List-decodable codes for the Z–channel

2022 IEEE International Symposium on Information Theory / June 2022

Nikita Polyanskii

nikitapolyansky@gmail.com

Yihan Zhang

zephyr.z798@gmail.com

This talk is about…

This talk is about…

… codes with large asymmetric list-decoding radius

This talk is about…

… codes with large asymmetric list-decoding radius

1. Code = set of binary words of length $\boldsymbol{n}$
2. “Adversarial” Z-channel injects up to $\boldsymbol{n\tau}$ asymmetric errors to codeword
3. Decoding radius for list size $\boldsymbol{L-1}$ is the maximum $\boldsymbol{R} > \boldsymbol{0}$ such that any Z-ball with radius $\boldsymbol{R}$ contains $< \boldsymbol{L}$ codewords

This talk is about…

… codes with large asymmetric list-decoding radius

1. Code = set of binary words of length $\boldsymbol{n}$
2. "Adversarial" Z-channel injects up to $\boldsymbol{n\tau}$ asymmetric errors to codeword
3. Decoding radius for list size $\boldsymbol{L-1}$ is the maximum $\boldsymbol{R > 0}$ such that any Z-ball with radius $\boldsymbol{R}$ contains $< \boldsymbol{L}$ codewords

Main result (Informal):

- Largest list-decodable code $\boldsymbol{\varepsilon}$-above the *Plotkin point* has size of order $\boldsymbol{\varepsilon^{-3/2}}$ *irrespective* of list size

This talk is about…

… codes with large asymmetric list-decoding radius

1. Code = set of binary words of length $\boldsymbol{n}$
2. "Adversarial" Z-channel injects up to $\boldsymbol{n\tau}$ asymmetric errors to codeword
3. Decoding radius for list size $\boldsymbol{L-1}$ is the maximum $\boldsymbol{R>0}$ such that any Z-ball with radius $\boldsymbol{R}$ contains $<\boldsymbol{L}$ codewords

fraction of errors $\boldsymbol{\tau=\varepsilon+L^{-\frac{1}{L-1}}-L^{-\frac{L}{L-1}}}$

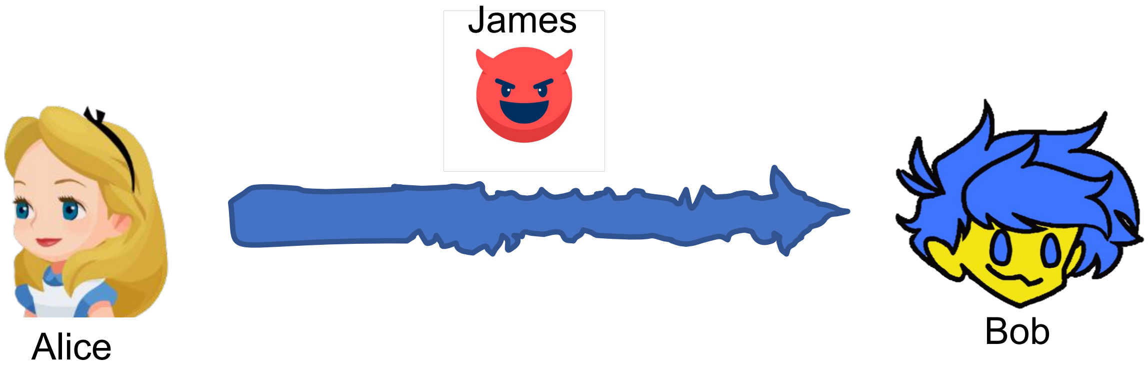
Main result (Informal):

- Largest list-decodable code ε-above the *Plotkin point* has size of order $\boldsymbol{\varepsilon^{-3/2}}$ *irrespective* of list size

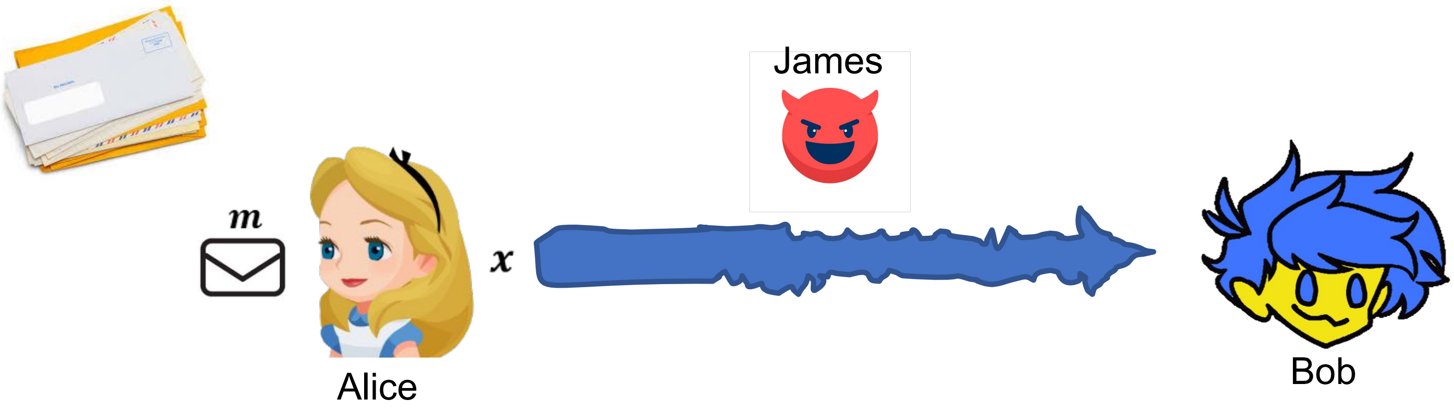
Outline

Introduction	Construction
Converse bound	Conclusion

List-decoding for adversarial channel

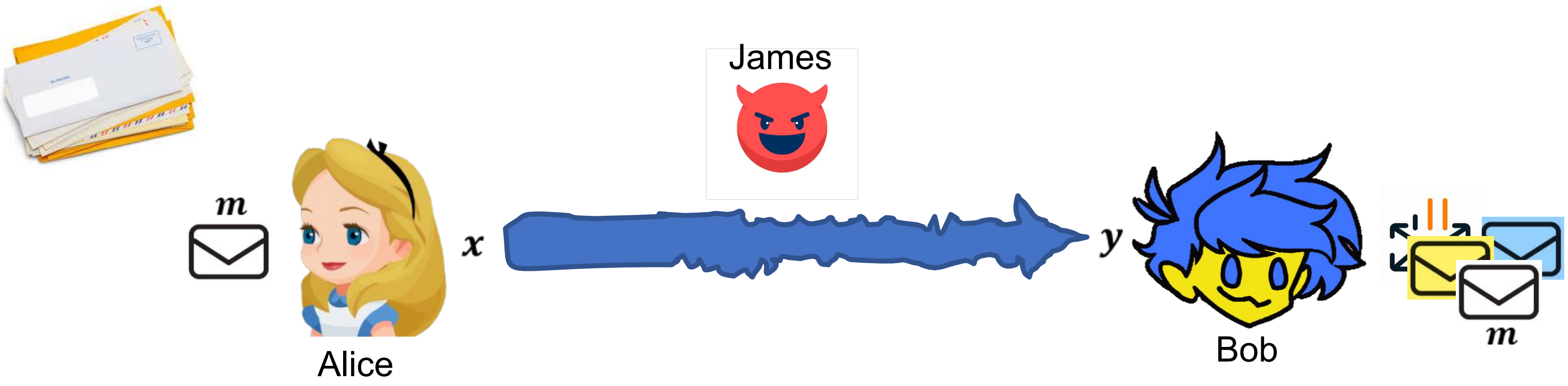


List-decoding for adversarial channel



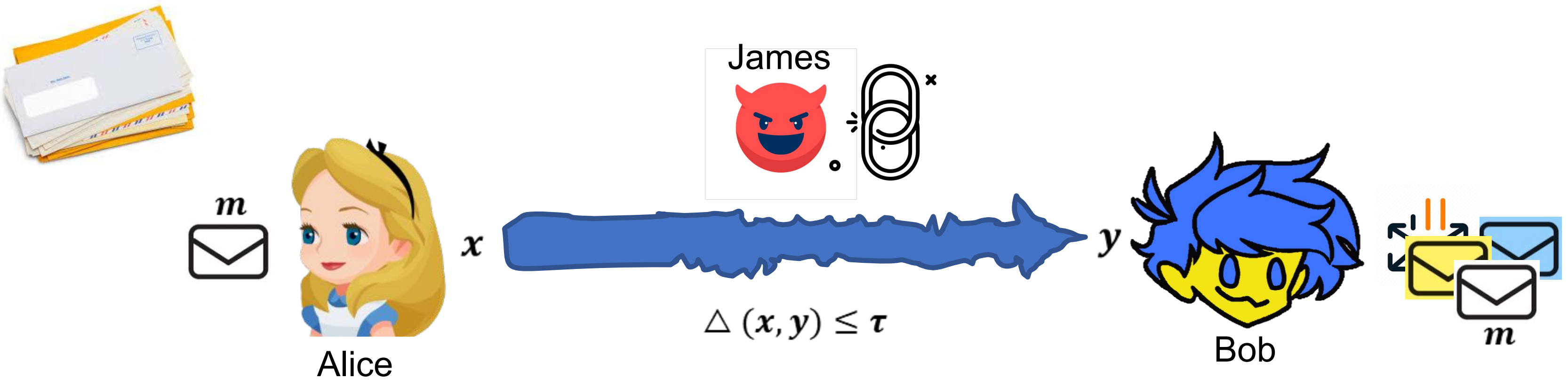
- Alice picks a message m, encode it to x and transmit x over the noisy channel

List-decoding for adversarial channel



- Alice picks a message $\boldsymbol{m}$, encode it to $\boldsymbol{x}$ and transmit $\boldsymbol{x}$ over the noisy channel
- Bob's goal is, based on $\boldsymbol{y}$, to reconstruct a list of messages of size $< \boldsymbol{L}$, which includes $\boldsymbol{m}$

List-decoding for adversarial channel



- Alice picks a message m, encode it to x and transmit x over the noisy channel
- Bob's goal is, based on y, to reconstruct a list of messages of size $< L$, which includes m
- James can inflict to the codeword only a fraction τ of errors

List-decodable codes for Z-channel

$$\boldsymbol{x} = (x_1, \dots, x_n)$$

$$\downarrow$$

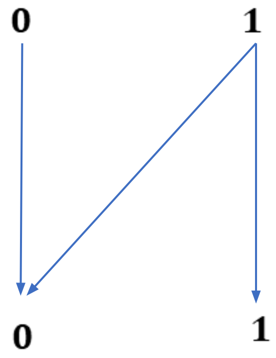
$$\boldsymbol{y} = (y_1, \dots, y_n)$$

List-decodable codes for Z-channel

$$x = (x_1, \dots, x_n)$$

$$\downarrow$$

$$y = (y_1, \dots, y_n)$$

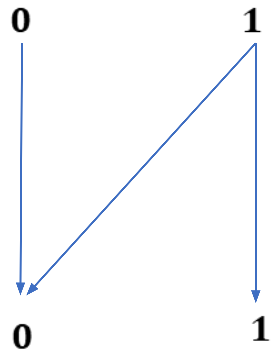


List-decodable codes for Z-channel

$$\boldsymbol{x} = (x_1, \dots, x_n)$$

$$\downarrow$$

$$\boldsymbol{y} = (y_1, \dots, y_n)$$

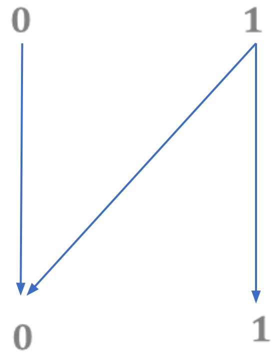


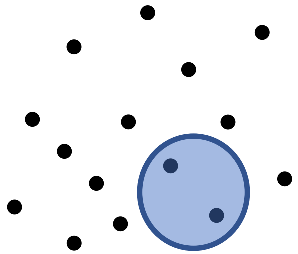
$\triangle(\boldsymbol{x}, \boldsymbol{y}) \le \boldsymbol{\tau}$, the number of positions where 1 changed to 0 is at most $\boldsymbol{\tau n}$

List-decodable codes for Z-channel

$x = (x_1, \dots, x_n)$

$y = (y_1, \dots, y_n)$





any Z-ball contains $< L$ codewords

$\triangle(x, y) \le \tau$, the number of positions where 1 changed to 0 is at most τn

Definition:

- $C \subseteq \{0,1\}^n$ is a $(\tau, L-1)$-list decodable code if for any word $y \in \{0,1\}^n$, the Z-ball centered at y with radius τn contains $< L$ codewords.

Related works

- Bit-flip errors

Theorem (Blinovsky`86, Polyanskiy`16, ABP`18, ZBJ`20)

1. For $L = 2k, 2k+1$, exponential-sized $(\tau, L-1)$-list-decodable codes exist when
$$\tau < \frac{1}{2} - 2^{-(2k+1)}\binom{2k}{k}$$
2. For $\tau = \varepsilon + \frac{1}{2} - 2^{-(2k+1)}\binom{2k}{k}$, the largest $(\tau, L-1)$-list-decodable code has size
$$\begin{cases} \Theta(\varepsilon^{-1}) \text{ for even } L \\ \Theta(\varepsilon^{-3/2}) \text{ for } L = 3 \end{cases}$$

Related works

- Asymmetric errors (Z-channel)

Theorem (ZBJ`20, LLP`21, DG`21)

Exponential-sized $(\tau, L-1)$-list-decodable codes exist when

$$\tau < L^{-\frac{1}{L-1}} - L^{-\frac{L}{L-1}}$$

Related works

- Asymmetric errors (Z-channel)

Theorem (ZBJ`20, LLP`21, DG`21)

Exponential-sized $(\tau, L-1)$-list-decodable codes exist when

$$\tau < L^{-\frac{1}{L-1}} - L^{-\frac{L}{L-1}}$$

What can we say when $\tau = \varepsilon + L^{-\frac{1}{L-1}} - L^{-\frac{L}{L-1}}$

Constant-weight codes

Consider $\boldsymbol{w}$-constant-weight $(\boldsymbol{\tau}, \boldsymbol{L}-\mathbf{1})$-list-decodable code of size $\boldsymbol{M}$.

Constant-weight codes

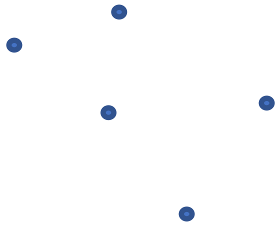
Consider $\boldsymbol{w}$-constant-weight $(\boldsymbol{\tau}, \boldsymbol{L}-\mathbf{1})$-list-decodable code of size $\boldsymbol{M}$.
Define $\boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}) \triangleq \boldsymbol{w}-\boldsymbol{w}^{\boldsymbol{L}}$.

Constant-weight codes

Consider $\boldsymbol{w}$-constant-weight $(\boldsymbol{\tau}, \boldsymbol{L}-\mathbf{1})$-list-decodable code of size $\boldsymbol{M}$.
Define $\boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}) \triangleq \boldsymbol{w} - \boldsymbol{w}^{\boldsymbol{L}}$.

By double counting arguments (distances to center of Z-ball covering each $\boldsymbol{L}$-tuple)

$$\frac{\boldsymbol{M}^{\boldsymbol{L}}}{\boldsymbol{M}(\boldsymbol{M}-\mathbf{1})\ldots(\boldsymbol{M}-\boldsymbol{L}+\mathbf{1})} \geq \frac{\boldsymbol{\tau}}{\boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w})}$$

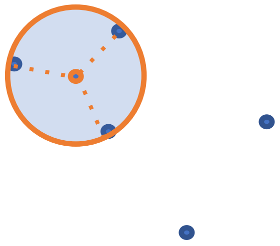


Constant-weight codes

Consider w-constant-weight $(\tau, L-1)$-list-decodable code of size M.
Define $\tau_L(w) \triangleq w - w^L$.

By double counting arguments (distances to center of Z-ball covering each L-tuple)

$$\frac{M^L}{M(M-1)\dots(M-L+1)} \geq \frac{\tau}{\tau_L(w)}$$

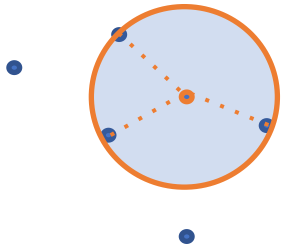


Constant-weight codes

Consider $\boldsymbol{w}$-constant-weight $(\boldsymbol{\tau}, \boldsymbol{L}-\mathbf{1})$-list-decodable code of size $\boldsymbol{M}$.
Define $\boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}) \triangleq \boldsymbol{w} - \boldsymbol{w}^{\boldsymbol{L}}$.

By double counting arguments (distances to center of Z-ball covering each $\boldsymbol{L}$-tuple)

$$\frac{\boldsymbol{M}^{\boldsymbol{L}}}{\boldsymbol{M}(\boldsymbol{M}-\mathbf{1}) \ldots (\boldsymbol{M}-\boldsymbol{L}+\mathbf{1})} \geq \frac{\boldsymbol{\tau}}{\boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w})}$$

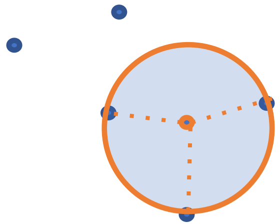


Constant-weight codes

Consider w-constant-weight $(\tau, L-1)$-list-decodable code of size M.
Define $\tau_L(w) \triangleq w - w^L$.

By double counting arguments (distances to center of Z-ball covering each L-tuple)

$$\frac{M^L}{M(M-1)\ldots(M-L+1)} \geq \frac{\tau}{\tau_L(w)}$$

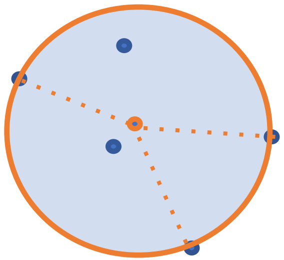


Constant-weight codes

Consider w-constant-weight $(\tau, L-1)$-list-decodable code of size M.
Define $\tau_L(w) \triangleq w - w^L$.

By double counting arguments (distances to center of Z-ball covering each L-tuple)

$$\frac{M^L}{M(M-1)\dots(M-L+1)} \geq \frac{\tau}{\tau_L(w)}$$



Constant-weight codes

Consider w-constant-weight $(\tau, L-1)$-list-decodable code of size M.
Define $\tau_L(w) \triangleq w - w^L$.

By double counting arguments (distances to center of Z-ball covering each L-tuple)

$$\frac{M^L}{M(M-1)\dots(M-L+1)} \geq \frac{\tau}{\tau_L(w)}$$

Lemma:

- Code with $\tau = \varepsilon + \tau_L(w)$ has size $O_L(1/\varepsilon)$

Almost constant-weight codes

Consider almost w-constant-weight $(\tau, L-1)$-list-decodable code of size M.

Almost constant-weight codes

Consider almost w-constant-weight $(\tau, L-1)$-list-decodable code of size M.

weight of each codeword belongs to $(w-\varepsilon, w+\varepsilon)$

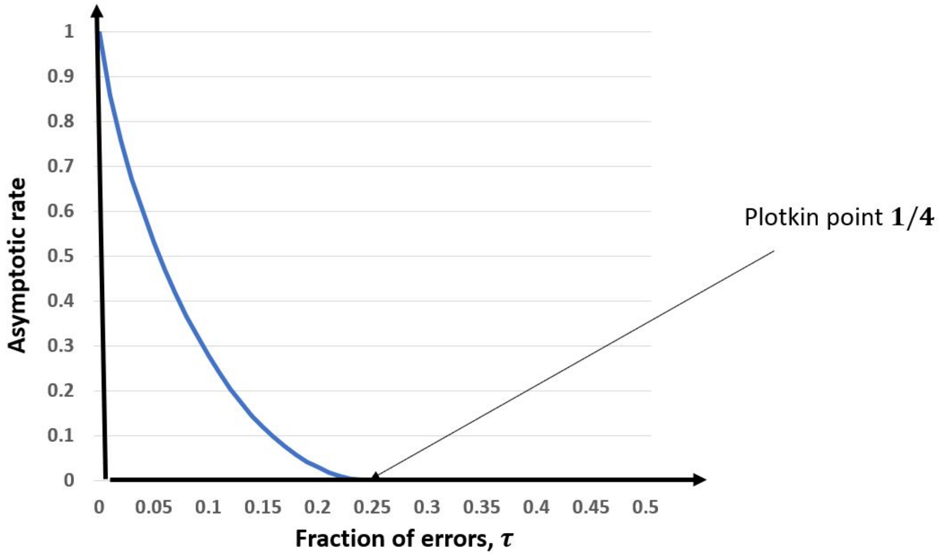
Almost constant-weight codes

Consider almost w-constant-weight $(\tau, L-1)$-list-decodable code of size M.

weight of each codeword belongs to $(w-\varepsilon, w+\varepsilon)$

Lemma:
- Code with $\tau = \varepsilon + \tau_L(w)$ has size $O_L(1/\varepsilon)$

Plotkin point

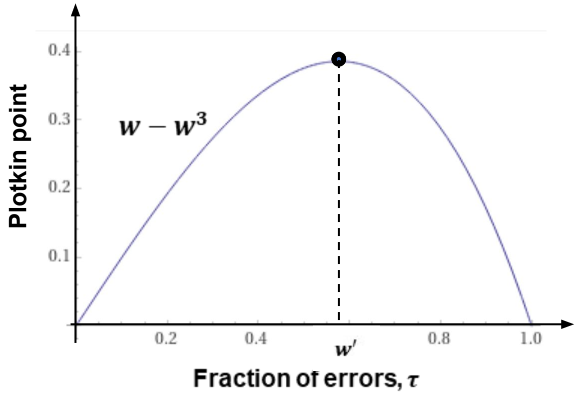


Plotkin point

The Plotkin point for $\boldsymbol{w}$-constant-weight codes for Z-channel is described by $\boldsymbol{\tau_L(w) = w - w^L}$, which is is maximized at $\boldsymbol{w' = L^{-\frac{1}{L-1}}}$.

Plotkin point

The Plotkin point for $\boldsymbol{w}$-constant-weight codes for Z-channel is described by $\boldsymbol{\tau_L(w)} = \boldsymbol{w - w^L}$, which is is maximized at $\boldsymbol{w' = L^{-\frac{1}{L-1}}}$.

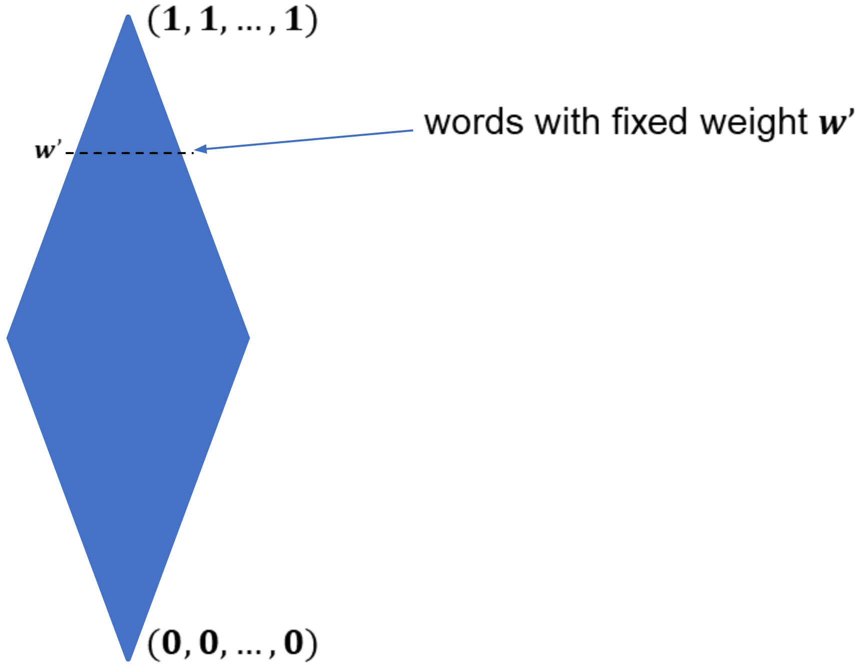


Plotkin point

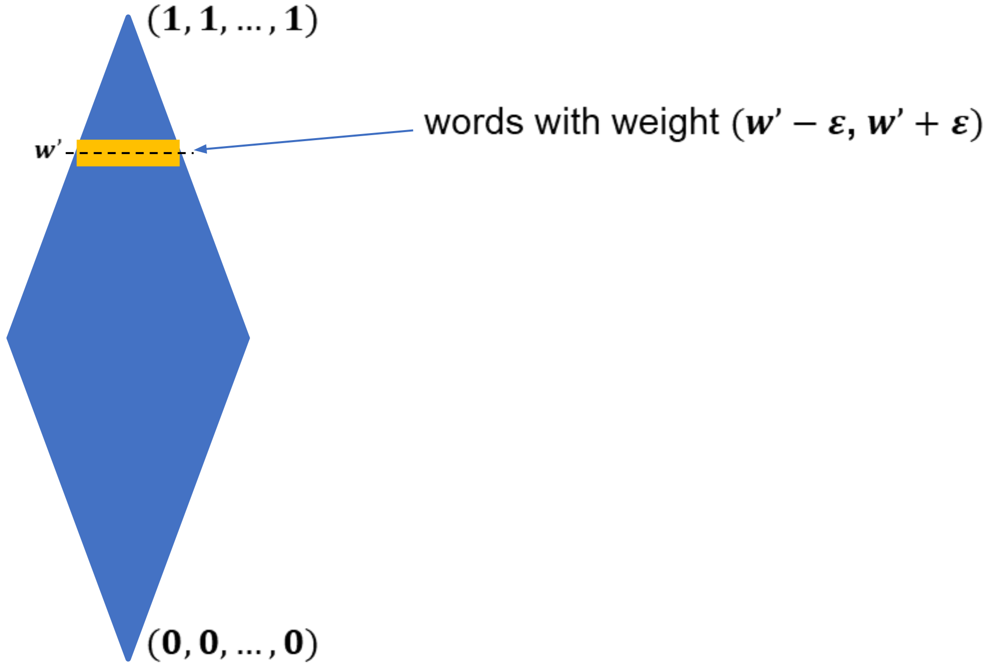
The Plotkin point for $\boldsymbol{w}$-constant-weight codes for Z-channel is described by $\boldsymbol{\tau_L}(\boldsymbol{w}) = \boldsymbol{w} - \boldsymbol{w}^{\boldsymbol{L}}$, which is is maximized at $\boldsymbol{w}' = \boldsymbol{L}^{-\frac{1}{L-1}}$.

Thus, focus on $(\boldsymbol{\tau}, \boldsymbol{L} - \mathbf{1})$-list-decodable codes $\boldsymbol{\varepsilon}$-far from the Plotkin point for Z-channel, i.e. $\boldsymbol{\tau} = \boldsymbol{\varepsilon} + \boldsymbol{\tau_L}(\boldsymbol{w}')$

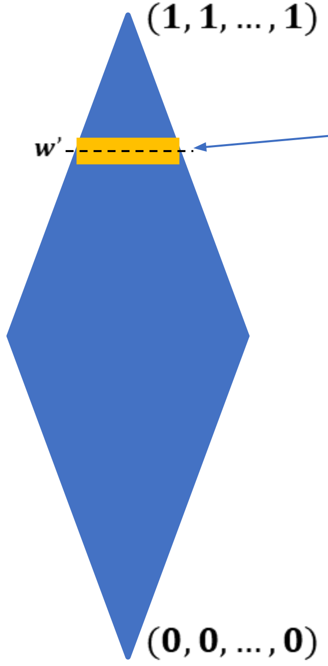
Partition the space



Partition the space



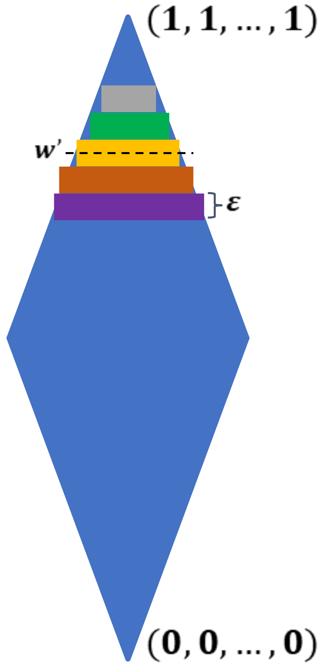
Partition the space



words with weight $(w' - \varepsilon, w' + \varepsilon)$

By Lemma, $O_L(\varepsilon)$ codewords could lie in this slice

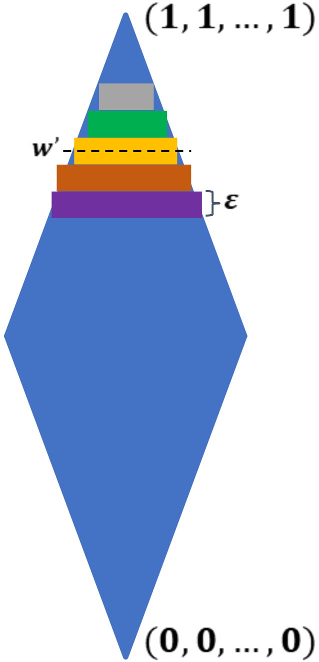
Partition the space



Partition the space into $O(1/\varepsilon)$ slices

Partition the space

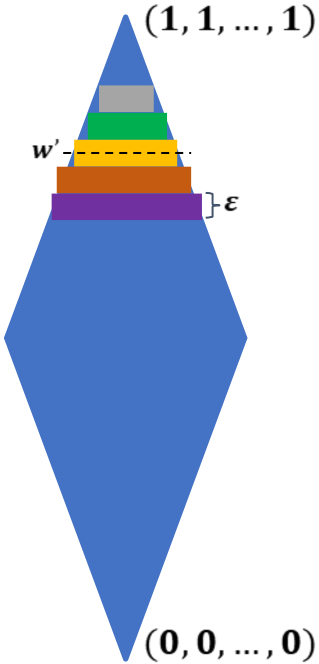
Introduction | Construction | **Converse bound** | Conclusion



Partition the space into $O(1/\varepsilon)$ slices

Each slice contains $O_L(1/\varepsilon)$ codewords

Partition the space

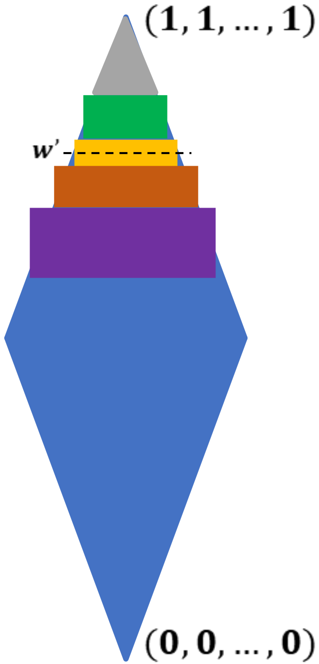


Partition the space into $O(1/\varepsilon)$ slices

Each slice contains $O_L(1/\varepsilon)$ codewords

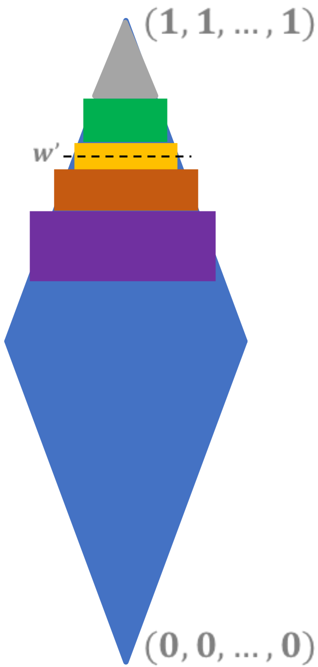
Thus, largest code has size $O_L(1/\varepsilon^2)$

Partition the space



But, this bound can be improved by non-uniform partition!!

Partition the space



But, this bound can be improved by non-uniform partition!!

Theorem:

- Codes with $\boldsymbol{\tau = \varepsilon + \tau_L(w')}$ have size $\boldsymbol{O_L\left(\varepsilon^{-3/2}\right)}$

Constant-weight codes

$$
\left.\begin{array}{ccccccc}
1 & 1 & 1 & 0 & 0 & \dots & 0 \\
1 & 0 & 0 & 1 & 1 & \dots & 0 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & 1 & 0 & 1 & 0 & \dots & 1 \\
0 & 0 & 1 & 0 & 1 & \dots & 1
\end{array}\right\}
$$

$\boldsymbol{m}$ rows
$\boldsymbol{wm}$ ones in each column

Constant-weight codes

1	1	1	0	0	…	0
1	0	0	1	1	…	0
…	…	…	…	…	…	…
0	1	0	1	0	…	1
0	0	1	0	1	…	1

$\boldsymbol{m}$ rows
$\boldsymbol{wm}$ ones in each column

$\binom{m}{wm}$ columns

Constant-weight codes

codewords

$$\underbrace{\begin{matrix} 1 & 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & 1 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 1 & 0 & 1 & 0 & \dots & 1 \\ 0 & 0 & 1 & 0 & 1 & \dots & 1 \end{matrix}}_{\binom{m}{wm} \text{ columns}}$$

$\boldsymbol{m}$ rows
$\boldsymbol{wm}$ ones in each column

Constant-weight codes

codewords

1	1	1	0	0	…	0
1	0	0	1	1	…	0
…	…	…	…	…	…	…
0	1	0	1	0	…	1
0	0	1	0	1	…	1

- $\boldsymbol{w}$-constant-weight code of size $\boldsymbol{m}$ and length $\binom{\boldsymbol{m}}{\boldsymbol{wm}}$

Constant-weight codes

codewords

1	1	1	0	0	…	0
1	0	0	1	1	…	0
…	…	…	…	…	…	…
0	1	0	1	0	…	1
0	0	1	0	1	…	1

- $\boldsymbol{w}$-constant-weight code of size $\boldsymbol{m}$ and length $\binom{\boldsymbol{m}}{\boldsymbol{wm}}$
- $(\boldsymbol{\tau}, \boldsymbol{L}-\mathbf{1})$-list-decodable with $\boldsymbol{\tau} = \boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}) + \boldsymbol{\Omega}(\boldsymbol{m}^{-1})$

Constant-weight codes

codewords

1	1	1	0	0	…	0
1	0	0	1	1	…	0
…	…	…	…	…	…	…
0	1	0	1	0	…	1
0	0	1	0	1	…	1

Lemma:

- Exist w-constant-weight codes with $\tau = \varepsilon + \tau_L(w)$ of size $O_L(\varepsilon^{-1})$

❖ w-constant-weight code of size m and length $\binom{m}{wm}$

❖ $(\tau, L-1)$-list-decodable with $\tau = \tau_L(w) + \Omega(m^{-1})$

Almost constant-weight codes

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

$\boldsymbol{w}'$-constant weight with $\boldsymbol{\tau} = \boldsymbol{\varepsilon} + \boldsymbol{\tau}_{L}(\boldsymbol{w}')$

Almost constant-weight codes

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

$(\boldsymbol{w}' + \boldsymbol{\varepsilon})$-constant weight with $\boldsymbol{\tau} = \boldsymbol{\Omega}(\boldsymbol{\varepsilon}) + \boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}')$

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

$\boldsymbol{w}'$-constant weight with $\boldsymbol{\tau} = \boldsymbol{\varepsilon} + \boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}')$

Almost constant-weight codes

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

$(\boldsymbol{w}' + \boldsymbol{\varepsilon})$-constant weight with $\boldsymbol{\tau} = \boldsymbol{\Omega}(\boldsymbol{\varepsilon}) + \boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}')$

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

$\boldsymbol{w}'$-constant weight with $\boldsymbol{\tau} = \boldsymbol{\varepsilon} + \boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}')$

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

$(\boldsymbol{w}' - \boldsymbol{\varepsilon})$-constant weight with $\boldsymbol{\tau} = \boldsymbol{\Omega}(\boldsymbol{\varepsilon}) + \boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}')$

Almost constant-weight codes

$\Omega(\varepsilon^{-1/2})$ codes

...

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

$(\boldsymbol{w}' + \boldsymbol{\varepsilon})$-constant weight with $\boldsymbol{\tau} = \boldsymbol{\Omega}(\boldsymbol{\varepsilon}) + \boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}')$

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

$\boldsymbol{w}'$-constant weight with $\boldsymbol{\tau} = \boldsymbol{\varepsilon} + \boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}')$

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

$(\boldsymbol{w}' - \boldsymbol{\varepsilon})$-constant weight with $\boldsymbol{\tau} = \boldsymbol{\Omega}(\boldsymbol{\varepsilon}) + \boldsymbol{\tau}_{\boldsymbol{L}}(\boldsymbol{w}')$

...

Almost constant-weight codes

$\Omega(\varepsilon^{-1/2})$ codes

...

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

Repetition + independent permutation

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

Repetition + independent permutation

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

Repetition + independent permutation

...

Almost constant-weight codes

$\Omega(\varepsilon^{-1/2})$ codes

...

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

1	1	1	0	0	...	0
1	0	0	1	1	...	0
...	..	...	..	...	...	...
0	1	0	1	0	...	1
0	0	1	0	1	...	1

...

Theorem:

- Exist codes with $\boldsymbol{\tau} = \boldsymbol{\varepsilon} + \boldsymbol{\tau_L(w')}$ of size $\boldsymbol{O_L\left(\varepsilon^{-3/2}\right)}$

Summary

- Discussed list-decodable codes for the adversarial Z-channel

Summary

- Discussed list-decodable codes for the adversarial Z-channel
- Obtained characterization of codes ε-far from the Plotkin point

Summary

- Discussed list-decodable codes for the adversarial Z-channel
- Obtained characterization of codes $\boldsymbol{\varepsilon}$-far from the Plotkin point
- The length of the proposed code construction is exponential (in $\boldsymbol{\varepsilon}^{-1}$)

Summary

- Discussed list-decodable codes for the adversarial Z-channel
- Obtained characterization of codes $\boldsymbol{\varepsilon}$-far from the Plotkin point
- The length of the proposed code construction is exponential (in $\boldsymbol{\varepsilon}^{-1}$)

  Q: Can be reduced to polynomial by taking random subset of coordinates?

Summary

- Discussed list-decodable codes for the adversarial Z-channel
- Obtained characterization of codes ε-far from the Plotkin point
- The length of the proposed code construction is exponential (in ε^{-1})

Q: Can be reduced to polynomial by taking random subset of coordinates?

++

- Provided bounds on the rate of codes below the Plotkin point

Summary

- Discussed list-decodable codes for the adversarial Z-channel
- Obtained characterization of codes ε-far from the Plotkin point
- The length of the proposed code construction is exponential (in ε^{-1})

  Q: Can be reduced to polynomial by taking random subset of coordinates?

++

- Provided bounds on the rate of codes below the Plotkin point

  Q: Non-optimal except the Plotkin point $\tau = \tau_L(w')$ and noiseless case $\tau = 0$.

  How to improve?

Thanks!

Questions?