

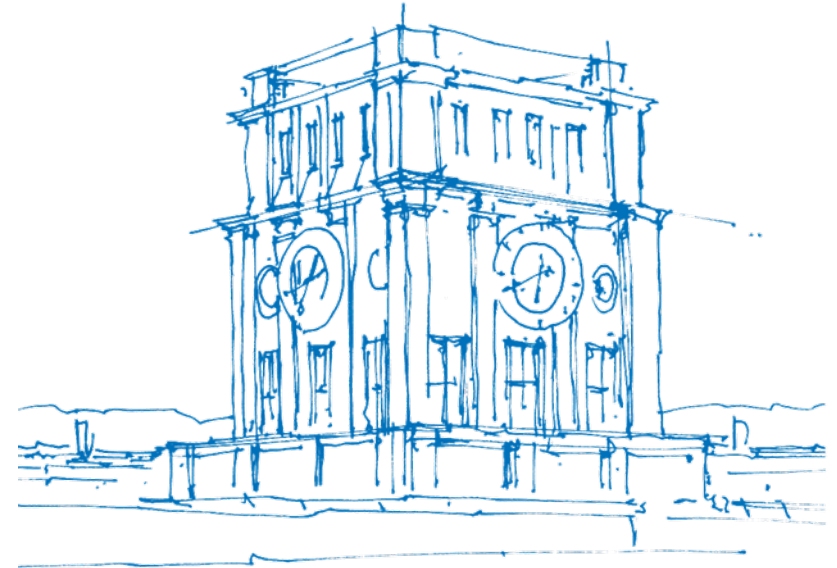
Decoding Insertions/Deletions via List Recovery

Anisha Banerjee¹, Roni Con², Antonia Wachter-Zeh¹ and Eitan Yaakobi²

¹ Technical University of Munich
Institute for Communications Engineering

²Technion – Israel Institute of Technology
Department of Computer Science

June 25, 2025



TUM Uhrenturm

Outline

Introduction

Decoding via List Recovery

- Adversarial Insdels

- Probabilistic Insdels

Adapting Koetter-Vardy Algorithm

Conclusion

Introduction

Decoding via List Recovery

Adversarial Insdels

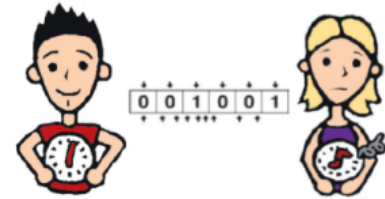
Probabilistic Insdels

Adapting Koetter-Vardy Algorithm

Conclusion

Motivation

- Insertions & deletions occur
 - due to improper synchronization



G. M. Church *et al.*, "Next-generation digital information storage in dna," *Science*, vol. 337, no. 6102, pp. 1628–1628, Sep. 2012

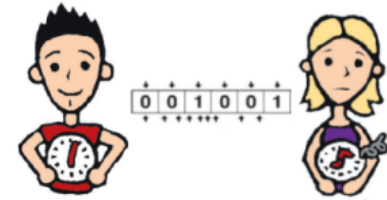
N. Goldman *et al.*, "Towards practical, high-capacity, low-maintenance information storage in synthesized dna," *Nature*, vol. 494, no. 7435,

pp. 77–80, Feb. 2013

Anisha Banerjee (TUM)

Motivation

- Insertions & deletions occur
 - due to improper synchronization
 - in molecular storage paradigms, e.g. DNA data storage



G. M. Church *et al.*, "Next-generation digital information storage in dna," *Science*, vol. 337, no. 6102, pp. 1628–1628, Sep. 2012

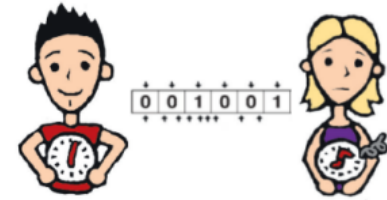
N. Goldman *et al.*, "Towards practical, high-capacity, low-maintenance information storage in synthesized dna," *Nature*, vol. 494, no. 7435,

pp. 77–80, Feb. 2013

Anisha Banerjee (TUM)

Motivation

- Insertions & deletions occur
 - due to improper synchronization
 - in molecular storage paradigms, e.g. DNA data storage
- Hard to perform decoding efficiently.



G. M. Church *et al.*, "Next-generation digital information storage in dna," *Science*, vol. 337, no. 6102, pp. 1628–1628, Sep. 2012

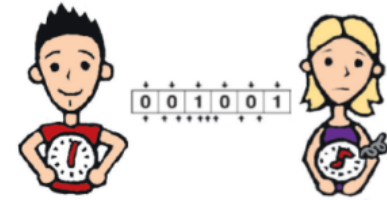
N. Goldman *et al.*, "Towards practical, high-capacity, low-maintenance information storage in synthesized dna," *Nature*, vol. 494, no. 7435,

pp. 77–80, Feb. 2013

Anisha Banerjee (TUM)

Motivation

- Insertions & deletions occur
 - due to improper synchronization
 - in molecular storage paradigms, e.g. DNA data storage
- Hard to perform decoding efficiently.
- *Trick*: reduce the insdel-decoding problem to *list recovery*!



G. M. Church *et al.*, "Next-generation digital information storage in dna," *Science*, vol. 337, no. 6102, pp. 1628–1628, Sep. 2012
 N. Goldman *et al.*, "Towards practical, high-capacity, low-maintenance information storage in synthesized dna," *Nature*, vol. 494, no. 7435,

What is List Recovery?

- Consider $\mathcal{C} \subseteq \mathbb{F}_q^n$ that corrects t substitutions.
- Assume integers $t' > t$ and $L, \ell > 1$.

V. Guruswami, “Algorithmic results in list decoding,” *Foundations and Trends® in Theoretical Computer Science*, vol. 2, no. 2, pp. 107–195,

2006

Anisha Banerjee (TUM)

What is List Recovery?

- Consider $\mathcal{C} \subseteq \mathbb{F}_q^n$ that corrects t substitutions.
- Assume integers $t' > t$ and $L, \ell > 1$.
- **Unique Decoding:**
Returns $\hat{\mathbf{c}} \in \mathcal{C}$ s.t. $|\{i \in [n] : \hat{c}_i \neq y_i\}| \leq t$.

Decoder input

$$\mathbf{y} = \begin{array}{|c|c|c|c|} \hline 1 & 3 & \dots\dots & 0 \\ \hline \end{array} \in \mathbb{F}_{q=4}^n$$

V. Guruswami, "Algorithmic results in list decoding," *Foundations and Trends® in Theoretical Computer Science*, vol. 2, no. 2, pp. 107–195,

2006

Anisha Banerjee (TUM)

What is List Recovery?

- Consider $\mathcal{C} \subseteq \mathbb{F}_q^n$ that corrects t substitutions.
- Assume integers $t' > t$ and $L, \ell > 1$.
- **Unique Decoding:**
Returns $\hat{\mathbf{c}} \in \mathcal{C}$ s.t. $|\{i \in [n] : \hat{c}_i \neq y_i\}| \leq t$.
- **List Decoding:**
Returns $\leq L$ codewords $\hat{\mathbf{c}} \in \mathcal{C}$ s.t. $|\{i \in [n] : \hat{c}_i \neq y_i\}| \leq t'$.

Decoder input

$$\mathbf{y} = \begin{array}{|c|c|c|c|} \hline 1 & 3 & \dots\dots & 0 \\ \hline \end{array} \in \mathbb{F}_{q=4}^n$$

V. Guruswami, "Algorithmic results in list decoding," *Foundations and Trends® in Theoretical Computer Science*, vol. 2, no. 2, pp. 107–195,

2006

Anisha Banerjee (TUM)

What is List Recovery?

- Consider $\mathcal{C} \subseteq \mathbb{F}_q^n$ that corrects t substitutions.
- Assume integers $t' > t$ and $L, \ell > 1$.
- **Unique Decoding:**
Returns $\hat{\mathbf{c}} \in \mathcal{C}$ s.t. $|\{i \in [n] : \hat{c}_i \neq y_i\}| \leq t$.
- **List Decoding:**
Returns $\leq L$ codewords $\hat{\mathbf{c}} \in \mathcal{C}$ s.t. $|\{i \in [n] : \hat{c}_i \neq y_i\}| \leq t'$.
- **List Recovery:**
Returns $\leq L$ codewords $\hat{\mathbf{c}} \in \mathcal{C}$ s.t. $|\{i \in [n] : \hat{c}_i \notin S_i\}| \leq t'$.

Decoder input

$$\mathbf{y} = \boxed{1} \boxed{3} \boxed{\dots\dots} \boxed{0} \in \mathbb{F}_{q=4}^n$$

$$S = \boxed{\{1,0\}} \boxed{\{2,3\}} \boxed{\dots\dots} \boxed{\{0,2\}} \in \left(\mathbb{F}_{\ell=2}^{q=4}\right)^n$$

V. Guruswami, "Algorithmic results in list decoding," *Foundations and Trends® in Theoretical Computer Science*, vol. 2, no. 2, pp. 107–195,

2006

Anisha Banerjee (TUM)

What is List Recovery?

- Consider $\mathcal{C} \subseteq \mathbb{F}_q^n$ that corrects t substitutions.
- Assume integers $t' > t$ and $L, \ell > 1$.
- Unique Decoding:**
Returns $\hat{\mathbf{c}} \in \mathcal{C}$ s.t. $|\{i \in [n] : \hat{c}_i \neq y_i\}| \leq t$.
- List Decoding:**
Returns $\leq L$ codewords $\hat{\mathbf{c}} \in \mathcal{C}$ s.t. $|\{i \in [n] : \hat{c}_i \neq y_i\}| \leq t'$.
- List Recovery:**
Returns $\leq L$ codewords $\hat{\mathbf{c}} \in \mathcal{C}$ s.t. $|\{i \in [n] : \hat{c}_i \notin S_i\}| \leq t'$.

Decoder input

$$\mathbf{y} = \boxed{1} \boxed{3} \dots \boxed{0} \in \mathbb{F}_{q=4}^n$$

$$S = \boxed{\{1, 0\}} \boxed{\{2, 3\}} \dots \boxed{\{0, 2\}} \in \left(\mathbb{F}_{q=4}^{\ell=2}\right)^n$$

V. Guruswami, "Algorithmic results in list decoding," *Foundations and Trends® in Theoretical Computer Science*, vol. 2, no. 2, pp. 107–195,

2006

Anisha Banerjee (TUM)

List-Recoverable Codes

Definition (List-Decodable Codes)

For $\rho \in [0, 1]$ and integer L , a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is (ρ, L) -list-decodable if for any $\mathbf{y} \in \mathbb{F}_q^n$ there are $\leq L$ codewords $\mathbf{c} \in \mathcal{C}$ that satisfy $|\{i \in [n] : c_i \neq y_i\}| \leq \rho n$.

List-Recoverable Codes

Definition (List-Decodable Codes)

For $\rho \in [0, 1]$ and integer L , a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is (ρ, L) -*list-decodable* if for any $\mathbf{y} \in \mathbb{F}_q^n$ there are $\leq L$ codewords $\mathbf{c} \in \mathcal{C}$ that satisfy $|\{i \in [n] : c_i \neq y_i\}| \leq \rho n$.

Definition (List-Recoverable Codes)

For $\rho \in [0, 1]$ and integers ℓ, L , a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is (ρ, ℓ, L) -*list-recoverable* if for any $\mathbf{S} \in \binom{\mathbb{F}_q}{\ell}^n$ there are $\leq L$ codewords $\mathbf{c} \in \mathcal{C}$ that satisfy $|\{i \in [n] : c_i \notin S_i\}| \leq \rho n$.

List-Recoverable Codes

Definition (List-Decodable Codes)

For $\rho \in [0, 1]$ and integer L , a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is (ρ, L) -list-decodable if for any $\mathbf{y} \in \mathbb{F}_q^n$ there are $\leq L$ codewords $\mathbf{c} \in \mathcal{C}$ that satisfy $|\{i \in [n] : c_i \neq y_i\}| \leq \rho n$.

Definition (List-Recoverable Codes)

For $\rho \in [0, 1]$ and integers ℓ, L , a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is (ρ, ℓ, L) -list-recoverable if for any $\mathbf{S} \in \binom{\mathbb{F}_q}{\ell}^n$ there are $\leq L$ codewords $\mathbf{c} \in \mathcal{C}$ that satisfy $|\{i \in [n] : c_i \notin S_i\}| \leq \rho n$.

- A (ρ, L) -list-decodable code \equiv a $(\rho, \ell = 1, L)$ -list-recoverable code.

List-Recoverable Codes

Definition (List-Decodable Codes)

For $\rho \in [0, 1]$ and integer L , a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is (ρ, L) -list-decodable if for any $\mathbf{y} \in \mathbb{F}_q^n$ there are $\leq L$ codewords $\mathbf{c} \in \mathcal{C}$ that satisfy $|\{i \in [n] : c_i \neq y_i\}| \leq \rho n$.

Definition (List-Recoverable Codes)

For $\rho \in [0, 1]$ and integers ℓ, L , a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is (ρ, ℓ, L) -list-recoverable if for any $\mathbf{S} \in \binom{\mathbb{F}_q}{\ell}^n$ there are $\leq L$ codewords $\mathbf{c} \in \mathcal{C}$ that satisfy $|\{i \in [n] : c_i \notin S_i\}| \leq \rho n$.

- A (ρ, L) -list-decodable code \equiv a $(\rho, \ell = 1, L)$ -list-recoverable code.
- **Example:** RS codes are efficiently list-recoverable by the Guruswami-Sudan (GS) decoder.

Prior Work

- Efficient insdel decoder with synchronization symbols [\[Haeupler and Shahrabi '17\]](#)

Prior Work

- Efficient insdel decoder with synchronization symbols [[Haeupler and Shahrabi '17](#)]
- Reed-Solomon codes for insdels
 - [[Safavi-Naini and Wang '02](#)], [[Wang *et al.* '04](#)], [[Tonien and Safavi-Naini '07](#)], [[Duc *et al.* '21](#)], [[Liu and Tjuawinata '21](#)], [[Con *et al.* '23](#)], [[Liu '24](#)], [[Con *et al.* '24](#)]

Prior Work

- Efficient insdel decoder with synchronization symbols [Haeupler and Shahrabi '17]
- Reed-Solomon codes for insdels
 - [Safavi-Naini and Wang '02], [Wang *et al.* '04], [Tonien and Safavi-Naini '07], [Duc *et al.* '21], [Liu and Tjuawinata '21], [Con *et al.* '23], [Liu '24], [Con *et al.* '24]
- Only efficient non-trivial insdel decoder for $[n, k = 2]_q$ RS codes [Singhvi '24]
 - for $[n, k = 2]_q$ RS codes for insdels in [Con *et al.* '24]
 - corrects $n - 3$ deletions in linear time.

Overview of Results

- $d_{\text{ed}}(\mathbf{x}, \mathbf{y}) \leftarrow$ edit distance between $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$

Overview of Results

- $d_{\text{ed}}(\mathbf{x}, \mathbf{y}) \leftarrow$ edit distance between $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$

Definition (List-Decodable-Insdel Codes)

For $\rho \in [0, 1]$ and integer $L \geq 1$, $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a (ρ, L) -list-decodable-insdel code if for any $\mathbf{y} \in \mathbb{F}_q^m$ it holds that $|\{\mathbf{c} \in \mathcal{C} : d_{\text{ed}}(\mathbf{c}, \mathbf{y}) \leq \rho n\}| \leq L$.

Overview of Results

- $d_{\text{ed}}(\mathbf{x}, \mathbf{y}) \leftarrow$ edit distance between $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$

Definition (List-Decodable-Insdel Codes)

For $\rho \in [0, 1]$ and integer $L \geq 1$, $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a (ρ, L) -list-decodable-insdel code if for any $\mathbf{y} \in \mathbb{F}_q^m$ it holds that $|\{\mathbf{c} \in \mathcal{C} : d_{\text{ed}}(\mathbf{c}, \mathbf{y}) \leq \rho n\}| \leq L$.

Our Results

- Any $(\rho, 2\rho n + 1, L)$ -list-recoverable code \mathcal{C} is a (ρ, L) -list-decodable-insdel code.

Overview of Results

- $d_{\text{ed}}(\mathbf{x}, \mathbf{y}) \leftarrow$ edit distance between $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$

Definition (List-Decodable-Insdel Codes)

For $\rho \in [0, 1]$ and integer $L \geq 1$, $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a (ρ, L) -list-decodable-insdel code if for any $\mathbf{y} \in \mathbb{F}_q^m$ it holds that $|\{\mathbf{c} \in \mathcal{C} : d_{\text{ed}}(\mathbf{c}, \mathbf{y}) \leq \rho n\}| \leq L$.

Our Results

- Any $(\rho, 2\rho n + 1, L)$ -list-recoverable code \mathcal{C} is a (ρ, L) -list-decodable-insdel code.
 - First efficient insdel-list-decoder for $[n, k > 2]$ RS codes!

Overview of Results

- $d_{\text{ed}}(\mathbf{x}, \mathbf{y}) \leftarrow$ edit distance between $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$

Definition (List-Decodable-Insel Codes)

For $\rho \in [0, 1]$ and integer $L \geq 1$, $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a (ρ, L) -list-decodable-insdel code if for any $\mathbf{y} \in \mathbb{F}_q^m$ it holds that $|\{\mathbf{c} \in \mathcal{C} : d_{\text{ed}}(\mathbf{c}, \mathbf{y}) \leq \rho n\}| \leq L$.

Our Results

- Any $(\rho, 2\rho n + 1, L)$ -list-recoverable code \mathcal{C} is a (ρ, L) -list-decodable-insdel code.
 - First efficient insdel-list-decoder for $[n, k > 2]$ RS codes!
 - Rate-error tradeoffs for adversarial & probabilistic insdel channels

Overview of Results

- $d_{\text{ed}}(\mathbf{x}, \mathbf{y}) \leftarrow$ edit distance between $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$

Definition (List-Decodable-Insdel Codes)

For $\rho \in [0, 1]$ and integer $L \geq 1$, $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a (ρ, L) -list-decodable-insdel code if for any $\mathbf{y} \in \mathbb{F}_q^m$ it holds that $|\{\mathbf{c} \in \mathcal{C} : d_{\text{ed}}(\mathbf{c}, \mathbf{y}) \leq \rho n\}| \leq L$.

Our Results

- Any $(\rho, 2\rho n + 1, L)$ -list-recoverable code \mathcal{C} is a (ρ, L) -list-decodable-insdel code.
 - First efficient insdel-list-decoder for $[n, k > 2]$ RS codes!
 - Rate-error tradeoffs for adversarial & probabilistic insdel channels
- Adapted the Koetter-Vardy algorithm for probabilistic insdel channel [\[Davey and MacKay '01\]](#)
 - also for jointly decoding multiple received sequences

Introduction

Decoding via List Recovery

Adversarial Insdels

Probabilistic Insdels

Adapting Koetter-Vardy Algorithm

Conclusion

Correct One Insertion via List Recovery

Example

Consider a $(\rho, \ell = 2, L)$ -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_{q=3}^{n=5}$.

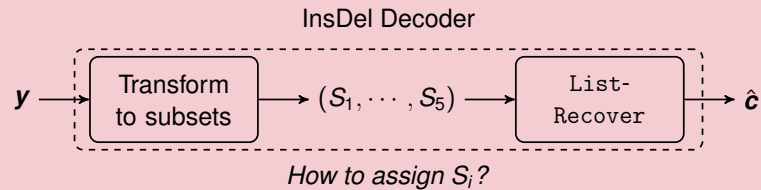
$$\mathbf{c} \in \mathcal{C} \xrightarrow{1 \text{ insertion}} \mathbf{y} = (0, 2, 1, 1, 0, 2)$$

Correct One Insertion via List Recovery

Example

Consider a $(\rho, \ell = 2, L)$ -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_{q=3}^{n=5}$.

$$\mathbf{c} \in \mathcal{C} \xrightarrow{1 \text{ insertion}} \mathbf{y} = (0, 2, 1, 1, 0, 2)$$



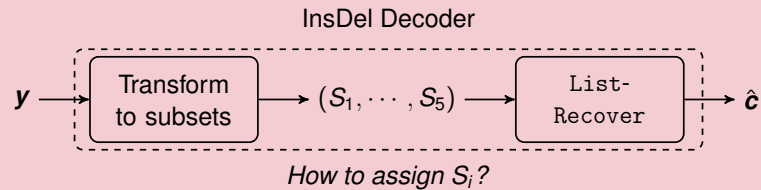
Correct One Insertion via List Recovery

Example

Consider a $(\rho, \ell = 2, L)$ -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_{q=3}^{n=5}$.

$$\mathbf{c} \in \mathcal{C} \xrightarrow{1 \text{ insertion}} \mathbf{y} = (0, 2, 1, 1, 0, 2)$$

$$c_1 \in \{0, 2\}$$



Correct One Insertion via List Recovery

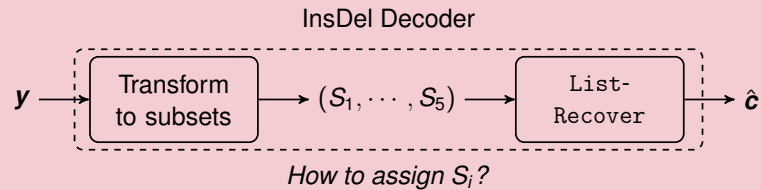
Example

Consider a $(\rho, \ell = 2, L)$ -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_{q=3}^{n=5}$.

$$\mathbf{c} \in \mathcal{C} \xrightarrow{1 \text{ insertion}} \mathbf{y} = (0, 2, 1, 1, 0, 2)$$

$$c_1 \in \{0, 2\}$$

$$c_2 \in \{2, 1\}$$



Correct One Insertion via List Recovery

Example

Consider a $(\rho, \ell = 2, L)$ -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_{q=3}^{n=5}$.

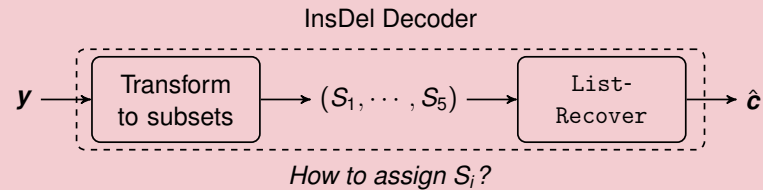
$$\mathbf{c} \in \mathcal{C} \xrightarrow{1 \text{ insertion}} \mathbf{y} = (0, 2, 1, 1, 0, 2)$$

$$c_1 \in \{0, 2\}$$

$$c_2 \in \{2, 1\}$$

$$\vdots$$

$$c_5 \in \{0, 2\}$$



Correct One Insertion via List Recovery

Example

Consider a $(\rho, \ell = 2, L)$ -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_{q=3}^{n=5}$.

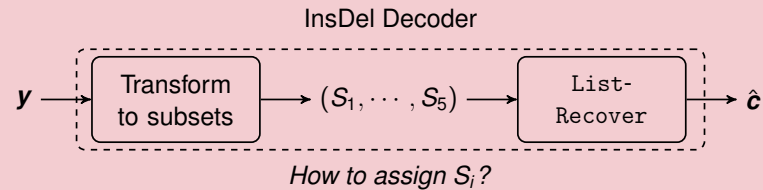
$$\mathbf{c} \in \mathcal{C} \xrightarrow{1 \text{ insertion}} \mathbf{y} = (0, 2, 1, 1, 0, 2)$$

$$\mathbf{c}_1 \in \{0, 2\} \rightarrow S_1$$

$$\mathbf{c}_2 \in \{2, 1\} \rightarrow S_2$$

$$\vdots$$

$$\mathbf{c}_5 \in \{0, 2\} \rightarrow S_5$$



Decoding Algorithm

For a (ρ, ℓ, L) -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_q^n$,

Algorithm: Decode

Input: $(y_1, \dots, y_m), \ell$

Output: Codewords $\mathbf{c} \in \mathcal{C}$

Decoding Algorithm

For a (ρ, ℓ, L) -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_q^n$,

Algorithm: Decode

Input: $(y_1, \dots, y_m), \ell$

Output: Codewords $\mathbf{c} \in \mathcal{C}$

```

1 for  $i \in [n]$  do
2    $S_i \leftarrow \{y_{\max\{1, i-\lfloor \ell/2 \rfloor\}}, \dots, y_{\min\{m, i+\lfloor \ell/2 \rfloor\}}\}$ 

```

Decoding Algorithm

For a (ρ, ℓ, L) -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_q^n$,

Algorithm: Decode

Input: $(y_1, \dots, y_m), \ell$

Output: Codewords $\mathbf{c} \in \mathcal{C}$

- 1 **for** $i \in [n]$ **do**
 - 2 $S_i \leftarrow \{y_{\max\{1, i-\lfloor \ell/2 \rfloor\}}, \dots, y_{\min\{m, i+\lfloor \ell/2 \rfloor\}}\}$
 - 3 **Execute List-Recover** with the lists S_1, \dots, S_n to get $\mathcal{L} \subseteq \mathcal{C}$.
-

Decoding Algorithm

For a (ρ, ℓ, L) -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_q^n$,

Algorithm: Decode

Input: $(y_1, \dots, y_m), \ell$

Output: Codewords $\mathbf{c} \in \mathcal{C}$

- 1 **for** $i \in [n]$ **do**
 - 2 $S_i \leftarrow \{y_{\max\{1, i-\lfloor \ell/2 \rfloor\}}, \dots, y_{\min\{m, i+\lfloor \ell/2 \rfloor\}}\}$
 - 3 Execute List-Recover with the lists S_1, \dots, S_n to get $\mathcal{L} \subseteq \mathcal{C}$.
 - 4 **return** $\{\mathbf{c} \in \mathcal{L} \mid d_{\text{ed}}(\mathbf{c}, \mathbf{y}) \leq \rho n\}$.
-

Decoding Adversarial Insdels

Theorem

Let $\rho \in [0, 1]$ and set $\ell = 2\rho n + 1$. Assume that $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a (ρ, ℓ, L) -list-recoverable code with an algorithm **List-Recover** that runs in time T .

Decoding Adversarial Insdels

Theorem

Let $\rho \in [0, 1]$ and set $\ell = 2\rho n + 1$. Assume that $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a (ρ, ℓ, L) -list-recoverable code with an algorithm **List-Recover** that runs in time T .

1. Then, running alg. Decode on input $\mathbf{y} \in \mathbb{F}_q^m$ returns a list $\mathcal{L}' \subseteq \mathcal{C}$ such that
 - for every $\mathbf{c} \in \mathcal{L}'$, $d_{\text{ed}}(\mathbf{c}, \mathbf{y}) \leq \rho n$, and
 - $|\mathcal{L}'| \leq L$.

Decoding Adversarial Insdels

Theorem

Let $\rho \in [0, 1]$ and set $\ell = 2\rho n + 1$. Assume that $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a (ρ, ℓ, L) -list-recoverable code with an algorithm **List-Recover** that runs in time T .

1. Then, running alg. **Decode** on input $\mathbf{y} \in \mathbb{F}_q^m$ returns a list $\mathcal{L}' \subseteq \mathcal{C}$ such that
 - for every $\mathbf{c} \in \mathcal{L}'$, $d_{\text{ed}}(\mathbf{c}, \mathbf{y}) \leq \rho n$, and
 - $|\mathcal{L}'| \leq L$.
2. The running time of Alg. **Decode** is $O(T + L \cdot n^2)$.

Decoding Adversarial Insdels

Theorem

Let $\rho \in [0, 1]$ and set $\ell = 2\rho n + 1$. Assume that $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a (ρ, ℓ, L) -list-recoverable code with an algorithm **List-Recover** that runs in time T .

1. Then, running alg. Decode on input $\mathbf{y} \in \mathbb{F}_q^m$ returns a list $\mathcal{L}' \subseteq \mathcal{C}$ such that
 - for every $\mathbf{c} \in \mathcal{L}'$, $d_{\text{ed}}(\mathbf{c}, \mathbf{y}) \leq \rho n$, and
 - $|\mathcal{L}'| \leq L$.
2. The running time of Alg. Decode is $O(T + L \cdot n^2)$.
3. Moreover, if $\rho n \leq \lfloor \frac{d_{\text{ed}}(\mathcal{C})-1}{2} \rfloor$, then $|\mathcal{L}'| \leq 1$.

Reed-Solomon Codes

- Efficiently list-recoverable!

Definition

Let $\alpha_0, \dots, \alpha_{n-1} \in \mathbb{F}_q$ be distinct. An $[n, k]_q$ *Reed-Solomon (RS) code* is defined as

$$\mathcal{RS}(n, k)_q = \{(f(\alpha_0), \dots, f(\alpha_{n-1})) \mid f \in \mathbb{F}_q[x], \deg(f) < k\}.$$

Reed-Solomon Codes

- Efficiently list-recoverable!

Definition

Let $\alpha_0, \dots, \alpha_{n-1} \in \mathbb{F}_q$ be distinct. An $[n, k]_q$ *Reed-Solomon (RS) code* is defined as

$$\mathcal{RS}(n, k)_q = \{(f(\alpha_0), \dots, f(\alpha_{n-1})) \mid f \in \mathbb{F}_q[x], \deg(f) < k\}.$$

Corollary (Guruswami-Sudan Decoder)

Let $\varepsilon > 0$ and \mathcal{C} be an $[n, k]_q$ RS code that corrects from t insdels where

$$t \leq n - \sqrt{(1 + \varepsilon) \cdot kn \cdot (2t + 1)}. \quad (1)$$

Then, \mathcal{C} has a deterministic unique-decoding algorithm that **corrects t insdels in time $O(n^3 \varepsilon^{-6})$** .

Reed-Solomon Codes

- Efficiently list-recoverable!

Definition

Let $\alpha_0, \dots, \alpha_{n-1} \in \mathbb{F}_q$ be distinct. An $[n, k]_q$ *Reed-Solomon (RS) code* is defined as

$$\mathcal{RS}(n, k)_q = \{(f(\alpha_0), \dots, f(\alpha_{n-1})) \mid f \in \mathbb{F}_q[x], \deg(f) < k\}.$$

Corollary (Guruswami-Sudan Decoder)

Let $\varepsilon > 0$ and \mathcal{C} be an $[n, k]_q$ RS code that corrects from t insdels where

$$t \leq n - \sqrt{(1 + \varepsilon) \cdot kn \cdot (2t + 1)}. \quad (1)$$

Then, \mathcal{C} has a deterministic unique-decoding algorithm that **corrects t insdels in time $O(n^3 \varepsilon^{-6})$** .

- **Note:** (1) requires $k \cdot t = O(n)$.

Introduction

Decoding via List Recovery

Adversarial Insdels

Probabilistic Insdels

Adapting Koetter-Vardy Algorithm

Conclusion

Probabilistic Deletion Channel

- Deletes each transmitted symbol independently with probability $P_d \in (0, 1)$.

Probabilistic Deletion Channel

- Deletes each transmitted symbol independently with probability $P_d \in (0, 1)$.
- How to assign the subsets S_i for List-Recover?

Probabilistic Deletion Channel

- Deletes each transmitted symbol independently with probability $P_d \in (0, 1)$.
- How to assign the subsets S_i for List-Recover?
 - I.e., if \mathbf{c} is transmitted, in which size- ℓ window of \mathbf{y} is c_i most likely to appear?

Probabilistic Deletion Channel

- Deletes each transmitted symbol independently with probability $P_d \in (0, 1)$.
- How to assign the subsets S_i for List-Recover?
 - I.e., if \mathbf{c} is transmitted, in which size- ℓ window of \mathbf{y} is c_i most likely to appear?
 - *Hint:* i symbols transmitted $\rightarrow (1 - P_d)i$ symbols received on average.

Probabilistic Deletion Channel

- Deletes each transmitted symbol independently with probability $P_d \in (0, 1)$.
- How to assign the subsets S_i for List-Recover?
 - I.e., if \mathbf{c} is transmitted, in which size- ℓ window of \mathbf{y} is c_i most likely to appear?
 - *Hint:* i symbols transmitted $\rightarrow (1 - P_d)i$ symbols received on average.
- For a (ρ, ℓ, L) -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_q^n$,

Algorithm: Decode

Probabilistic Deletion Channel

- Deletes each transmitted symbol independently with probability $P_d \in (0, 1)$.
- How to assign the subsets S_i for List-Recover?
 - I.e., if \mathbf{c} is transmitted, in which size- ℓ window of \mathbf{y} is c_i most likely to appear?
 - *Hint:* i symbols transmitted $\rightarrow (1 - P_d)i$ symbols received on average.
- For a (ρ, ℓ, L) -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_q^n$,

Algorithm: Decode

Input: $(y_1, \dots, y_m), \ell, n$

Output: Codewords $\mathbf{c} \in \mathcal{C}$

Probabilistic Deletion Channel

- Deletes each transmitted symbol independently with probability $P_d \in (0, 1)$.
- How to assign the subsets S_i for List-Recover?
 - I.e., if \mathbf{c} is transmitted, in which size- ℓ window of \mathbf{y} is c_i most likely to appear?
 - *Hint:* i symbols transmitted $\rightarrow (1 - P_d)i$ symbols received on average.
- For a (ρ, ℓ, L) -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_q^n$,

Algorithm: Decode

Input: $(y_1, \dots, y_m), \ell, n$

Output: Codewords $\mathbf{c} \in \mathcal{C}$

```

1 for  $i \in [n]$  do
2    $S_i \leftarrow \{y_{\max\{1, (1-P_d)i-\ell/2\}}, \dots, y_{\min\{m, (1-P_d)i+\ell/2\}}\}$ 
  
```

Probabilistic Deletion Channel

- Deletes each transmitted symbol independently with probability $P_d \in (0, 1)$.
- How to assign the subsets S_i for List-Recover?
 - I.e., if \mathbf{c} is transmitted, in which size- ℓ window of \mathbf{y} is c_i most likely to appear?
 - *Hint:* i symbols transmitted $\rightarrow (1 - P_d)i$ symbols received on average.
- For a (ρ, ℓ, L) -list-recoverable code $\mathcal{C} \subseteq \mathbb{F}_q^n$,

Algorithm: Decode

Input: $(y_1, \dots, y_m), \ell, n$

Output: Codewords $\mathbf{c} \in \mathcal{C}$

```

1 for  $i \in [n]$  do
2    $S_i \leftarrow \{y_{\max\{1, (1-P_d)i-\ell/2\}}, \dots, y_{\min\{m, (1-P_d)i+\ell/2\}}\}$ 
3 Execute List-Recover with the lists  $S_1, \dots, S_n$  to get  $\mathcal{L} \subseteq \mathcal{C}$ .
4 return  $\{\mathbf{c} \in \mathcal{L} \mid d_{\text{ed}}(\mathbf{c}, \mathbf{y}) \leq \rho n\}$ .
```

Probabilistic Deletions

Theorem

Let $P_d \in (0, 1)$, $\varepsilon > 0$ and $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a $(P_d + \varepsilon, n^{1/2+0.001}, L)$ -list-recoverable code with an efficient list recoverable algorithm List-recover.

Probabilistic Deletions

Theorem

Let $P_d \in (0, 1)$, $\varepsilon > 0$ and $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a $(P_d + \varepsilon, n^{1/2+0.001}, L)$ -list-recoverable code with an efficient list recoverable algorithm List-recover.

Say the transmission of $\mathbf{c} \in \mathcal{C}$ over a channel with deletion probability P_d produces $\mathbf{y} \in \mathbb{F}_q^m$.

Probabilistic Deletions

Theorem

Let $P_d \in (0, 1)$, $\varepsilon > 0$ and $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a $(P_d + \varepsilon, n^{1/2+0.001}, L)$ -list-recoverable code with an efficient list recoverable algorithm List-recover.

Say the transmission of $\mathbf{c} \in \mathcal{C}$ over a channel with deletion probability P_d produces $\mathbf{y} \in \mathbb{F}_q^m$.

1. Then, with probability $\exp(-\Omega(n^{0.002}))$, alg. Decode produces a list \mathcal{L} such that $\mathbf{c} \in \mathcal{L}$.

Probabilistic Deletions

Theorem

Let $P_d \in (0, 1)$, $\varepsilon > 0$ and $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a $(P_d + \varepsilon, n^{1/2+0.001}, L)$ -list-recoverable code with an efficient list recoverable algorithm List-recover.

Say the transmission of $\mathbf{c} \in \mathcal{C}$ over a channel with deletion probability P_d produces $\mathbf{y} \in \mathbb{F}_q^m$.

1. Then, with probability $\exp(-\Omega(n^{0.002}))$, alg. Decode produces a list \mathcal{L} such that $\mathbf{c} \in \mathcal{L}$.
2. Moreover, if $(P_d + \varepsilon)n \leq \lfloor \frac{d_{\text{ed}}(\mathcal{C})-1}{2} \rfloor$, then $|\mathcal{L}| = 1$.

Probabilistic Deletions

Theorem

Let $P_d \in (0, 1)$, $\varepsilon > 0$ and $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a $(P_d + \varepsilon, n^{1/2+0.001}, L)$ -list-recoverable code with an efficient list recoverable algorithm List-recover.

Say the transmission of $\mathbf{c} \in \mathcal{C}$ over a channel with deletion probability P_d produces $\mathbf{y} \in \mathbb{F}_q^m$.

1. Then, with probability $\exp(-\Omega(n^{0.002}))$, alg. Decode produces a list \mathcal{L} such that $\mathbf{c} \in \mathcal{L}$.
2. Moreover, if $(P_d + \varepsilon)n \leq \lfloor \frac{d_{\text{ed}}(\mathcal{C})-1}{2} \rfloor$, then $|\mathcal{L}| = 1$.

- Unique, efficient decoding (with high probability) for any $P_d \in (0, 1)$, needs $k = O(n^{1/2-0.001})$.
 - Better rate-error tradeoff than the adversarial setting: $k \cdot t = O(n)$

Probabilistic Deletions

Theorem

Let $P_d \in (0, 1)$, $\varepsilon > 0$ and $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a $(P_d + \varepsilon, n^{1/2+0.001}, L)$ -list-recoverable code with an efficient list recoverable algorithm List-recover.

Say the transmission of $\mathbf{c} \in \mathcal{C}$ over a channel with deletion probability P_d produces $\mathbf{y} \in \mathbb{F}_q^m$.

1. Then, with probability $\exp(-\Omega(n^{0.002}))$, alg. Decode produces a list \mathcal{L} such that $\mathbf{c} \in \mathcal{L}$.
2. Moreover, if $(P_d + \varepsilon)n \leq \lfloor \frac{d_{\text{ed}}(\mathcal{C})-1}{2} \rfloor$, then $|\mathcal{L}| = 1$.

- Unique, efficient decoding (with high probability) for any $P_d \in (0, 1)$, needs $k = O(n^{1/2-0.001})$.
 - Better rate-error tradeoff than the adversarial setting: $k \cdot t = O(n)$
 - Similar result for a probabilistic insdel channel! [Davey and MacKay '01]

Introduction

Decoding via List Recovery

Adversarial Insdels

Probabilistic Insdels

Adapting Koetter-Vardy Algorithm

Conclusion

Koetter-Vardy Algorithm

- Soft-decision decoder for RS codes [[Koetter and Vardy '03](#)]

Koetter-Vardy Algorithm

- Soft-decision decoder for RS codes [\[Koetter and Vardy '03\]](#)
 - Recall: $\mathcal{RS}(n, k)_q = \{(f(\alpha_0), \dots, f(\alpha_{n-1})) \mid f \in \mathbb{F}_q[x], \deg(f) < k\}$,

Koetter-Vardy Algorithm

- Soft-decision decoder for RS codes [\[Koetter and Vardy '03\]](#)
 - Recall: $\mathcal{RS}(n, k)_q = \{(f(\alpha_0), \dots, f(\alpha_{n-1})) \mid f \in \mathbb{F}_q[x], \deg(f) < k\}$,
 - [Decoding task](#): Find best f that fits $(f(\alpha_0), \dots, f(\alpha_{n-1}))$ best to \mathbf{y} .

Koetter-Vardy Algorithm

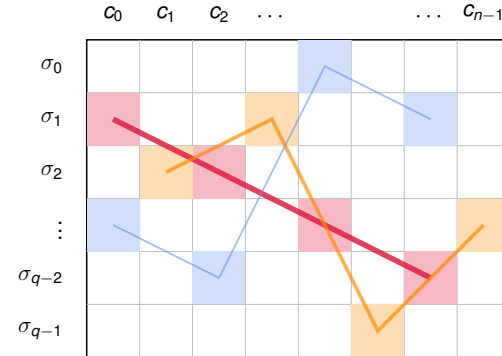
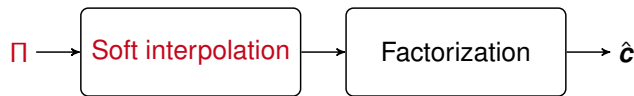
- Soft-decision decoder for RS codes [Koetter and Vardy '03]
 - Recall: $\mathcal{RS}(n, k)_q = \{(f(\alpha_0), \dots, f(\alpha_{n-1})) \mid f \in \mathbb{F}_q[x], \deg(f) < k\}$,
 - **Decoding task**: Find best f that fits $(f(\alpha_0), \dots, f(\alpha_{n-1}))$ best to \mathbf{y} .
- **Reliability matrix** $\Pi \in (0, 1)^{q \times n}$ incorporates soft information on the transmitted symbols.

Koetter-Vardy Algorithm

- Soft-decision decoder for RS codes [Koetter and Vardy '03]
 - Recall: $\mathcal{RS}(n, k)_q = \{(f(\alpha_0), \dots, f(\alpha_{n-1})) \mid f \in \mathbb{F}_q[x], \deg(f) < k\}$,
 - **Decoding task**: Find best f that fits $(f(\alpha_0), \dots, f(\alpha_{n-1}))$ best to \mathbf{y} .
- **Reliability matrix** $\Pi \in (0, 1)^{q \times n}$ incorporates soft information on the transmitted symbols.
 - If $\mathbb{F}_q = \{\sigma_0, \dots, \sigma_{q-1}\}$, then for received vector $\mathbf{y} \in \mathbb{F}_q^m$, $\pi_{i,j} = \Pr[c_j = \sigma_i | \mathbf{y}]$.

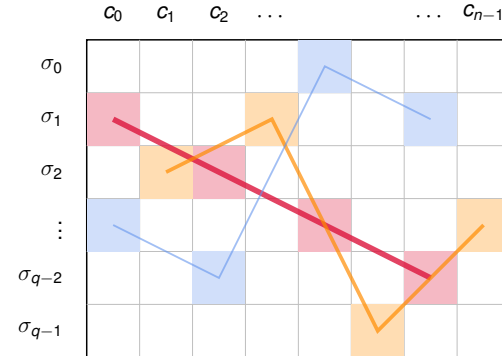
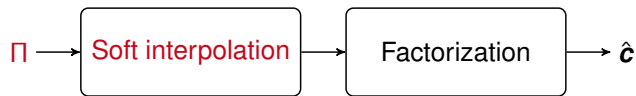
Koetter-Vardy Algorithm

- Soft-decision decoder for RS codes [Koetter and Vardy '03]
 - Recall: $\mathcal{RS}(n, k)_q = \{(f(\alpha_0), \dots, f(\alpha_{n-1})) \mid f \in \mathbb{F}_q[x], \deg(f) < k\}$,
 - **Decoding task**: Find best f that fits $(f(\alpha_0), \dots, f(\alpha_{n-1}))$ best to \mathbf{y} .
- **Reliability matrix** $\Pi \in (0, 1)^{q \times n}$ incorporates soft information on the transmitted symbols.
 - If $\mathbb{F}_q = \{\sigma_0, \dots, \sigma_{q-1}\}$, then for received vector $\mathbf{y} \in \mathbb{F}_q^m$, $\pi_{i,j} = \Pr[c_j = \sigma_i | \mathbf{y}]$.



Koetter-Vardy Algorithm

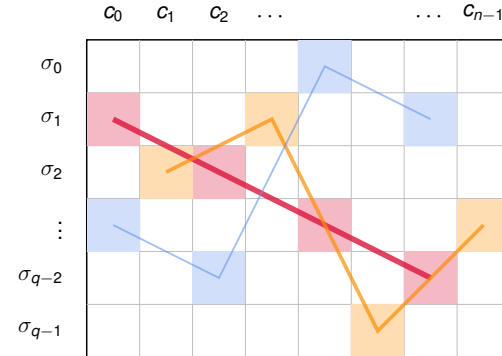
- Soft-decision decoder for RS codes [Koetter and Vardy '03]
 - Recall: $\mathcal{RS}(n, k)_q = \{(f(\alpha_0), \dots, f(\alpha_{n-1})) \mid f \in \mathbb{F}_q[x], \deg(f) < k\}$,
 - **Decoding task**: Find best f that fits $(f(\alpha_0), \dots, f(\alpha_{n-1}))$ best to \mathbf{y} .
- **Reliability matrix** $\Pi \in (0, 1)^{q \times n}$ incorporates soft information on the transmitted symbols.
 - If $\mathbb{F}_q = \{\sigma_0, \dots, \sigma_{q-1}\}$, then for received vector $\mathbf{y} \in \mathbb{F}_q^m$, $\pi_{i,j} = \Pr[c_j = \sigma_i | \mathbf{y}]$.



- We compute Π for the Davey-MacKay channel given $\mathbf{y}_1, \dots, \mathbf{y}_M$!

Koetter-Vardy Algorithm

- Soft-decision decoder for RS codes [Koetter and Vardy '03]
 - Recall: $\mathcal{RS}(n, k)_q = \{(f(\alpha_0), \dots, f(\alpha_{n-1})) \mid f \in \mathbb{F}_q[x], \deg(f) < k\}$,
 - **Decoding task**: Find best f that fits $(f(\alpha_0), \dots, f(\alpha_{n-1}))$ best to \mathbf{y} .
- **Reliability matrix** $\Pi \in (0, 1)^{q \times n}$ incorporates soft information on the transmitted symbols.
 - If $\mathbb{F}_q = \{\sigma_0, \dots, \sigma_{q-1}\}$, then for received vector $\mathbf{y} \in \mathbb{F}_q^m$, $\pi_{i,j} = \Pr[c_j = \sigma_i | \mathbf{y}]$.



- We compute Π for the Davey-MacKay channel given $\mathbf{y}_1, \dots, \mathbf{y}_M$!
 - *Joint decoding*: complexity grows linearly in M .

Davey-MacKay Channel

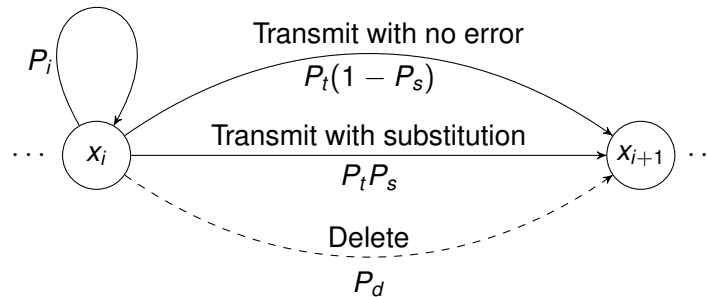
- Induces random insertions, deletions and substitutions [\[Davey and MacKay '01\]](#)

Davey-MacKay Channel

- Induces random insertions, deletions and substitutions [\[Davey and MacKay '01\]](#)
- Let channel input be $\mathbf{x} = (x_1, \dots, x_T)$.
 - When x_i awaits transmission, four events possible.

Davey-MacKay Channel

- Induces random insertions, deletions and substitutions [\[Davey and MacKay '01\]](#)
- Let channel input be $\mathbf{x} = (x_1, \dots, x_T)$.
 - When x_i awaits transmission, four events possible.

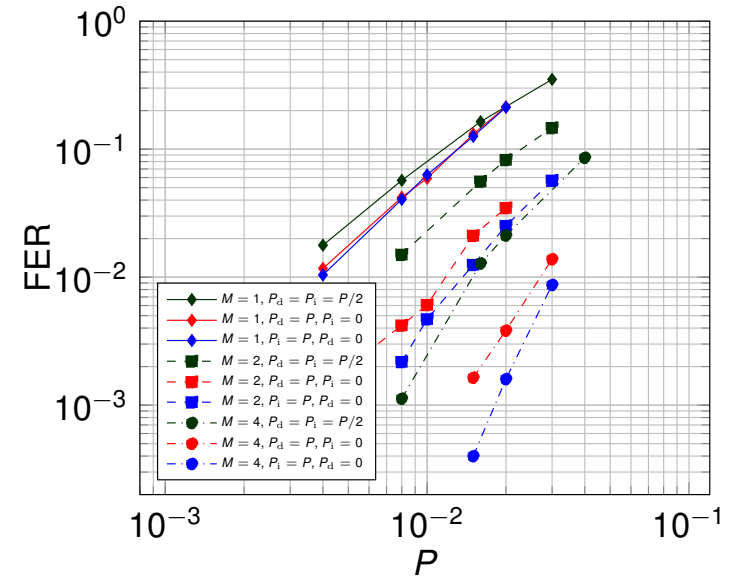


Simulation Results

- Primitive $\mathcal{RS}(100, 33)$ over \mathbb{F}_{101}
 - But eval. points randomly permuted. [\[Beelen *et al.* '25\]](#)
- List size set to 5.

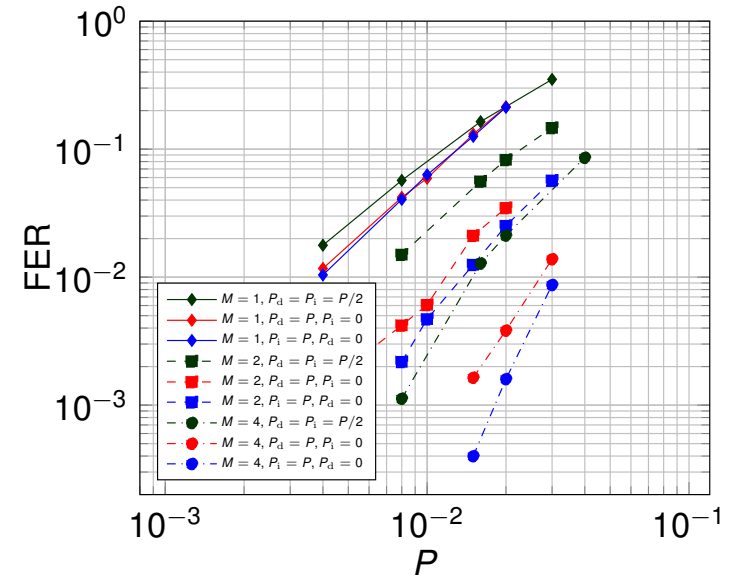
Simulation Results

- Primitive $\mathcal{RS}(100, 33)$ over \mathbb{F}_{101}
 - But eval. points randomly permuted. [\[Beelen et al. '25\]](#)
- List size set to 5.



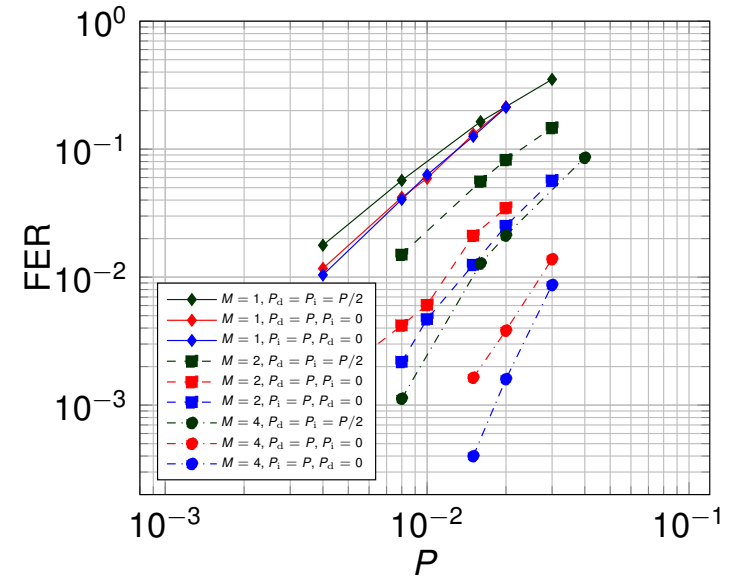
Simulation Results

- Primitive $\mathcal{RS}(100, 33)$ over \mathbb{F}_{101}
 - But eval. points randomly permuted. [Beelen *et al.* '25]
- List size set to 5.
- Observations:
 - Deletions harder to correct than insertions.



Simulation Results

- Primitive $\mathcal{RS}(100, 33)$ over \mathbb{F}_{101}
 - But eval. points randomly permuted. [Beelen *et al.* '25]
- List size set to 5.
- Observations:
 - Deletions harder to correct than insertions.
 - As M increases, FER decreases.



Introduction

Decoding via List Recovery

Adversarial Insdels

Probabilistic Insdels

Adapting Koetter-Vardy Algorithm

Conclusion

Conclusion

Results

- Showed that any $(\rho, 2\rho n + 1, L)$ -list-recoverable code \mathcal{C} is a (ρ, L) -list decodable-insdel code.
 - First efficient insdel decoder for $[n, k]$ RS codes for $k > 2$!
 - Better rate-error tradeoff for the probabilistic model.
- Adapted the Koetter-Vardy algorithm for insdels for $M \geq 1$ received sequences

Conclusion

Results

- Showed that any $(\rho, 2\rho n + 1, L)$ -list-recoverable code \mathcal{C} is a (ρ, L) -list decodable-insdel code.
 - First efficient insdel decoder for $[n, k]$ RS codes for $k > 2!$
 - Better rate-error tradeoff for the probabilistic model.
- Adapted the Koetter-Vardy algorithm for insdels for $M \geq 1$ received sequences

Future work

- Alternant codes, folded RS codes..

Conclusion

Results

- Showed that any $(\rho, 2\rho n + 1, L)$ -list-recoverable code \mathcal{C} is a (ρ, L) -list decodable-insdel code.
 - First efficient insdel decoder for $[n, k]$ RS codes for $k > 2$!
 - Better rate-error tradeoff for the probabilistic model.
- Adapted the Koetter-Vardy algorithm for insdels for $M \geq 1$ received sequences

Future work

- Alternant codes, folded RS codes..

Thank you!



European
Innovation
Council



Funded by
the European Union

References I

- [1] G. M. Church, Y. Gao, and S. Kosuri, “Next-generation digital information storage in dna,” *Science*, vol. 337, no. 6102, pp. 1628–1628, Sep. 2012.
- [2] N. Goldman *et al.*, “Towards practical, high-capacity, low-maintenance information storage in synthesized dna,” *Nature*, vol. 494, no. 7435, pp. 77–80, Feb. 2013.
- [3] V. Guruswami, “Algorithmic results in list decoding,” *Foundations and Trends® in Theoretical Computer Science*, vol. 2, no. 2, pp. 107–195, 2006.
- [4] B. Haeupler and A. Shahrasbi, “Synchronization strings: Codes for insertions and deletions approaching the Singleton bound,” in *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, ACM, 2017, pp. 33–46.
- [5] R. Safavi-Naini and Y. Wang, “Traitor tracing for shortened and corrupted fingerprints,” in *ACM workshop on Digital Rights Management*, Springer, 2002, pp. 81–100.
- [6] Y. Wang, L. McAven, and R. Safavi-Naini, “Deletion correcting using generalized Reed-Solomon codes,” in *Coding, Cryptography and Combinatorics*, Springer, 2004, pp. 345–358.

References II

- [7] D. Tonien and R. Safavi-Naini, “Construction of deletion correcting codes using generalized Reed–Solomon codes and their subcodes,” *Designs, Codes and Cryptography*, vol. 42, no. 2, pp. 227–237, 2007.
- [8] T. D. Duc, S. Liu, I. Tjuawinata, and C. Xing, “Explicit constructions of two-dimensional Reed-Solomon codes in high insertion and deletion noise regime,” *IEEE Transactions on Information Theory*, vol. 67, no. 5, pp. 2808–2820, 2021.
- [9] S. Liu and I. Tjuawinata, “On 2-dimensional insertion-deletion Reed-Solomon codes with optimal asymptotic error-correcting capability,” *Finite Fields and Their Applications*, vol. 73, p. 101 841, 2021.
- [10] R. Con, A. Shpilka, and I. Tamo, “Reed–Solomon codes against adversarial insertions and deletions,” *IEEE Transactions on Information Theory*, 2023.
- [11] J. Liu, “Optimal RS codes and GRS codes against adversarial insertions and deletions and optimal constructions,” *IEEE Transactions on Information Theory*, 2024.
- [12] R. Con, Z. Guo, R. Li, and Z. Zhang, “Random reed-solomon codes achieve the half-singleton bound for insertions and deletions over linear-sized alphabets,” *arXiv preprint arXiv:2407.07299*, 2024.
- [13] S. Singhvi, “Optimally decoding two-dimensional reed-solomon codes up to the half-singleton bound,” *arXiv preprint arXiv:2412.20771*, 2024.

References III

- [14] R. Con, A. Shpilka, and I. Tamo, “Optimal two-dimensional reed–solomon codes correcting insertions and deletions,” *IEEE Transactions on Information Theory*, 2024.
- [15] M. Davey and D. MacKay, “Reliable communication over channels with insertions, deletions, and substitutions,” *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 687–698, Feb. 2001.
- [16] R. Koetter and A. Vardy, “Algebraic soft-decision decoding of reed-solomon codes,” *IEEE Transactions on Information Theory*, vol. 49, no. 11, pp. 2809–2825, Nov. 2003.
- [17] P. Beelen, R. Con, A. Gruica, M. Montanucci, and E. Yaakobi, *Reed-solomon codes against insertions and deletions: Full-length and rate- $\frac{1}{2}$ codes*, Jan. 2025. arXiv: 2501.11371 [cs].