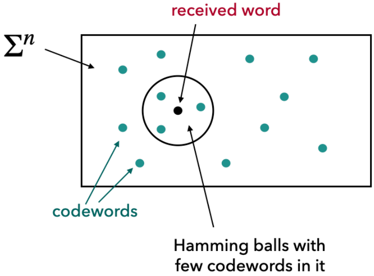
- large code rate R, large decoding radius ρ and list size small L
- Fix R, larger $\rho \iff$ larger L
- Fix ρ, larger $R \iff$ larger L
- Fix L, larger $R \iff$ smaller ρ

Sphere Packing: Given a code (subset or subspace of $\mathbb{F}_q^n$), we want to determine the best trade-off between the relative (Hamming) radius $\rho := d/n$, the rate $R = k/n$, and the list size L.



Core Challenge in List Decoding

Sphere Packing: Given a code (subset or subspace of $\mathbb{F}_q^n$), we want to determine the best trade-off between the relative (Hamming) radius $\rho := d/n$, the rate $R = k/n$, and the list size L.



Core Challenge: Design such codes with efficient encoding and decoding algorithms!

More About Linear Codes: Reed–Solomon Codes

For list decoding, what we care the most is a classical family of linear codes called Reed–Solomon (RS) codes.

More About Linear Codes: Reed–Solomon Codes

For list decoding, what we care the most is a classical family of linear codes called Reed–Solomon (RS) codes.

Definition (RS codes)

Given n distinct points $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$, the corresponding $[n, k]$ RS code is

$$\mathrm{RS}_{n,k}(\alpha_1, \ldots, \alpha_n) := \left\{ (f(\alpha_1), \ldots, f(\alpha_n)) \;\middle|\; \begin{array}{c} f \in \mathbb{F}_q[x], \\ \deg f < k \end{array} \right\} \subseteq \mathbb{F}_q^n.$$

For list decoding, what we care the most is a classical family of linear codes called Reed–Solomon (RS) codes.

Definition (RS codes)

Given n distinct points $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$, the corresponding $[n, k]$ RS code is

$$\mathrm{RS}_{n,k}(\alpha_1, \ldots, \alpha_n) := \left\{ (f(\alpha_1), \ldots, f(\alpha_n)) \;\middle|\; \begin{array}{c} f \in \mathbb{F}_q[x], \\ \deg f < k \end{array} \right\} \subseteq \mathbb{F}_q^n.$$

Remark: $d(\mathrm{RS}_{n,k}(\alpha_1, \ldots, \alpha_n)) = n - k + 1.$

More About Linear Codes: Reed–Solomon Codes

For list decoding, what we care the most is a classical family of linear codes called Reed–Solomon (RS) codes.

Definition (RS codes)

Given n distinct points $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$, the corresponding $[n, k]$ RS code is

$$\mathrm{RS}_{n,k}(\alpha_1, \ldots, \alpha_n) := \left\{ (f(\alpha_1), \ldots, f(\alpha_n)) \;\middle|\; \begin{array}{l} f \in \mathbb{F}_q[x], \\ \deg f < k \end{array} \right\} \subseteq \mathbb{F}_q^n.$$

Remark: $d(\mathrm{RS}_{n,k}(\alpha_1, \ldots, \alpha_n)) = n - k + 1$. (best trade-off)

More About Linear Codes: Reed–Solomon Codes

For list decoding, what we care the most is a classical family of linear codes called Reed–Solomon (RS) codes.

Definition (RS codes)

Given n distinct points $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$, the corresponding $[n, k]$ RS code is

$$\mathrm{RS}_{n,k}(\alpha_1, \ldots, \alpha_n) := \left\{ (f(\alpha_1), \ldots, f(\alpha_n)) \;\middle|\; \begin{array}{l} f \in \mathbb{F}_q[x], \\ \deg f < k \end{array} \right\} \subseteq \mathbb{F}_q^n.$$

Remark: $d(\mathrm{RS}_{n,k}(\alpha_1, \ldots, \alpha_n)) = n - k + 1$. (best trade-off)

Proposition (Singleton bound)

For any $[n, k]$ linear code $C \subset \mathbb{F}_q^n$ we have $d(C) \leq n - k + 1$.

Reed–Solomon Code Codeword: An Example

Let $(m_1, m_2, m_3) \in \mathbb{F}_q^3$ be a message of length 3. Then the encoder of $\mathsf{RS}_{4,3}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ is below

$$(m_1, m_2, m_3) \xrightarrow{\text{encoder}} (f(\alpha_1), f(\alpha_2), f(\alpha_3), f(\alpha_4))$$

where $f(X) = m_1 + m_2 X + m_3 X^2$.

A First Bound for List Decodability

- Johnson Bound: Any code C with large distance $d(C) \xrightarrow{implies}$ (relatively) good list decodability: $\left(1 - \sqrt{1 - \frac{d(C)}{n}}, qnd(C)\right)$

A First Bound for List Decodability

- Johnson Bound: Any code C with large distance $d(C) \xrightarrow{\textit{implies}}$ (relatively) good list decodability: $\left(1 - \sqrt{1 - \frac{d(C)}{n}}, qnd(C)\right)$
- Guruswami and Sudan (FOCS'98) provide the first list decoding algorithm of Reed–Solomon codes up to the Johnson bound.

A First Bound for List Decodability

- Johnson Bound: Any code C with large distance $d(C) \xrightarrow{implies}$ (relatively) good list decodability: $\left(1 - \sqrt{1 - \frac{d(C)}{n}}, qnd(C)\right)$
- Guruswami and Sudan (FOCS'98) provide the first list decoding algorithm of Reed–Solomon codes up to the Johnson bound.

Theorem (Sudan'97 and Guruswami–Sudan'98)

Given n distinct points $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$, the corresponding $[n, k]$ Reed–Solomon code $\mathrm{RS}_{n,k}(\alpha_1, \ldots, \alpha_n)$ can always be list decoded up to the radius $n - \sqrt{nk}$ with list size at most qn^2 in $\mathrm{poly}(n)$ time.

A First Bound for List Decodability

- Johnson Bound: Any code C with large distance $d(C) \xrightarrow{\textit{implies}}$ (relatively) good list decodability: $\left(1-\sqrt{1-\frac{d(C)}{n}}, qnd(C)\right)$
- Guruswami and Sudan (FOCS'98) provide the first list decoding algorithm of Reed–Solomon codes up to the Johnson bound.

Theorem (Sudan'97 and Guruswami–Sudan'98)

Given n distinct points $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$, the corresponding $[n, k]$ Reed–Solomon code $\mathrm{RS}_{n,k}(\alpha_1, \ldots, \alpha_n)$ can always be list decoded up to the radius $n - \sqrt{nk}$ with list size at most qn^2 in $\mathrm{poly}(n)$ time.

Question: Can we design explicit codes with efficient list decoding algorithms beyond the Johnson bound?

List Decoding Capacity

Theorem (List decoding capacity theorem)

- *A random code is, with high probability,* $(1 - R - \varepsilon, L)$ *list decodable for* $L = O(1/\varepsilon)$.
- *If a code of rate* R *and length* n *is* $(1 - R + \varepsilon, L)$ *list decodable code, then* $L \geq 2^{\Omega_\varepsilon(n)}$.

List Decoding Capacity

Theorem (List decoding capacity theorem)

- *A random code is, with high probability,* $(1 - R - \varepsilon, L)$ *list decodable for* $L = O(1/\varepsilon)$*.*
- *If a code of rate* R *and length* n *is* $(1 - R + \varepsilon, L)$ *list decodable code, then* $L \geq 2^{\Omega_\varepsilon(n)}$*.*

Definition (Capacity-achieving codes (informal))

A code of rate R is said to achieve list decoding capacity, if it is $(1 - R - \varepsilon, L)$ list decodable with small list size $L \leq O_\varepsilon(1)$ or even (weaker) $L \leq n^{O_\varepsilon(1)}$.

List Decoding Capacity

Theorem (List decoding capacity theorem)

- *A random code is, with high probability,* $(1 - R - \varepsilon, L)$ *list decodable for* $L = O(1/\varepsilon)$.
- *If a code of rate* R *and length* n *is* $(1 - R + \varepsilon, L)$ *list decodable code, then* $L \geq 2^{\Omega_\varepsilon(n)}$.

Definition (Capacity-achieving codes (informal))

A code of rate R is said to achieve list decoding capacity, if it is $(1 - R - \varepsilon, L)$ list decodable with small list size $L \leq O_\varepsilon(1)$ or even (weaker) $L \leq n^{O_\varepsilon(1)}$.

Question: Can we design explicit codes with efficient list decoding algorithms up to the list decoding capacity?

From now on, we will focus on two variants of RS codes, both of which are sublinear codes.

More About Subinear Codes: Folded RS Codes

From now on, we will focus on two variants of RS codes, both of which are sublinear codes. The first one is called folded RS codes, introduced by Guruswami–Rudra (STOC'06).

More About Subinear Codes: Folded RS Codes

From now on, we will focus on two variants of RS codes, both of which are sublinear codes. The first one is called folded RS codes, introduced by Guruswami–Rudra (STOC'06).

Definition (Folded RS codes)

A folded RS code $\mathsf{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ over $\mathbb{F}_q^s$ is defined as

$$\left\{ \begin{pmatrix} f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_n) \\ f(\gamma\alpha_1) & f(\gamma\alpha_2) & \cdots & f(\gamma\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ f(\gamma^{s-1}\alpha_1) & f(\gamma^{s-1}\alpha_2) & \cdots & f(\gamma^{s-1}\alpha_n) \end{pmatrix} : \substack{f(X)\in\mathbb{F}_q[X] \\ \deg(f)<k} \right\} \subseteq (\mathbb{F}_q^s)^n$$

where γ is a generator of the multiplicative group of $\mathbb{F}_q$.

From now on, we will focus on two variants of RS codes, both of which are sublinear codes. The first one is called folded RS codes, introduced by Guruswami–Rudra (STOC'06).

Definition (Folded RS codes)

A folded RS code $\mathsf{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ over $\mathbb{F}_q^s$ is defined as

$$\left\{ \begin{pmatrix} f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_n) \\ f(\gamma\alpha_1) & f(\gamma\alpha_2) & \cdots & f(\gamma\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ f(\gamma^{s-1}\alpha_1) & f(\gamma^{s-1}\alpha_2) & \cdots & f(\gamma^{s-1}\alpha_n) \end{pmatrix} : {\scriptstyle f(X)\in\mathbb{F}_q[X] \atop \deg(f)<k} \right\} \subseteq (\mathbb{F}_q^s)^n$$

where γ is a generator of the multiplicative group of $\mathbb{F}_q$. We assume the sn evaluation points $\gamma^i\alpha_j$ are distinct.

From now on, we will focus on two variants of RS codes, both of which are sublinear codes. The first one is called folded RS codes, introduced by Guruswami–Rudra (STOC'06).

Definition (Folded RS codes)

A folded RS code $\mathrm{FRS}_{n,k,q,s}(\alpha_1,\ldots,\alpha_n)$ over $\mathbb{F}_q^s$ is defined as

$$\left\{\begin{pmatrix} f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_n) \\ f(\gamma\alpha_1) & f(\gamma\alpha_2) & \cdots & f(\gamma\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ f(\gamma^{s-1}\alpha_1) & f(\gamma^{s-1}\alpha_2) & \cdots & f(\gamma^{s-1}\alpha_n) \end{pmatrix} : \substack{f(X)\in\mathbb{F}_q[X] \\ \deg(f)<k} \right\} \subseteq (\mathbb{F}_q^s)^n$$

where γ is a generator of the multiplicative group of $\mathbb{F}_q$. We assume the sn evaluation points $\gamma^i\alpha_j$ are distinct.

Remark: $d(\mathrm{FRS}_{n,k,q,s}(\alpha_1,\ldots,\alpha_n)) = sn - k + 1$.

The other one we considered is multiplicity codes, popularized by Kopparty–Saraf–Yekhanin (STOC'11).

The other one we considered is multiplicity codes, popularized by Kopparty–Saraf–Yekhanin (STOC'11). Before the formal definition, we may introduce a notation called Hasse derivative.

More About Subinear Codes: Multiplicity Codes

The other one we considered is multiplicity codes, popularized by Kopparty–Saraf–Yekhanin (STOC'11). Before the formal definition, we may introduce a notation called Hasse derivative.

Definition (Hasse derivative)

Given a finite field $\mathbb{F}_q, j \in \mathbb{N}$, and a polynomial $f(X)$, the j-th Hasse derivative $f^{(j)}(X)$ is defined as the coefficient of Z^j in the expansion

$$f(X+Z) = \sum_{i \in \mathbb{N}} f^{(j)}(X) Z^j.$$

More About Subinear Codes: Multiplicity Codes

Definition (Multiplicity codes)

An order-s multiplicity code $\mathrm{MULT}^{s}_{n,k,q}(\alpha_1,\ldots,\alpha_n)$ over $\mathbb{F}_q^s$ is defined as

$$\left\{ \begin{pmatrix} f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_n) \\ f^{(1)}(\alpha_1) & f^{(1)}(\alpha_2) & \cdots & f^{(1)}(\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ f^{(s-1)}(\alpha_1) & f^{(s-1)}(\alpha_2) & \cdots & f^{(s-1)}(\alpha_n) \end{pmatrix} : \substack{f(X)\in\mathbb{F}_q[X] \\ \deg(f)<k} \right\} \subseteq \left(\mathbb{F}_q^s\right)^n$$

where we normally need $\mathrm{char}(\mathbb{F}_q)$ be large enough.

More About Subinear Codes: Multiplicity Codes

Definition (Multiplicity codes)

An order-s multiplicity code $\text{MULT}^{s}_{n,k,q}(\alpha_1,\ldots,\alpha_n)$ over $\mathbb{F}_q^s$ is defined as

$$\left\{ \begin{pmatrix} f(\alpha_1) & f(\alpha_2) & \cdots & f(\alpha_n) \\ f^{(1)}(\alpha_1) & f^{(1)}(\alpha_2) & \cdots & f^{(1)}(\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ f^{(s-1)}(\alpha_1) & f^{(s-1)}(\alpha_2) & \cdots & f^{(s-1)}(\alpha_n) \end{pmatrix} : \substack{f(X)\in\mathbb{F}_q[X] \\ \deg(f)<k} \right\} \subseteq \left(\mathbb{F}_q^s\right)^n$$

where we normally need $\text{char}(\mathbb{F}_q)$ be large enough.

Remark: $d(\text{MULT}^{s}_{n,k,q}(\alpha_1,\ldots,\alpha_n)) = sn - k + 1.$

Seminal Works

- It's time to mention seminal works addressing the two former questions.

Seminal Works

- It's time to mention seminal works addressing the two former questions.
- Parvaresh and Vardy (FOCS'05) constructed the first explicit codes with efficient encoder and (list) decoder beyond the Johnson bound.

Seminal Works

- It's time to mention seminal works addressing the two former questions.
- Parvaresh and Vardy (FOCS'05) constructed the first explicit codes with efficient encoder and (list) decoder beyond the Johnson bound.
- Guruswami and Rudra (STOC'06) provided the first explicit codes with efficient encoder and (list) decoder up to the list decoding capacity!

Seminal Works

- It's time to mention seminal works addressing the two former questions.
- Parvaresh and Vardy (FOCS'05) constructed the first explicit codes with efficient encoder and (list) decoder beyond the Johnson bound.
- Guruswami and Rudra (STOC'06) provided the first explicit codes with efficient encoder and (list) decoder up to the list decoding capacity! These codes are called folded Reed–Solomon codes, the same ones as we just introduced.

Seminal Works

- It's time to mention seminal works addressing the two former questions.
- Parvaresh and Vardy (FOCS'05) constructed the first explicit codes with efficient encoder and (list) decoder beyond the Johnson bound.
- Guruswami and Rudra (STOC'06) provided the first explicit codes with efficient encoder and (list) decoder up to the list decoding capacity! These codes are called folded Reed–Solomon codes, the same ones as we just introduced.
- **Barrier:** For folded RS codes of rate R and block length n, the best known list-decoding radius is $1 - R - \varepsilon$, but the list size of Guruswami–Rudra (STOC'06) is $n^{O(1/\varepsilon)}$.

Open Problem (Guruswami–Rudra'06)

It remains an open question to reduce this list size $n^{O(1/\varepsilon)}$*, given that existential random coding arguments work with a list size of* $O(1/\varepsilon)$.

Open Problem (Guruswami–Rudra'06)

It remains an open question to reduce this list size $n^{O(1/\varepsilon)}$, given that existential random coding arguments work with a list size of $O(1/\varepsilon)$.

The previous state-of-the-art is due to a work of Kopparty, Ron-Zewi, Saraf, and Wootters (FOCS'18), where they shrink the list size from $n^{O(1/\varepsilon)}$ to $\left(1/\varepsilon\right)^{O(1/\varepsilon)}$.

The Open Problem of Guruswami–Rudra at STOC'06

Open Problem (Guruswami–Rudra'06)

It remains an open question to reduce this list size $n^{O(1/\varepsilon)}$, given that existential random coding arguments work with a list size of $O(1/\varepsilon)$.

The previous state-of-the-art is due to a work of Kopparty, Ron-Zewi, Saraf, and Wootters (FOCS'18), where they shrink the list size from $n^{O(1/\varepsilon)}$ to $(1/\varepsilon)^{O(1/\varepsilon)}$. Simplified by a work of Tamo (IEEE TIT'24).

We fully resolved the near two-decade-old open problem of Guruswami and Rudra (STOC'06).

Our Results

We fully resolved the near two-decade-old open problem of Guruswami and Rudra (STOC'06).

Theorem (Chen–Zhang STOC'25)

For $L \geq 1$, any appropriate folded RS codes $\mathrm{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ *of rate $R := k/n$ and block length n is* $\left(\frac{L}{L+1}\left(1 - \frac{sR}{s-L+1}\right), L\right)$ *average-radius list decodable.*

Our Results

We fully resolved the near two-decade-old open problem of Guruswami and Rudra (STOC'06).

Theorem (Chen–Zhang STOC'25)

For $L \geq 1$, any appropriate folded RS codes $\mathrm{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ *of rate $R := k/n$ and block length n is* $\left(\frac{L}{L+1}\left(1 - \frac{sR}{s-L+1}\right), L\right)$ *average-radius list decodable. In particular, it is* $(1 - R - \varepsilon, O(1/\varepsilon))$ *average-radius list decodable by choosing* $L = \Theta(1/\varepsilon)$ *and* $s = \Theta(1/\varepsilon^2)$.

Our Results

We fully resolved the near two-decade-old open problem of Guruswami and Rudra (STOC'06).

Theorem (Chen–Zhang STOC'25)

For $L \geq 1$, any appropriate folded RS codes $\mathsf{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ *of rate $R := k/n$ and block length n is* $\left(\frac{L}{L+1}\left(1 - \frac{sR}{s-L+1}\right), L\right)$ *average-radius list decodable. In particular, it is* $(1 - R - \varepsilon, O(1/\varepsilon))$ *average-radius list decodable by choosing* $L = \Theta(1/\varepsilon)$ *and* $s = \Theta(1/\varepsilon^2)$.

Remark (Concurrent and Independent Work)

In a concurrent and independent work, Srivastava (SODA'25) shows the $\left(\frac{L}{L+1}\left(1 - \frac{sR}{s-L+1}\right), L^2\right)$ list-decodablility — a weaker result — for folded RS codes.

More about Our Results

Similarly, our methodology can prove that any multiplicity codes achieve the near-optimal trade-off in average-radius list decodability.

More about Our Results

Similarly, our methodology can prove that any multiplicity codes achieve the near-optimal trade-off in average-radius list decodability.

Theorem (Chen–Zhang STOC'25)

Let p be a prime number. For any integers $s, n, k, L \geq 1$, multiplicity codes $\mathsf{MULT}^{s}_{n,k,p}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *of rate $R := k/n$ and block length n is $\left(\frac{L}{L+1}\left(1 - \frac{sR}{s-L+1}\right), L\right)$ average-radius list-decodable.*

More about Our Results

Similarly, our methodology can prove that any multiplicity codes achieve the near-optimal trade-off in average-radius list decodability.

Theorem (Chen–Zhang STOC'25)

Let p be a prime number. For any integers $s, n, k, L \geq 1$, multiplicity codes $\mathsf{MULT}^{s}_{n,k,p}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *of rate $R := k/n$ and block length n is $\left(\frac{L}{L+1}\left(1 - \frac{sR}{s-L+1}\right), L\right)$ average-radius list-decodable. In particular, it is $(1 - R - \varepsilon, O(1/\varepsilon))$ average-radius list decodable by choosing $L = \Theta(1/\varepsilon)$ and $s = \Theta(1/\varepsilon^2)$.*

More about Our Results

Similarly, our methodology can prove that any multiplicity codes achieve the near-optimal trade-off in average-radius list decodability.

Theorem (Chen–Zhang STOC'25)

Let p be a prime number. For any integers $s, n, k, L \geq 1$, multiplicity codes $\mathrm{MULT}^{s}_{n,k,p}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of rate $R := k/n$ and block length n is $\left(\frac{L}{L+1}\left(1 - \frac{sR}{s-L+1}\right), L\right)$ average-radius list-decodable. In particular, it is $(1 - R - \varepsilon, O(1/\varepsilon))$ average-radius list decodable by choosing $L = \Theta(1/\varepsilon)$ and $s = \Theta(1/\varepsilon^2)$.

This also yields an exponential improvement over the previous state-of-the-art by Kopparty, Ron-Zewi, Saraf, and Wootters (FOCS'18), whose approach requires a list size of $(1/\varepsilon)^{O(1/\varepsilon)}$.

Generalized Singleton Bound

Our bound $\left(\frac{L}{L+1}\left(1-\frac{sR}{s-L+1}\right), L\right)$ is almost optimal!

Generalized Singleton Bound

Our bound $\left(\frac{L}{L+1}\left(1-\frac{sR}{s-L+1}\right), L\right)$ is almost optimal! The evidence is stated below.

Theorem (Generalized Singleton bound, Shangguan–Tamo STOC'20)

For any code C of rate R, if C is (ρ, L) list decodable and $q > L$, then

$$\rho \lesssim \frac{L}{L+1}(1-R).$$

FRS Proof Overview: The First Step

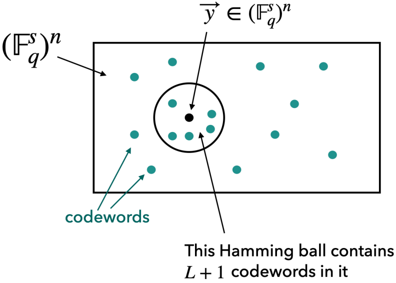
- Our proof is a proof by contradiction.

FRS Proof Overview: The First Step

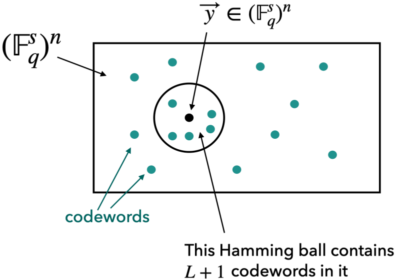
- Our proof is a proof by contradiction.
- Assume the $[n, k]$ FRS code $\mathrm{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ defined by $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^n$ is not $\left(\frac{L}{L+1}\left(1 - \frac{sR}{s-L+1}\right), L\right)$ (average-radius) list decodable.

FRS Proof Overview: The First Step

- Our proof is a proof by contradiction.
- Assume the $[n, k]$ FRS code $\mathrm{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ defined by $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^n$ is not $\left(\frac{L}{L+1}\left(1 - \frac{sR}{s-L+1}\right), L\right)$ (average-radius) list decodable.



FRS Proof Overview: The First Step



There exist a point $\vec{y} \in (\mathbb{F}_q^s)^n$ and $L+1$ pair-wise distinct codewords $\vec{c}_1, \vec{c}_2, \ldots, \vec{c}_{L+1} \in \mathsf{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ such that

$$\sum_{i=1}^{L+1} d(\vec{y}, \vec{c}_i) \leq L \left(n - \frac{k}{s - L + 1} \right).$$

FRS Proof Overview: The First Step

- There exist a point $\vec{y} \in (\mathbb{F}_q^s)^n$ and $L+1$ pair-wise distinct codewords $\vec{c}_1, \vec{c}_2, \ldots, \vec{c}_{L+1} \in \mathrm{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ such that

$$\sum_{i=1}^{L+1} d(\vec{y}, \vec{c}_i) \leq L\left(n - \frac{k}{s-L+1}\right).$$

- This means the codewords must have a lot of "agreements," which can be later captured in a hypergraph!

- There exist a point $\vec{y} \in (\mathbb{F}_q^s)^n$ and $L+1$ pair-wise distinct codewords $\vec{c}_1, \vec{c}_2, \ldots, \vec{c}_{L+1} \in \mathrm{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ such that

$$\sum_{i=1}^{L+1} d(\vec{y}, \vec{c}_i) \leq L\left(n - \frac{k}{s-L+1}\right).$$

- This means the codewords must have a lot of "agreements," which can be later captured in a hypergraph!

Definition (Agreements)

$I(\vec{y}, \vec{c}) := |\{i : x[i] = y[i]\}| \in [n]$, where $[n] := \{1, 2, \ldots, n\}$.

FRS Proof Overview: The First Step

- There exist a point $\vec{y} \in (\mathbb{F}_q^s)^n$ and $L+1$ pair-wise distinct codewords $\vec{c}_1, \vec{c}_2, \ldots, \vec{c}_{L+1} \in \mathsf{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ such that

$$\sum_{i=1}^{L+1} d(\vec{y}, \vec{c}_i) \leq L\left(n - \frac{k}{s-L+1}\right).$$

- This means the codewords must have a lot of "agreements," which can be later captured in a hypergraph!

Definition (Agreements)

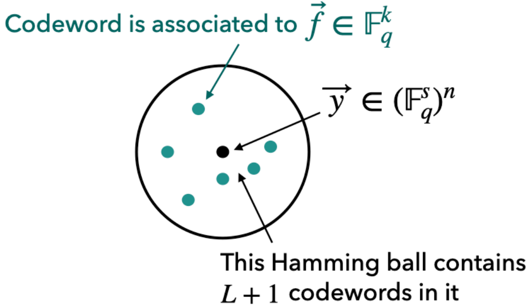
$I(\vec{y}, \vec{c}) := |\{i : x[i] = y[i]\}| \in [n]$, where $[n] := \{1, 2, \ldots, n\}$.

$$\sum_{i=1}^{L+1} I(\vec{y}, \vec{c}_i) \geq n + \frac{Lk}{s-L+1} \qquad (*)$$

Each $\vec{c}_j \in \mathsf{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ is associated to a low degree polynomial $f(X) \in \mathbb{F}_q[X]$.

Each $\vec{c}_j \in \mathsf{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ is associated to a low degree polynomial $f(X) \in \mathbb{F}_q[X]$. Its coefficients correspond to a vector $\vec{f} \in \mathbb{F}_q^k$.

Each $\vec{c}_j \in \mathsf{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$ is associated to a low degree polynomial $f(X) \in \mathbb{F}_q[X]$. Its coefficients correspond to a vector $\vec{f} \in \mathbb{F}_q^k$.



New Perspectives: Geometric Agreement Hypergraph

Consider the folded RS code $\mathsf{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$, a received word $\vec{y} \in (\mathbb{F}_q^s)^n$, and ℓ vectors $\vec{f}_1, \vec{f}_2, \ldots, \vec{f}_\ell \in \mathbb{F}_q^k$.

Consider the folded RS code $\mathrm{FRS}_{n,k,q,s}(\alpha_1,\ldots,\alpha_n)$, a received word $\vec{y} \in (\mathbb{F}_q^s)^n$, and ℓ vectors $\vec{f_1}, \vec{f_2}, \ldots, \vec{f_\ell} \in \mathbb{F}_q^k$.

Definition (Geometric agreement hypergraph based on FRS codes)

We define the geometric agreement hypergraph $(\mathcal{V}, \mathcal{E})$ with vertex set $\mathcal{V} := \left\{\vec{f_1}, \vec{f_2}, \ldots, \vec{f_\ell}\right\}$ and a tuple of n hyperedges $\mathcal{E} := \{e_1, e_2, \ldots, e_n\}$, where $e_i := \left\{\vec{f_j} \in \mathcal{V} : \vec{y}[i] = \mathrm{Enc}(f_j)[i]\right\}$.

Consider the folded RS code $\mathsf{FRS}_{n,k,q,s}(\alpha_1, \dots, \alpha_n)$, a received word $\vec{y} \in (\mathbb{F}_q^s)^n$, and ℓ vectors $\vec{f}_1, \vec{f}_2, \dots, \vec{f}_\ell \in \mathbb{F}_q^k$.

Definition (Geometric agreement hypergraph based on FRS codes)

We define the geometric agreement hypergraph $(\mathcal{V}, \mathcal{E})$ with vertex set $\mathcal{V} := \left\{\vec{f}_1, \vec{f}_2, \dots, \vec{f}_\ell\right\}$ and a tuple of n hyperedges $\mathcal{E} := \{e_1, e_2, \dots, e_n\}$, where $e_i := \left\{\vec{f}_j \in \mathcal{V} : \vec{y}[i] = \mathsf{Enc}(f_j)[i]\right\}$.

Definition (Weight)

We define the weight $\mathsf{wt}(\mathcal{V}, \mathcal{E}) := \sum_{i=1}^{n} \mathsf{wt}(e_i)$, where $\mathsf{wt}(e_i) := \max(|e_i| - 1, 0)$.

Consider the folded RS code $\mathrm{FRS}_{n,k,q,s}(\alpha_1, \ldots, \alpha_n)$, a received word $\vec{y} \in (\mathbb{F}_q^s)^n$, and ℓ vectors $\vec{f_1}, \vec{f_2}, \ldots, \vec{f_\ell} \in \mathbb{F}_q^k$.

Definition (Geometric agreement hypergraph based on FRS codes)

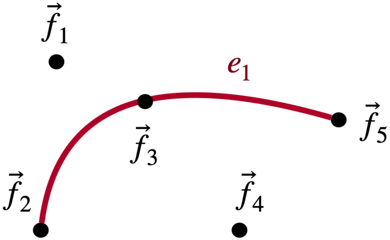
We define the geometric agreement hypergraph $(\mathcal{V}, \mathcal{E})$ with vertex set $\mathcal{V} := \left\{\vec{f_1}, \vec{f_2}, \ldots, \vec{f_\ell}\right\}$ and a tuple of n hyperedges $\mathcal{E} := \{e_1, e_2, \ldots, e_n\}$, where $e_i := \left\{\vec{f_j} \in \mathcal{V} : \vec{y}[i] = \mathrm{Enc}(f_j)[i]\right\}$.

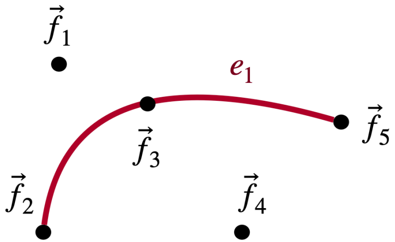
Definition (Weight)

We define the weight $\mathrm{wt}(\mathcal{V}, \mathcal{E}) := \sum_{i=1}^n \mathrm{wt}(e_i)$, where $\mathrm{wt}(e_i) := \max(|e_i| - 1, 0)$.

A lot of "agreements" implies the corresponding geometric agreement hypergraph has large enough weight.

Geometric Agreement Hypergraph: An Example





Consider an example when $\ell = 5$. Given $\vec{y} = (y_1, y_2, \ldots, y_n)$ in $(\mathbb{F}_q^s)^n$, the red hyperedge $e_1 = \{\vec{f}_2, \vec{f}_3, \vec{f}_5\}$ tells us that

$$\begin{aligned} y_1 &= \mathrm{Enc}(f_2)[1] := (f_2(\alpha_1), f_2(\gamma\alpha_1), \ldots, f_2(\gamma^{s-1}\alpha_1))^\top \\ &= \mathrm{Enc}(f_3)[1] := (f_3(\alpha_1), f_3(\gamma\alpha_1), \ldots, f_3(\gamma^{s-1}\alpha_1))^\top \\ &= \mathrm{Enc}(f_5)[1] := (f_5(\alpha_1), f_5(\gamma\alpha_1), \ldots, f_5(\gamma^{s-1}\alpha_1))^\top. \end{aligned}$$

Before the introduction of geometric polynomials, we need a matrix called the folded Wronskian.

Before the introduction of geometric polynomials, we need a matrix called the folded Wronskian.

Definition (Folded Wronskian, Guruswami–Kopparty FOCS'13)

Let $f_1(X), \ldots, f_h(X) \in \mathbb{F}_q[X]$ and $\gamma \in \mathbb{F}_q^\times$. We define their γ-folded Wronskian $W_\gamma(f_1, \ldots, f_h)(X) \in (\mathbb{F}_q[X])^{h \times h}$ by

$$W_\gamma(f_1, \ldots, f_h)(X) \stackrel{\text{def}}{=} \begin{pmatrix} f_1(X) & \ldots & f_h(X) \\ f_1(\gamma X) & \cdots & f_h(\gamma X) \\ \vdots & \ddots & \vdots \\ f_1(\gamma^{h-1} X) & \cdots & f_h(\gamma^{h-1} X) \end{pmatrix}.$$

New Perspectives: Geometric Polynomial

Before the introduction of geometric polynomials, we need a matrix called the folded Wronskian.

Definition (Folded Wronskian, Guruswami–Kopparty FOCS'13)

Let $f_1(X), \ldots, f_h(X) \in \mathbb{F}_q[X]$ and $\gamma \in \mathbb{F}_q^\times$. We define their γ-folded Wronskian $W_\gamma(f_1, \ldots, f_h)(X) \in (\mathbb{F}_q[X])^{h\times h}$ by

$$W_\gamma(f_1, \ldots, f_h)(X) \stackrel{\text{def}}{=} \begin{pmatrix} f_1(X) & \cdots & f_h(X) \\ f_1(\gamma X) & \cdots & f_h(\gamma X) \\ \vdots & \ddots & \vdots \\ f_1\left(\gamma^{h-1}X\right) & \cdots & f_h\left(\gamma^{h-1}X\right) \end{pmatrix}.$$

The building block of our geometric polynomial is the determinant of folded Wronskian!

Before the introduction of geometric polynomials, we need a matrix called the folded Wronskian.

Definition (Folded Wronskian, Guruswami–Kopparty FOCS'13)

Let $f_1(X), \ldots, f_h(X) \in \mathbb{F}_q[X]$ and $\gamma \in \mathbb{F}_q^\times$. We define their γ-folded Wronskian $W_\gamma(f_1, \ldots, f_h)(X) \in (\mathbb{F}_q[X])^{h \times h}$ by

$$W_\gamma(f_1, \ldots, f_h)(X) \stackrel{\text{def}}{=} \begin{pmatrix} f_1(X) & \cdots & f_h(X) \\ f_1(\gamma X) & \cdots & f_h(\gamma X) \\ \vdots & \ddots & \vdots \\ f_1(\gamma^{h-1} X) & \cdots & f_h(\gamma^{h-1} X) \end{pmatrix}.$$

The building block of our geometric polynomial is the determinant of folded Wronskian! But how should we ensure it is NOT identical zero?

The building block of our geometric polynomial is the determinant of folded Wronskian! But how should we ensure it is NOT identical zero?

Lemma (Folded Wronskian criterion for linear independence, Guruswami–Kopparty FOCS'13)

Let $k < q$ and $\vec{f}_1, \ldots, \vec{f}_h \in \mathbb{F}_q^k$. Let γ be a generator of $\mathbb{F}_q^\times$. Then $\vec{f}_1, \ldots, \vec{f}_h$ are linearly independent over $\mathbb{F}_q$ if and only if the folded Wronskian determinant $\det W_\gamma(f_1, \ldots, f_h)(X) \neq 0$.

Object: For a given geometric agreement hypergraph, we can define a corresponding geometric polynomial based on the determinant of folded Wronskian.

New Perspectives: Geometric Polynomial

Object: For a given geometric agreement hypergraph, we can define a corresponding geometric polynomial based on the determinant of folded Wronskian.

Definition (Geometric polynomial)

Given L non-zero vectors $\vec{f}_1, \vec{f}_2, \ldots, \vec{f}_L \in \mathbb{F}_q^k$ such that $\dim_{\mathbb{F}_q}(\mathrm{Span}_{\mathbb{F}_q}\{\vec{f}_1, \vec{f}_2, \ldots, \vec{f}_L\}) = \ell \in [L]$.

Object: For a given geometric agreement hypergraph, we can define a corresponding geometric polynomial based on the determinant of folded Wronskian.

Definition (Geometric polynomial)

Given L non-zero vectors $\vec{f}_1, \vec{f}_2, \ldots, \vec{f}_L \in \mathbb{F}_q^k$ such that $\dim_{\mathbb{F}_q}(\mathrm{Span}_{\mathbb{F}_q}\{\vec{f}_1, \vec{f}_2, \ldots, \vec{f}_L\}) = \ell \in [L]$. Then we define the geometric polynomial $V_{\{\vec{f}_i\}_{i \in L}}(X)$ as the following monic polynomial

$$\lambda_{i_1, i_2, \ldots, i_\ell} \cdot \det W_\gamma(f_{i_1}, \ldots, f_{i_\ell})(X),$$

where $\lambda_{i_1, i_2, \ldots, i_\ell} \in \mathbb{F}_q^\times$ and $\{f_{i_1}, \ldots, f_{i_\ell}\}$ forms a $\mathbb{F}_q$-basis of the space $\mathrm{Span}_{\mathbb{F}_q}\{\vec{f}_1, \vec{f}_2, \ldots, \vec{f}_L\}$.

Geometric Agreement Hypergraph Provides Zeros of a Geometric Polynomial With Multiplicity

For $\vec{f}_1, \vec{f}_2, \ldots, \vec{f}_m \in \mathbb{F}_q^k$, we define (informally) $\widetilde{\dim}_{\mathbb{F}_q}\left(\vec{f}_1, \ldots, \vec{f}_m\right)$ as the dimension of the smallest affine subspace that contains all these vectors.

Geometric Agreement Hypergraph Provides Zeros of a Geometric Polynomial With Multiplicity

For $\vec{f}_1, \vec{f}_2, \dots, \vec{f}_m \in \mathbb{F}_q^k$, we define (informally) $\widetilde{\dim}_{\mathbb{F}_q}\left(\vec{f}_1, \dots, \vec{f}_m\right)$ as the dimension of the smallest affine subspace that contains all these vectors.

Theorem (Alternatively stated in Guruswami–Kopparty FOCS'13)

Given L distinct non-zero $\vec{f}_1, \vec{f}_2, \dots, \vec{f}_L \in \mathbb{F}_q^k$. Let $(\mathcal{V}, \mathcal{E})$ be a geometric agreement hypergraph over $\mathcal{V} = \left\{0, \vec{f}_1, \dots, \vec{f}_L\right\}$ where $\mathcal{E} = \left\{e_1, \dots, e_n \subseteq \mathcal{V}\right\}$, then $V_{\{f_i\}_{i \in L}}(X)$ has at least

$$(s - \ell + 1) \sum_{i=1}^{n} \widetilde{\dim}_{\mathbb{F}_q}(e_i)$$

roots with multiplicity, where $\dim(\mathrm{Span}_{\mathbb{F}_q}\{\vec{f}_1, \dots, \vec{f}_L\}) = \ell$.

Contradiction: More Zeros Than Its Degree

A lot of "agreements" implies the corresponding geometric agreement hypergraph has large enough weight.

Contradiction: More Zeros Than Its Degree

A lot of "agreements" implies the corresponding geometric agreement hypergraph has large enough weight.

$$(*) \quad \xrightarrow{\text{implies}} \quad \mathsf{wt}(\mathcal{V}, \mathcal{E}) := \sum_{i=1}^{n} \max(|e_i| - 1, 0) \geq \frac{Lk}{s - L + 1}$$

Contradiction: More Zeros Than Its Degree

A lot of "agreements" implies the corresponding geometric agreement hypergraph has large enough weight.

$$(*) \xrightarrow{\text{implies}} \mathsf{wt}(\mathcal{V}, \mathcal{E}) := \sum_{i=1}^{n} \max(|e_i| - 1, 0) \geq \frac{Lk}{s - L + 1}$$

The degree of our geometric polynomials are bounded by $\ell(k-1)$.

Contradiction: More Zeros Than Its Degree

A lot of "agreements" implies the corresponding geometric agreement hypergraph has large enough weight.

$$(*) \xrightarrow{\text{implies}} \mathsf{wt}(\mathcal{V}, \mathcal{E}) := \sum_{i=1}^{n} \max(|e_i| - 1, 0) \geq \frac{Lk}{s - L + 1}$$

The degree of our geometric polynomials are bounded by $\ell(k-1)$.
Contradiction: Zeros $(s - \ell + 1) \sum_{i=1}^{n} \widetilde{\dim}_{\mathbb{F}_q}(e_i)$ are strictly larger than its degree bounded by $\ell(k-1)$!

Contradiction: More Zeros Than Its Degree

A lot of "agreements" implies the corresponding geometric agreement hypergraph has large enough weight.

$$(*) \xrightarrow{\text{implies}} \mathrm{wt}(\mathcal{V},\mathcal{E}) := \sum_{i=1}^{n} \max(|e_i|-1,0) \geq \frac{Lk}{s-L+1}$$

The degree of our geometric polynomials are bounded by $\ell(k-1)$.
Contradiction: Zeros $(s-\ell+1)\sum_{i=1}^{n}\widetilde{\dim}_{\mathbb{F}_q}(e_i)$ are strictly larger than its degree bounded by $\ell(k-1)$!

Definition (Loss function)

We define the loss function $\mathrm{Loss}:\mathcal{E}\to\mathbb{N}$ that sends a hyperedge $e\in\mathcal{E}$ to $\mathrm{Loss}(e) := \max\left(0, |e|-1-\widetilde{\dim}_{\mathbb{F}_q}(e)\right)$.

Contradiction: More Zeros Than Its Degree

A lot of "agreements" implies the corresponding geometric agreement hypergraph has large enough weight.

$$(*) \xrightarrow{\text{implies}} \mathsf{wt}(\mathcal{V}, \mathcal{E}) := \sum_{i=1}^{n} \max(|e_i| - 1, 0) \geq \frac{Lk}{s - L + 1}$$

The degree of our geometric polynomials are bounded by $\ell(k-1)$.
Contradiction: Zeros $(s - \ell + 1) \sum_{i=1}^{n} \widetilde{\dim}_{\mathbb{F}_q}(e_i)$ are strictly larger than its degree bounded by $\ell(k-1)$!

Definition (Loss function)

We define the loss function $\mathsf{Loss} : \mathcal{E} \to \mathbb{N}$ that sends a hyperedge $e \in \mathcal{E}$ to $\mathsf{Loss}(e) := \max\left(0, |e| - 1 - \widetilde{\dim}_{\mathbb{F}_q}(e)\right)$.

We do NOT have much loss!

Contradiction: More Zeros Than Its Degree

We finish the contradiction by bounding the loss!

Contradiction: More Zeros Than Its Degree

We finish the contradiction by bounding the loss!

Theorem (Chen–Zhang STOC'25)

Let $\{\vec{f}_i\}_{i\in[L]}$ *be a set of distinct non-zero vectors in* $\mathbb{F}_q^k$ *and vertices* $\mathcal{V} := \{0, \vec{f}_1, \ldots, \vec{f}_L\}$. *Let* $\dim_{\mathbb{F}_q}(\mathrm{Span}_{\mathbb{F}_q}\{\vec{f}_1, \ldots, \vec{f}_L\}) = \ell$.

Contradiction: More Zeros Than Its Degree

We finish the contradiction by bounding the loss!

Theorem (Chen–Zhang STOC'25)

Let $\{\vec{f}_i\}_{i\in[L]}$ be a set of distinct non-zero vectors in $\mathbb{F}_q^k$ and vertices $\mathcal{V} := \{0, \vec{f}_1, \ldots, \vec{f}_L\}$. Let $\dim_{\mathbb{F}_q}(\mathrm{Span}_{\mathbb{F}_q}\{\vec{f}_1, \ldots, \vec{f}_L\}) = \ell$. Consider a geometric agreement hypergraph $(\mathcal{V}, \mathcal{E})$ with n hyperedges $\mathcal{E} = \{e_1, e_2, \ldots, e_n \subseteq \mathcal{V}\}$ such that for any proper subset $\mathcal{H} \subsetneq \mathcal{V}$ with $|\mathcal{H}| \geq 2$, we have $\mathrm{wt}(\mathcal{H}, \mathcal{E}|_{\mathcal{H}}) < \frac{(|\mathcal{H}|-1)k}{s-|\mathcal{H}|+2}$.

Contradiction: More Zeros Than Its Degree

We finish the contradiction by bounding the loss!

Theorem (Chen–Zhang STOC'25)

Let $\{\vec{f}_i\}_{i\in[L]}$ be a set of distinct non-zero vectors in $\mathbb{F}_q^k$ and vertices $\mathcal{V} := \{0, \vec{f}_1, \ldots, \vec{f}_L\}$. Let $\dim_{\mathbb{F}_q}(\mathrm{Span}_{\mathbb{F}_q}\{\vec{f}_1, \ldots, \vec{f}_L\}) = \ell$. Consider a geometric agreement hypergraph $(\mathcal{V}, \mathcal{E})$ with n hyperedges $\mathcal{E} = \{e_1, e_2, \ldots, e_n \subseteq \mathcal{V}\}$ such that for any proper subset $\mathcal{H} \subsetneq \mathcal{V}$ with $|\mathcal{H}| \geq 2$, we have $\mathrm{wt}(\mathcal{H}, \mathcal{E}|_{\mathcal{H}}) < \frac{(|\mathcal{H}|-1)k}{s-|\mathcal{H}|+2}$. Then, we have the following upper bound on the loss function

$$\sum_{i\in[n]} \mathrm{Loss}(e_i) \leq \frac{(L-\ell)k}{s-L+1}.$$

Open Problems and Future Directions

- Explicit constructions of Reed–Solomon codes achieving list decoding capacity.

Open Problems and Future Directions

- Explicit constructions of Reed–Solomon codes achieving list decoding capacity.
- More efficient decoding algorithms.

Open Problems and Future Directions

- Explicit constructions of Reed–Solomon codes achieving list decoding capacity.
- More efficient decoding algorithms.
- Generalizations to list recoverable codes.

Open Problems and Future Directions

- Explicit constructions of Reed–Solomon codes achieving list decoding capacity.
- More efficient decoding algorithms.
- Generalizations to list recoverable codes.
    - A code is $(\rho, \ell = 1, L)$ list recoverable iff it is (ρ, L) list decodable.

Open Problems and Future Directions

- Explicit constructions of Reed–Solomon codes achieving list decoding capacity.
- More efficient decoding algorithms.
- Generalizations to list recoverable codes.
  - A code is $(\rho, \ell = 1, L)$ list recoverable iff it is (ρ, L) list decodable.
  - The optimal trade-off between the list recovery radius ρ, the rate R, and the parameter ℓ is not known.

Open Problems and Future Directions

- Explicit constructions of Reed–Solomon codes achieving list decoding capacity.
- More efficient decoding algorithms.
- Generalizations to list recoverable codes.
  - A code is $(\rho, \ell = 1, L)$ list recoverable iff it is (ρ, L) list decodable.
  - The optimal trade-off between the list recovery radius ρ, the rate R, and the parameter ℓ is not known.
  - Recently, (Chen–Zhang STOC'25) proved that RS (and FRS) codes are NOT $(1 - R - \varepsilon, \ell, \ell^{\frac{R}{2\varepsilon} - 1} - 1)$ list recoverable.

Open Problems and Future Directions

- Explicit constructions of Reed–Solomon codes achieving list decoding capacity.
- More efficient decoding algorithms.
- Generalizations to list recoverable codes.
  - A code is $(\rho, \ell = 1, L)$ list recoverable iff it is (ρ, L) list decodable.
  - The optimal trade-off between the list recovery radius ρ, the rate R, and the parameter ℓ is not known.
  - Recently, (Chen–Zhang STOC'25) proved that RS (and FRS) codes are NOT $(1 - R - \varepsilon, \ell, \ell^{\frac{R}{2\varepsilon}-1} - 1)$ list recoverable. On the other hand, FRS codes are $(1 - R - \varepsilon, \ell, \ell^{O\left(\frac{1+\log \ell}{\varepsilon}\right)})$ list recoverable (Kopparty–Ron-Zewi–Saraf–Wootter FOCS'18).

The End

Questions?