Two-stage coding over the Z-channel

Nikita Polyanskii

Skolkovo Institute of Science and Technology

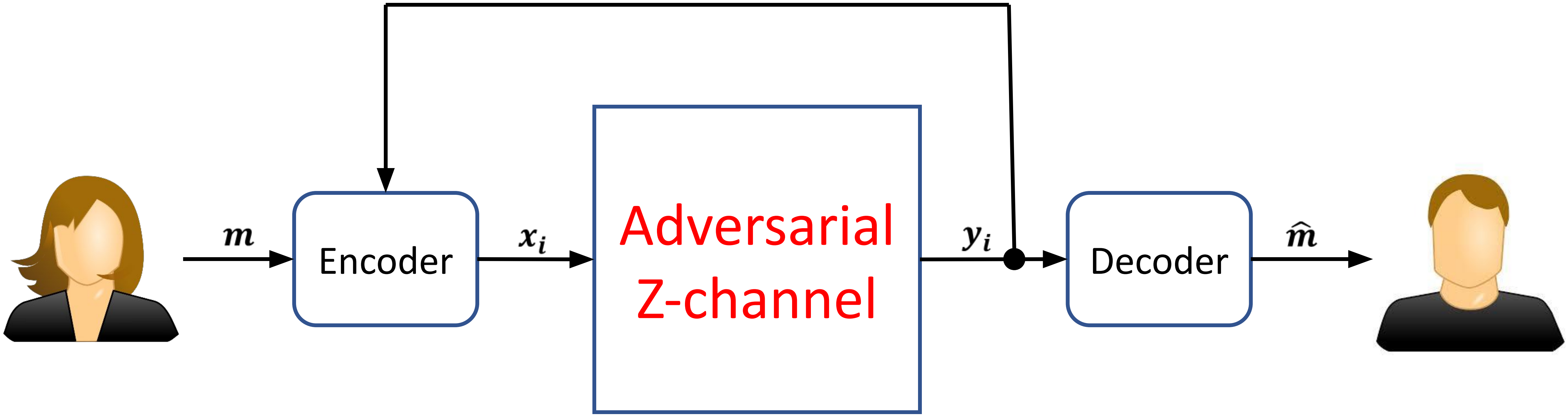
Technische Universität München

2021 IEEE International Symposium on Information Theory
Melbourne, Victoria, Australia

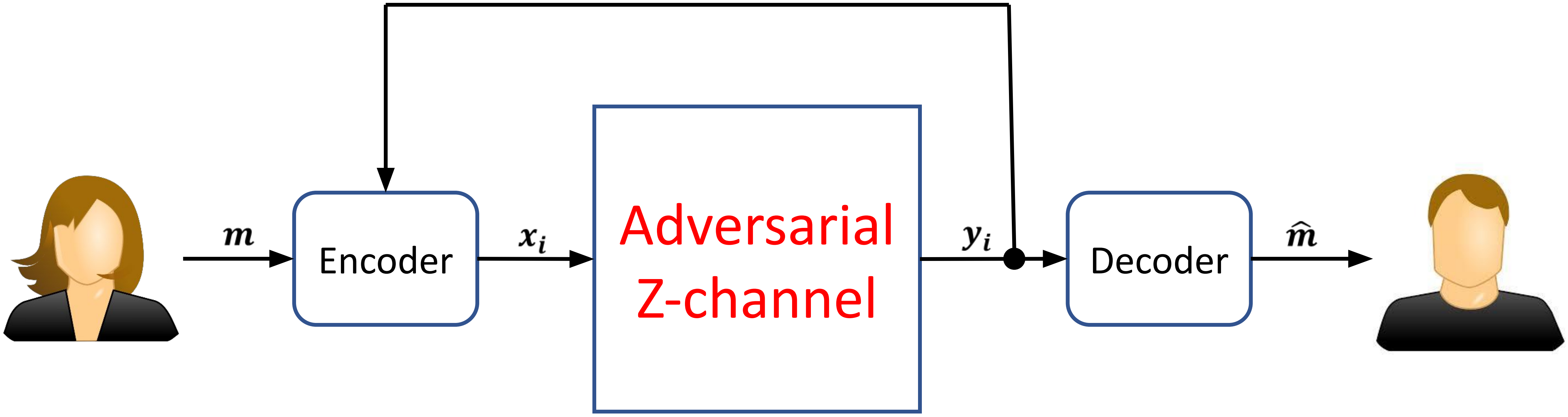
Outline

- Introduction
- Related work
- Achievability result (encoding algorithm)
- Converse result
- Conclusion

Introduction



- **Encoding strategy can be adapted based on feedback at one designated moment (Encoder)**
- **Errors are adversarial (Channel)**
- **Transmit information error-free (Decoder)**

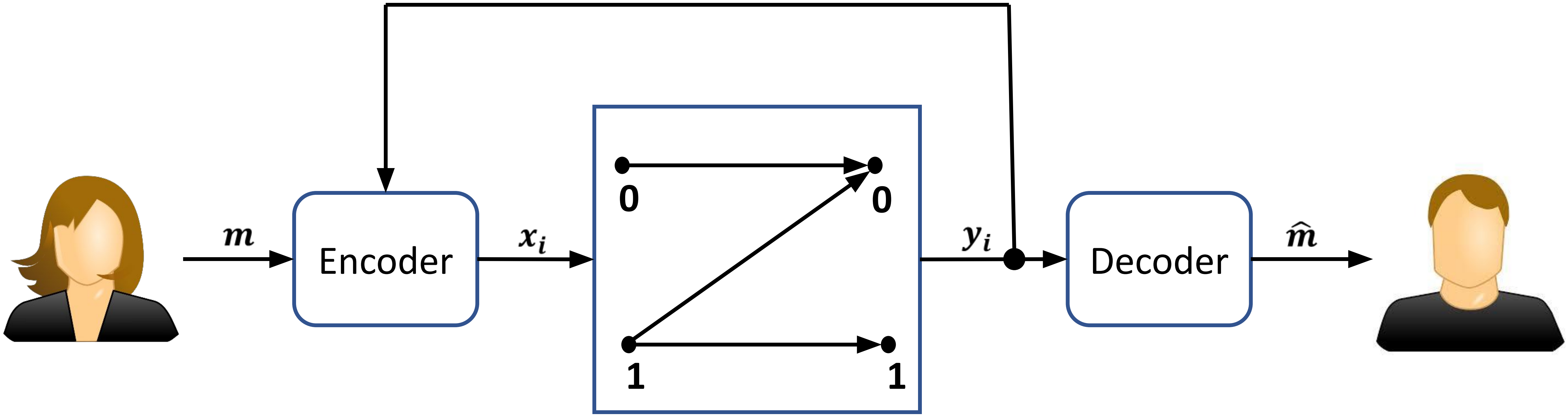


- **Encoding strategy can be adapted based on feedback at one designated moment (Encoder)**

Message $m \epsilon [M]$ is encoded to $(x_1, \ldots, x_n) \epsilon \{0, 1\}^n$, where

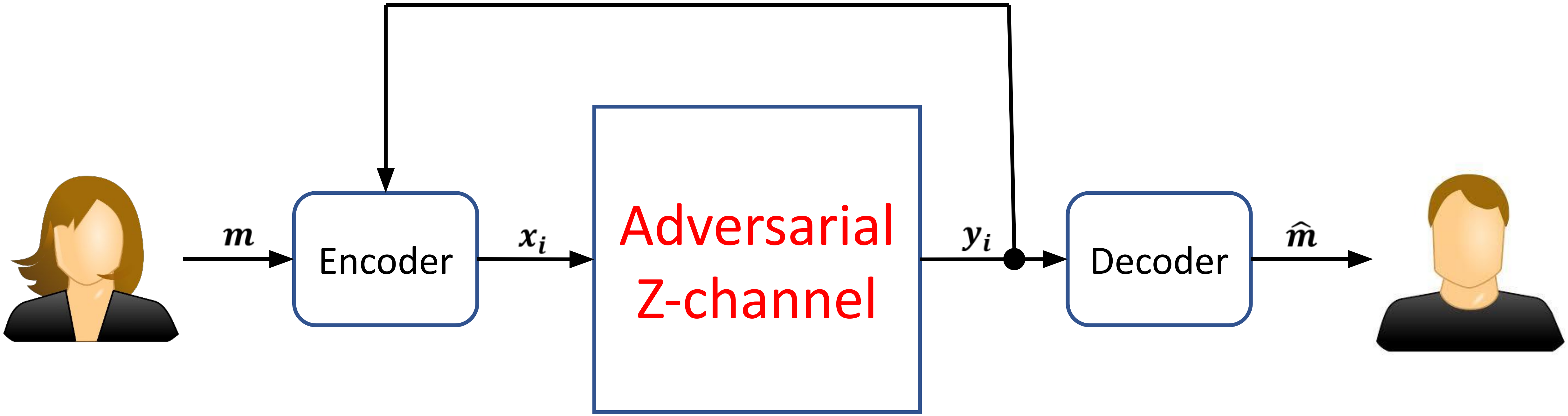
$x_i = x_i(m)$ for $i \leq n_1$

$x_i = x_i(m, y_1, \ldots, y_{n_1})$ for $i > n_1$



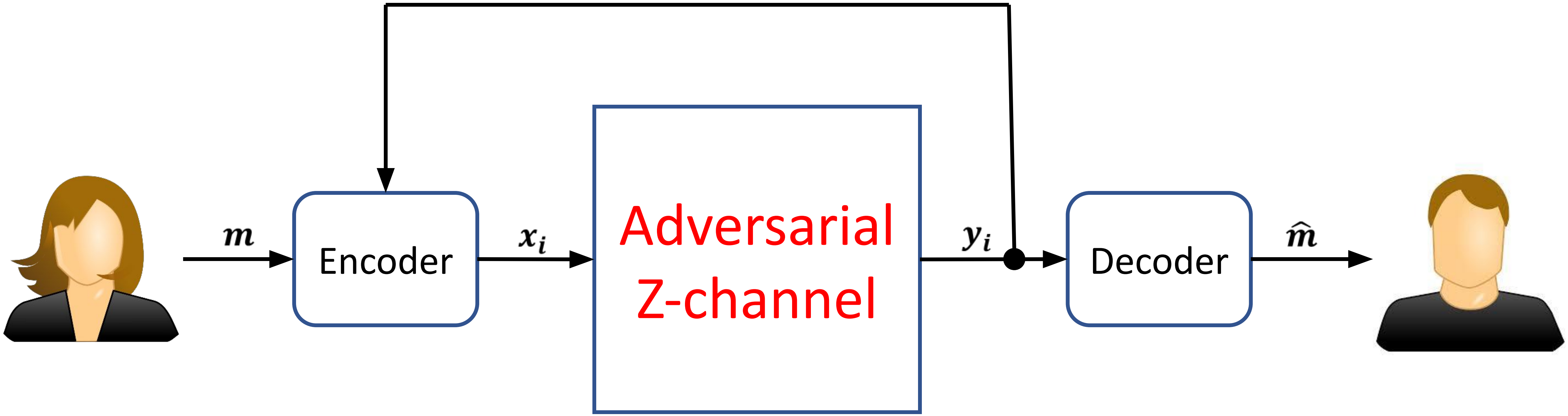
- **Errors are adversarial (Channel)**

Let $\underline{x} := (x_1, \dots, x_n)$ be an *input* string and $\underline{y} := (y_1, \dots, y_n)$ be an *output* string and $0 \le \tau \le 1$ be a *fraction of errors*. The channel can inflict any pattern of errors with full knowledge of the message and the code with the property $d_H(\underline{x}, \underline{y}) \le \tau n$.



- **Transmit information error-free (Decoder)**

For any pattern of errors, Bob has to *uniquely decode* the message, i.e., $\hat{\boldsymbol{m}}(\underline{\boldsymbol{y}}) = \boldsymbol{m}$.



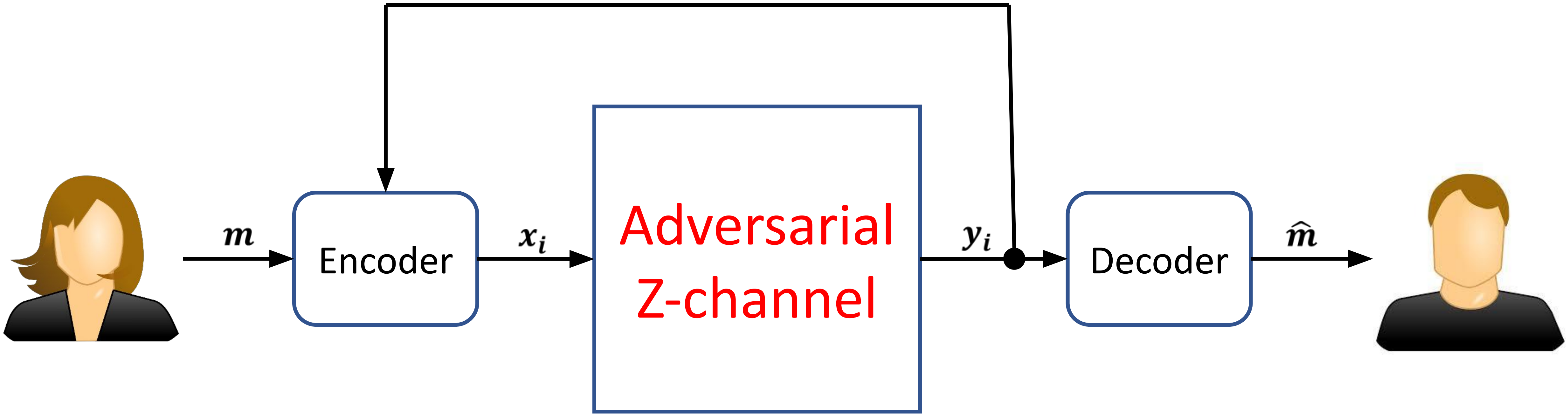
Goal:

Find the *maximum fraction* $\tau_Z^{(2)}$ of *correctable asymmetric* errors of positive-rate codes.

In other words,

for any $\tau < \tau_Z^{(2)}$, the maximum number of messages $M(\tau, n) = 2^{\Omega(n)}$.

for any $\tau > \tau_Z^{(2)}$, the maximum number of messages $M(\tau, n) = 2^{o(n)}$.



Main result:

$$\tau_Z^{(2)} = \max_w \frac{w + w^3}{1 + 4w^3} \approx 0.44\ldots$$

Related work

- Channel inflicts only a **constant** number of asymmetric errors [Dumitriu, Spencer’04]
- Fully adaptive encoding strategies [Deppe, Lebedev, Maringer, P.’ 20]
- Non-adaptive encoding algorithms [Bassalygo’65, Borden’83]

Most relevant work

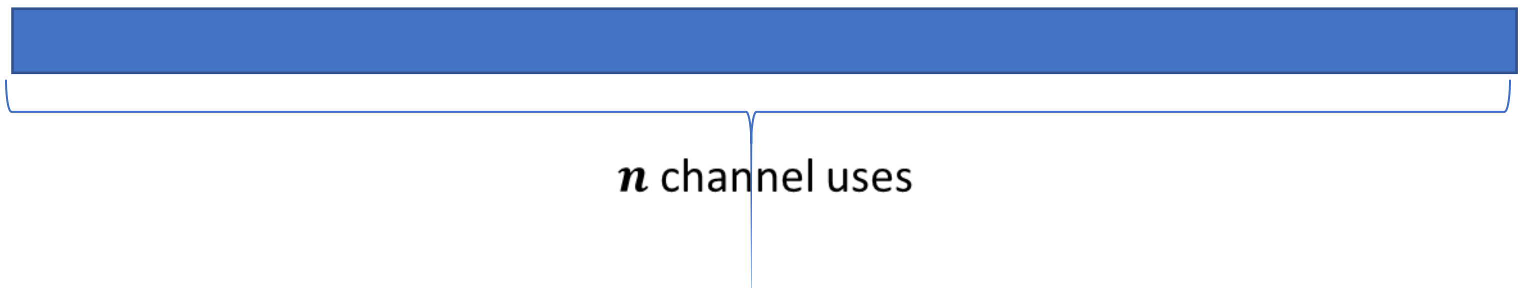
When the number of errors, $\boldsymbol{t}$, is fixed, the problem has been discussed under the guise of a *half-lie game* in numerous papers.

Theorem (Dumitriu-Spencer'05)
If the number of error is fixed, i.e., $\mathbf{t = O(1)}$*, then the maximum number of messages that Alice can send to Bob satisfies*

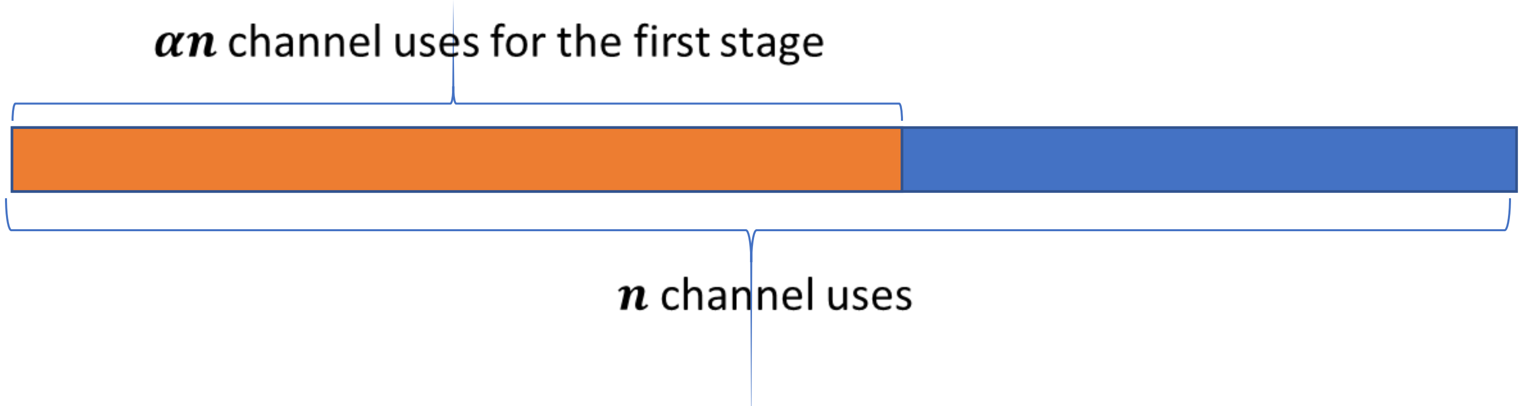
$$\boldsymbol{M^f(n,t) \approx 2^{n+t} t!\, n^{-t}}$$

Achievability result (algorithm)

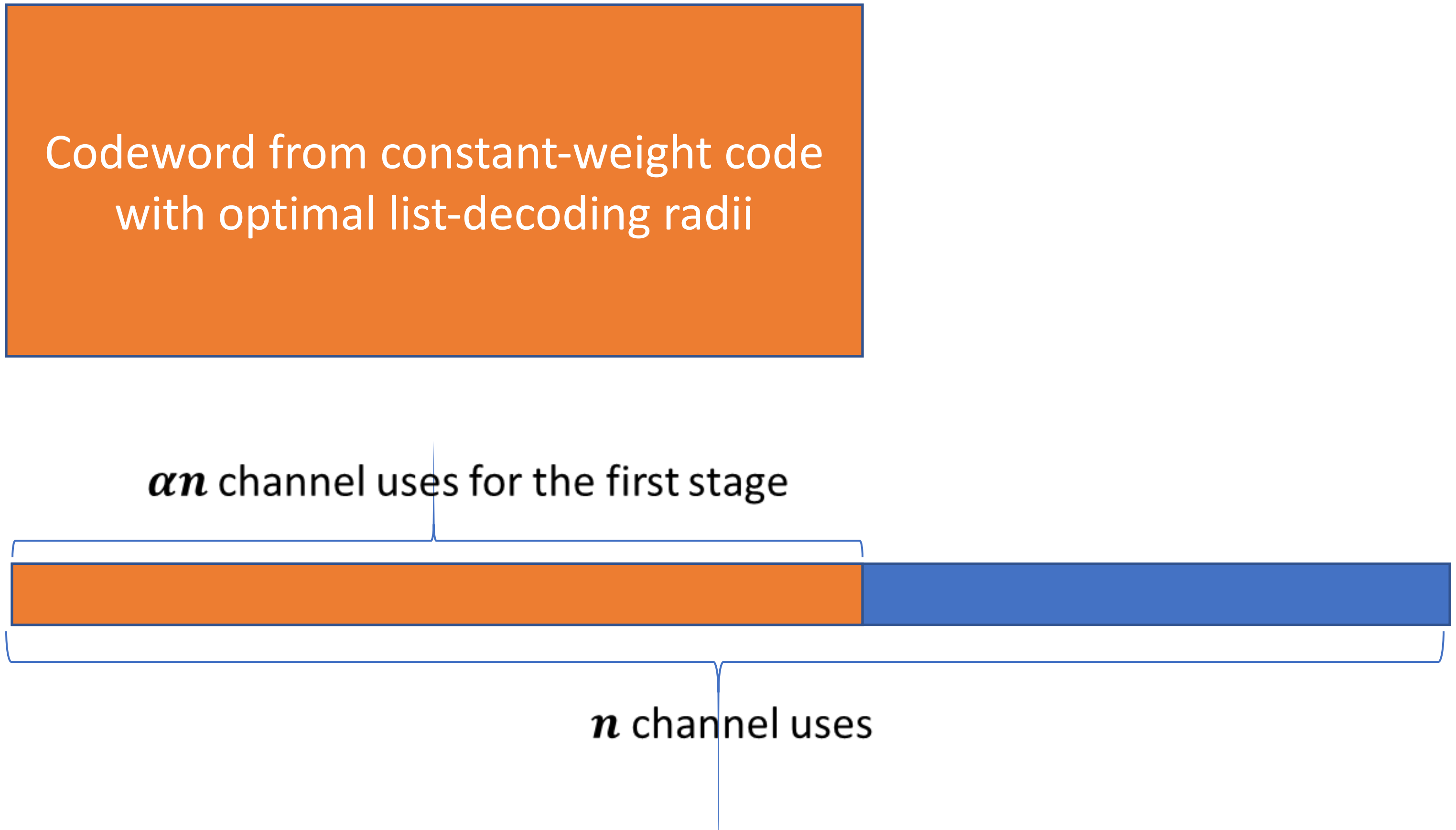
A high-level overview



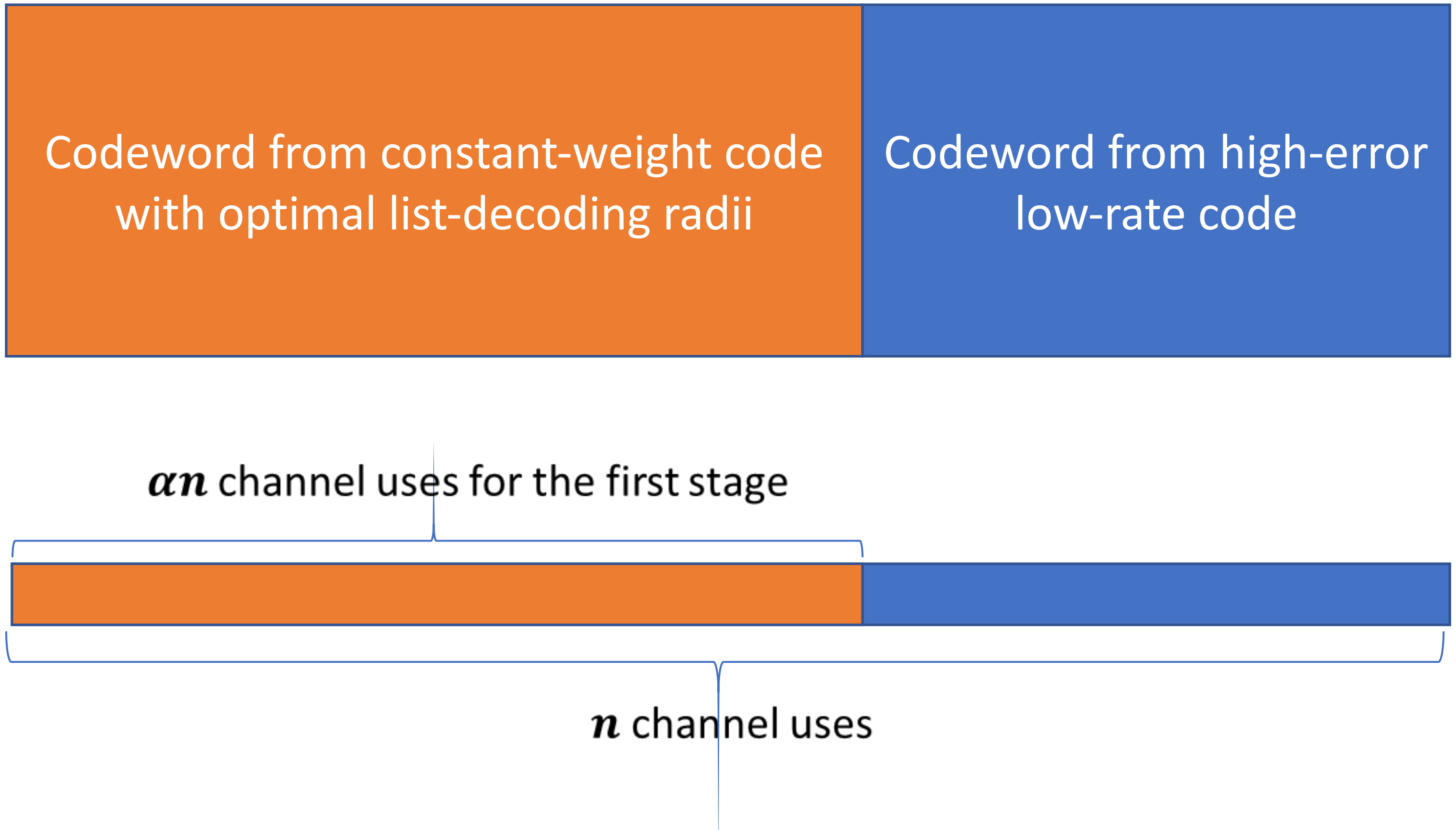
A high-level overview



A high-level overview



A high-level overview



Lemma (Random list-decodable codes, Informal)

Let $\boldsymbol{w}$ be a weight parameter, $\mathbf{0} < \boldsymbol{w} < \mathbf{1}$, and $\boldsymbol{\varepsilon} > \mathbf{0}$ be fixed.
There exists a positive-rate $\boldsymbol{w}$-constant-weight code with $\boldsymbol{L}$-list-decoding radius

$$\boldsymbol{w} - \boldsymbol{w}^{\boldsymbol{L}+\mathbf{1}} - \boldsymbol{\varepsilon}$$

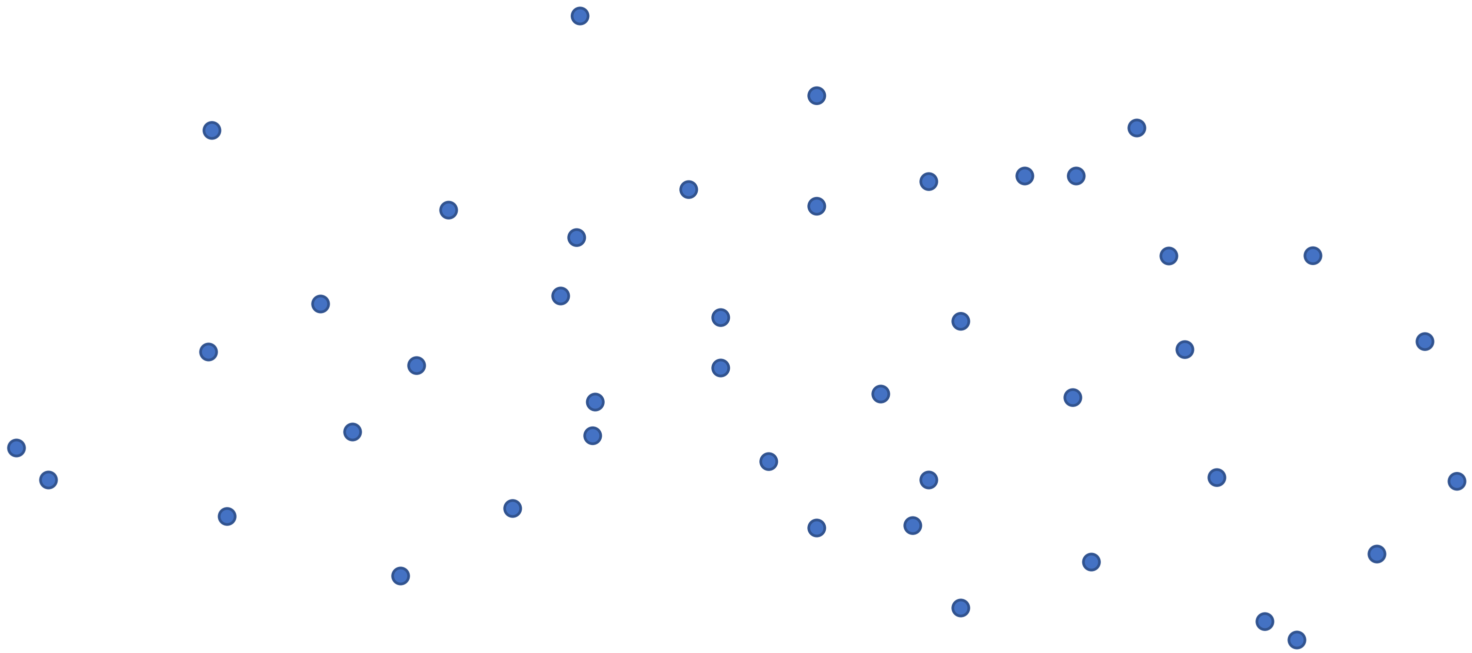
for all $\boldsymbol{L}, \mathbf{1} \leq \boldsymbol{L} \leq \boldsymbol{L}_{\mathbf{up}}$

<u>Lemma</u> (Random list-decodable codes, Informal)

Let $\boldsymbol{w}$ be a weight parameter, $\boldsymbol{0 < w < 1}$, and $\boldsymbol{\varepsilon > 0}$ be fixed. There exists a positive-rate $\boldsymbol{w}$-constant-weight code with $\boldsymbol{L}$-list-decoding radius

$$\boldsymbol{w - w^{L+1} - \varepsilon}$$

for all $\boldsymbol{L}, \boldsymbol{1 \leq L \leq L_{\mathrm{up}}}$



$\boldsymbol{C \subseteq \{0,1\}^n}$

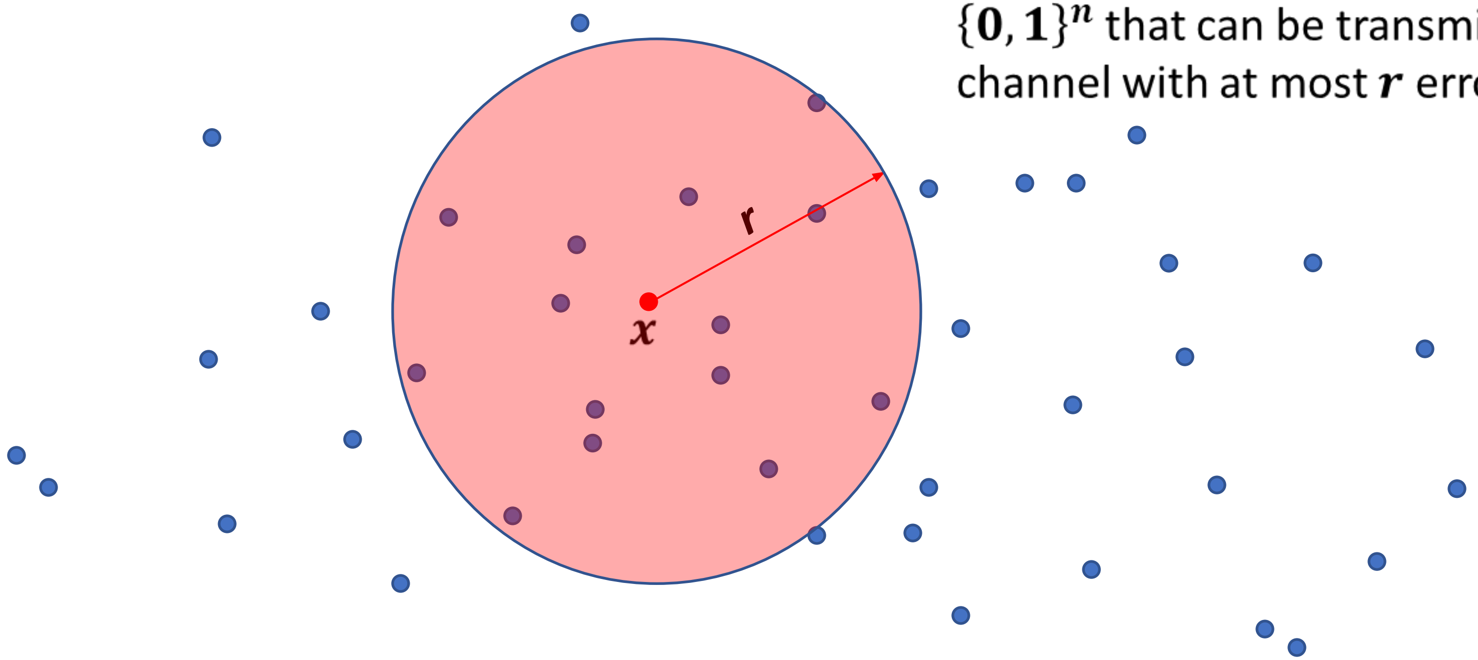
<u>Lemma</u> (Random list-decodable codes, Informal)

Let $\boldsymbol{w}$ be a weight parameter, $\boldsymbol{0 < w < 1}$, and $\boldsymbol{\varepsilon > 0}$ be fixed. There exists a positive-rate $\boldsymbol{w}$-constant-weight code with $\boldsymbol{L}$-list-decoding radius

$$\boldsymbol{w - w^{L+1} - \varepsilon}$$

for all $\boldsymbol{L}$, $\boldsymbol{1 \leq L \leq L_{\mathrm{up}}}$

Z-ball centered at $\boldsymbol{x}$ with radius $\boldsymbol{r}$ includes all words in $\{\boldsymbol{0,1}\}^{\boldsymbol{n}}$ that can be transmitted over the adversarial Z channel with at most $\boldsymbol{r}$ errors such that $\boldsymbol{x}$ is received



$\boldsymbol{C \subseteq \{0,1\}^n}$

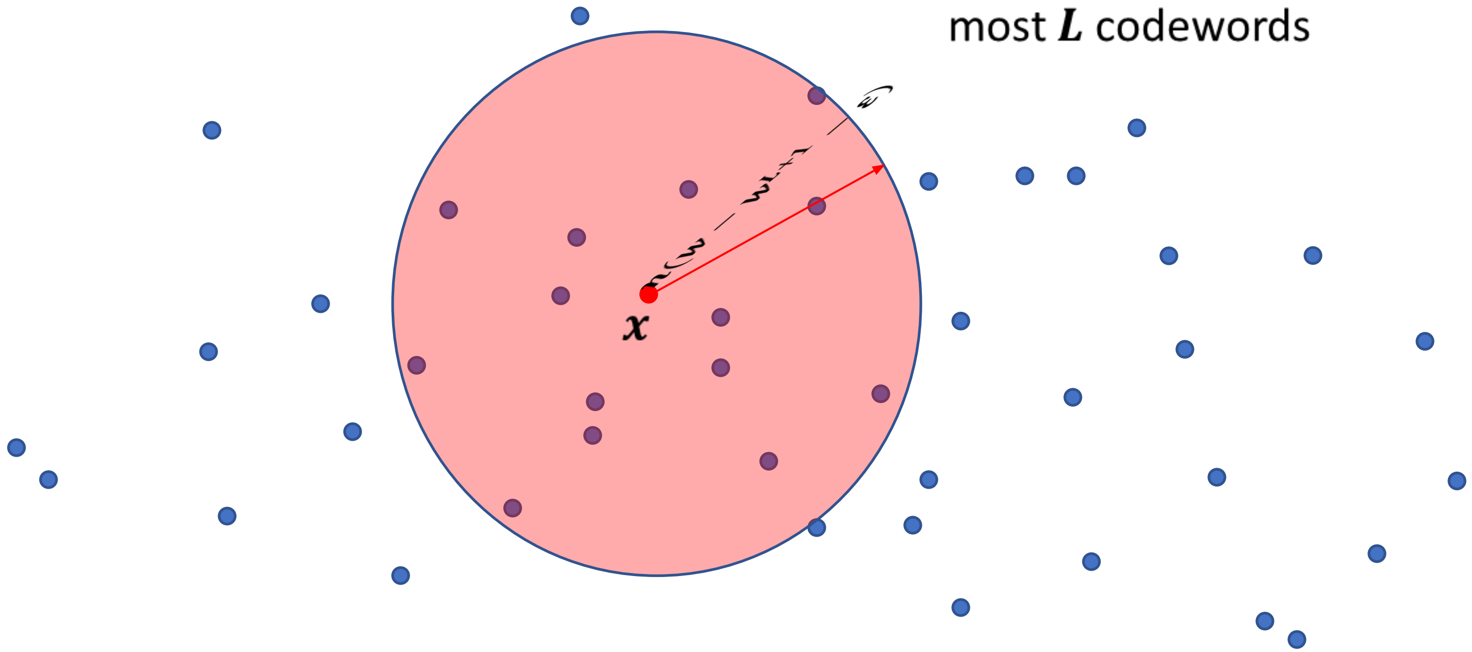
Lemma (Random list-decodable codes, Informal)

Let $\boldsymbol{w}$ be a weight parameter, $\mathbf{0} < \boldsymbol{w} < \mathbf{1}$, and $\boldsymbol{\varepsilon} > \mathbf{0}$ be fixed. There exists a positive-rate $\boldsymbol{w}$-constant-weight code with $\boldsymbol{L}$-list-decoding radius

$$\boldsymbol{w} - \boldsymbol{w}^{\boldsymbol{L}+\mathbf{1}} - \boldsymbol{\varepsilon}$$

for all $\boldsymbol{L}, \mathbf{1} \leq \boldsymbol{L} \leq \boldsymbol{L}_{\mathbf{up}}$

Any Z-ball with radius $\mathbf{r} = \boldsymbol{n}(\boldsymbol{w} - \boldsymbol{w}^{\boldsymbol{L}+\mathbf{1}} - \boldsymbol{\varepsilon})$ contains at most $\boldsymbol{L}$ codewords



$\boldsymbol{C} \subseteq \{\mathbf{0}, \mathbf{1}\}^{\boldsymbol{n}}$

Lemma (High-error low-rate codes, **Informal**) [Borden'83]

Let $\boldsymbol{\tau}_Z(\boldsymbol{M})$ *be the maximum fraction of correctable asymmetric errors in a code of size* $\boldsymbol{M}$*. Then* $\boldsymbol{\tau}_Z(\boldsymbol{M})$ *can be found by solving a maximization problem. In particular, for small* $\boldsymbol{M}$*, some values are depicted in Table*

M	$\tau_Z(M)$	M	$\tau_Z(M)$	M	$\tau_Z(M)$	M	$\tau_Z(M)$
15	$\frac{377}{1177}$	12	$\frac{1}{3}$	9	$\frac{13}{37}$	5,6	$\frac{2}{5}$
14	$\frac{35}{108}$	11	$\frac{31}{92}$	8	$\frac{4}{11}$	3,4	$\frac{1}{2}$
13	$\frac{18}{55}$	10	$\frac{9}{26}$	7	$\frac{3}{8}$	2	1

Lemma (High-error low-rate codes) [Follows from Levenstein'61]

$$\boldsymbol{\tau}_Z(\boldsymbol{M}) \geq \frac{M}{4M-2}$$

Encoding algorithm:

1) Transmit $\boldsymbol{m}$th codeword of a $\boldsymbol{w}$-constant-weight code of length $\boldsymbol{\alpha n}$ whose $\boldsymbol{L}$-list-decoding radius is $\boldsymbol{w - w^{L+1} - \varepsilon}$ for all small $\boldsymbol{L}$.
2) Let $\boldsymbol{\tau_1}$ be a fraction of occurred errors at the first stage.
   - If $\boldsymbol{w - w^{L} - \varepsilon < \tau_1 < w - w^{L+1} - \varepsilon}$, then need to distinguish the original message from $\boldsymbol{L}$ candidates. Use high-error low-rate code of size $\boldsymbol{L}$ correcting a fraction $\boldsymbol{\tau_Z(L)}$ of errors.
   - Otherwise, use ½-constant-weight positive-rate code correcting a fraction $\boldsymbol{¼ - \varepsilon}$ of errors.

Analysis of the algorithm:

The algorithm yields

$$\boldsymbol{\tau}_{Z}^{(2)} \geq \max_{\boldsymbol{w}} \max_{\boldsymbol{\alpha}} \boldsymbol{\tau}^{*}(\boldsymbol{\alpha}, \boldsymbol{w}),$$

where $\boldsymbol{\tau}^{*}(\boldsymbol{\alpha}, \boldsymbol{w})$ is the supremum over $\boldsymbol{\tau}$ that satisfies

$$\begin{cases} \boldsymbol{\tau} \leq \boldsymbol{\alpha}\left(\boldsymbol{w} - \boldsymbol{w}^{L}\right) + (\mathbf{1} - \boldsymbol{\alpha})\boldsymbol{\tau}_{Z}(\boldsymbol{L}), \forall \mathbf{L} > \mathbf{1}, \\ \boldsymbol{\tau} \leq \boldsymbol{\alpha}\boldsymbol{w} + (\mathbf{1} - \boldsymbol{\alpha})\frac{\mathbf{1}}{\mathbf{4}} \end{cases}$$

After some algebraic manipulations, we get

$$\boldsymbol{\tau}_{\mathbf{Z}}^{(2)} \geq \max_{\boldsymbol{w}} \frac{\boldsymbol{w} + \boldsymbol{w}^{3}}{\mathbf{1} + \mathbf{4}\boldsymbol{w}^{3}} \approx \mathbf{0.44}$$

Converse result

<u>Lemma</u> (Converse bound for list-decodable codes, Informal)

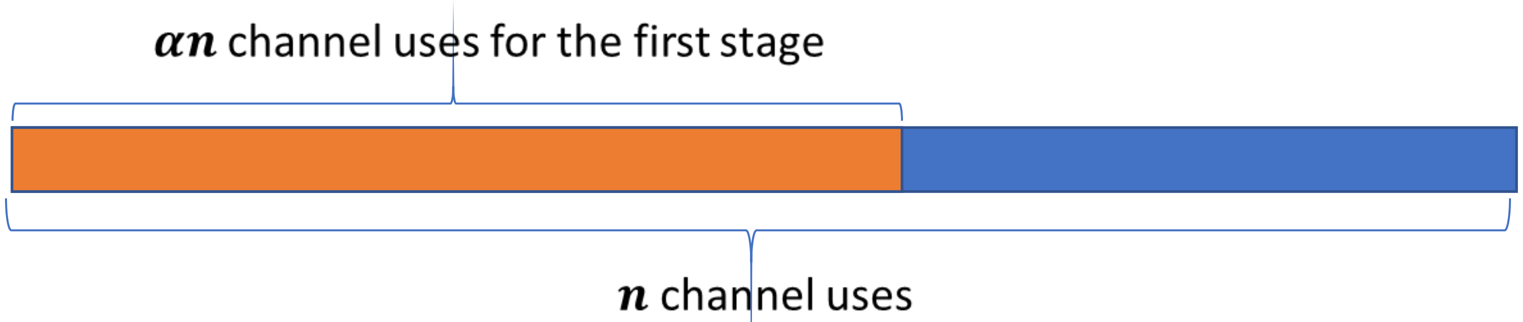
Let $\boldsymbol{w}$ be a weight parameter, $\mathbf{0} < \boldsymbol{w} < \mathbf{1}$, and $\boldsymbol{\varepsilon} > \mathbf{0}$ be fixed. If a $\boldsymbol{w}$-constant-weight code has $\boldsymbol{L}$-list-decoding radius

$$\boldsymbol{w} - \boldsymbol{w}^{\boldsymbol{L}+\mathbf{1}} + \boldsymbol{\varepsilon},$$

then its size is $\boldsymbol{O}(\mathbf{1})$.

A high-level idea

1. Suppose a two-stage encoding strategy tolerating a fraction $\boldsymbol{\tau}$ of asymmetric errors is given.
2. Some positive-rate $\boldsymbol{w}$-constant-weight subcode can be extracted at the first stage.
3. For any $\boldsymbol{L}$, there exists a pattern of errors of weight $\boldsymbol{w}-\boldsymbol{w}^{\boldsymbol{L}+\mathbf{1}}+\boldsymbol{\varepsilon}$ at the first stage such that the original message can not be distinguished from some other $\boldsymbol{L}-\mathbf{1}$ messages.
4. Any code of size $\boldsymbol{L}$ cannot correct a fraction $\boldsymbol{\tau}_Z(\boldsymbol{L})+\boldsymbol{\varepsilon}$ of asymmetric errors.



Analysis of the idea:

One can show that $\boldsymbol{\tau}$ satisfies

$$\begin{cases} \boldsymbol{\tau} \le \boldsymbol{\alpha}\left(\boldsymbol{w} - \boldsymbol{w}^{\boldsymbol{L}}\right) + (\mathbf{1} - \boldsymbol{\alpha})\boldsymbol{\tau}_{Z}(\boldsymbol{L}), \forall \mathbf{L} > \mathbf{1} \\ \boldsymbol{\tau} \le \boldsymbol{\alpha}\boldsymbol{w} + (\mathbf{1} - \boldsymbol{\alpha})\frac{\mathbf{1}}{\mathbf{4}} \end{cases}$$

Therefore, $\boldsymbol{\tau} \le \boldsymbol{\tau}^{*}\ (\boldsymbol{\alpha}, \boldsymbol{w}) \le \max_{\boldsymbol{w}} \max_{\boldsymbol{\alpha}} \boldsymbol{\tau}^{*}(\boldsymbol{\alpha}, \boldsymbol{w})$

Conclusion

Summary:

- In this paper, we discussed two-stage error-correcting codes for the adversarial Z-channel.
- We precisely characterized when exponential-sized (or positive-rate) codes exist for our model (when $\boldsymbol{\tau} < \boldsymbol{\tau}_{\mathbf{Z}}^{(2)} \approx \mathbf{0.44}$).
- Our proof relies on the concepts of list-decodable codes and high-error low-rate codes.

Further directions:

- Derive bounds on the rate when a fraction of errors $\boldsymbol{\tau} < \boldsymbol{\tau}_{\mathbf{Z}}^{(2)}$
- Investigate other channels (e.g., bit-flip errors)

Thanks!

If you have any questions please contact nikitapolyansky@gmail.com