Algebraic codes decoding in Hamming and Rank metrics: to unicity and beyond.

CAIPI SYMPOSIUM - Montpellier

11-12 December 2025

Ilaria Zappatore

Université de Limoges

Part 1 : Hamming metric

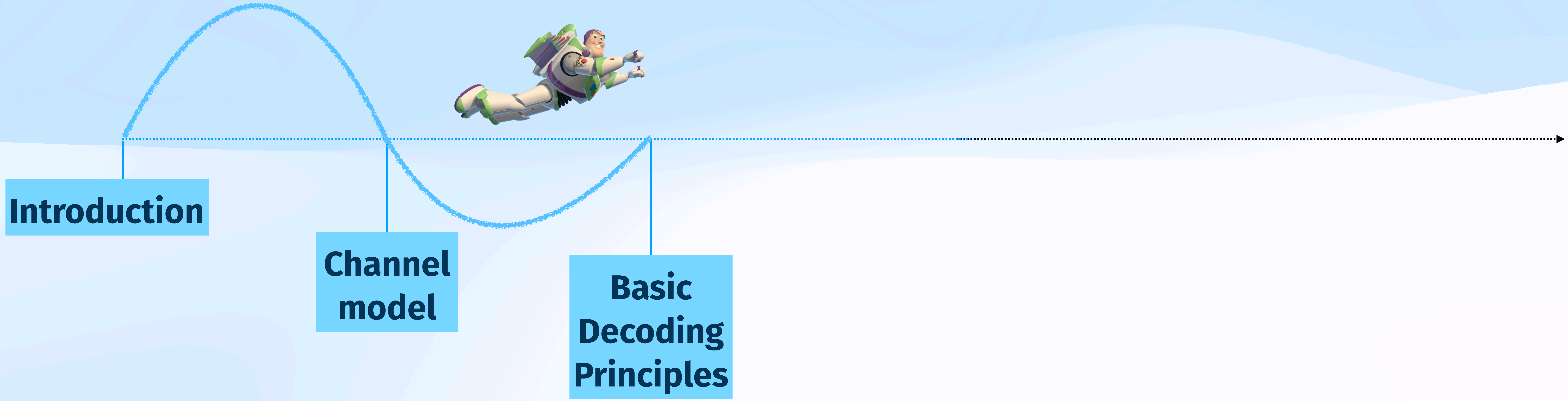
Introduction

Part 1 : Hamming metric

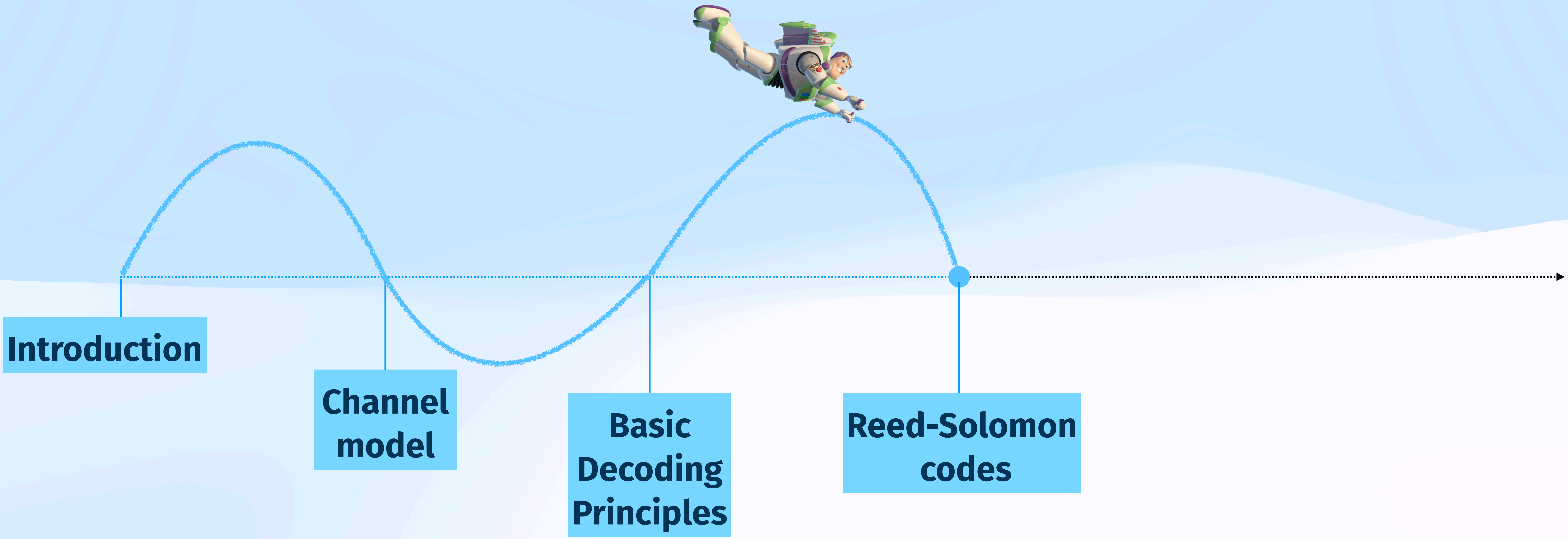
Introduction

Channel model

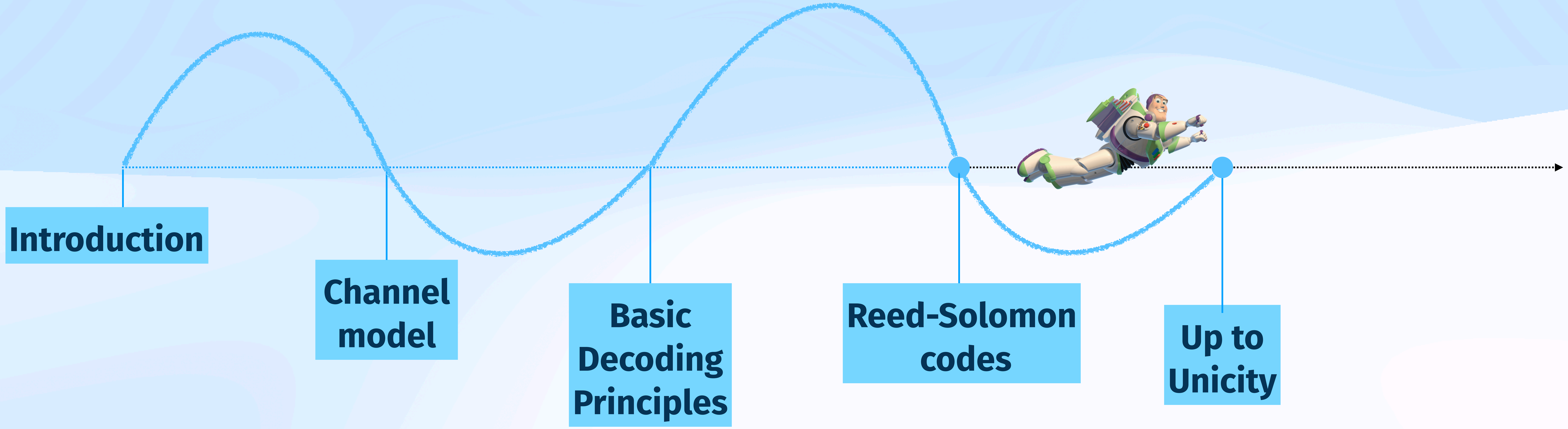
Part 1 : Hamming metric



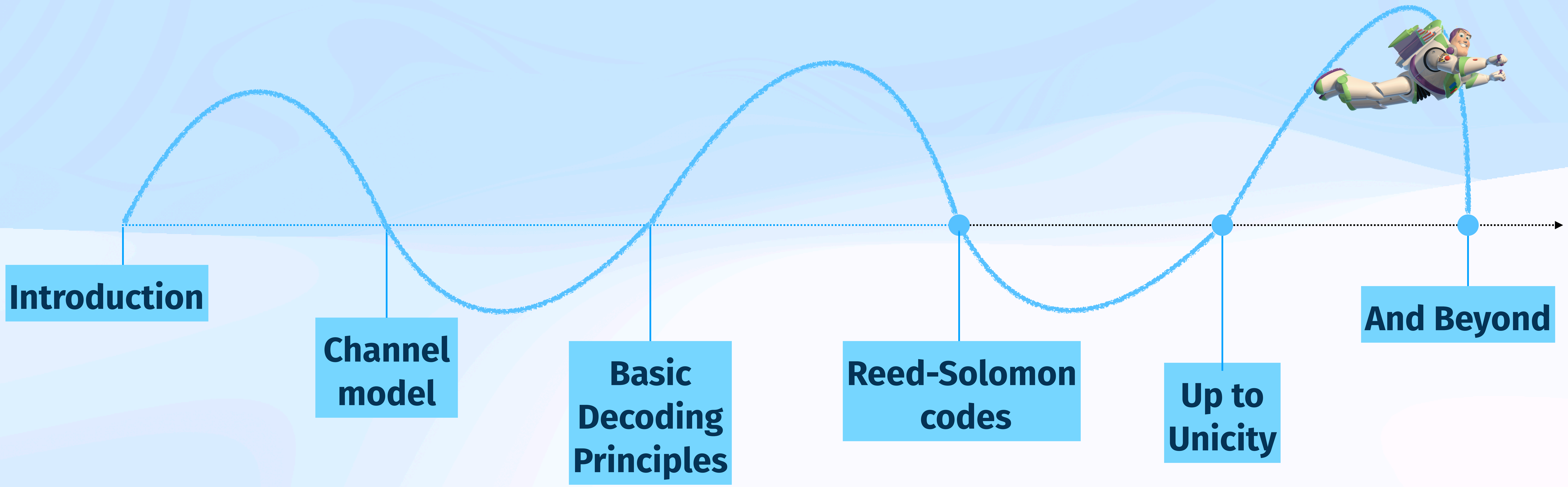
Part 1 : Hamming metric



Part 1 : Hamming metric



Part 1 : Hamming metric



Part 1 : Hamming metric

Introduction

Introduction

Richard Hamming (1915-1998)

« Damn it, if the machine can detect an error,

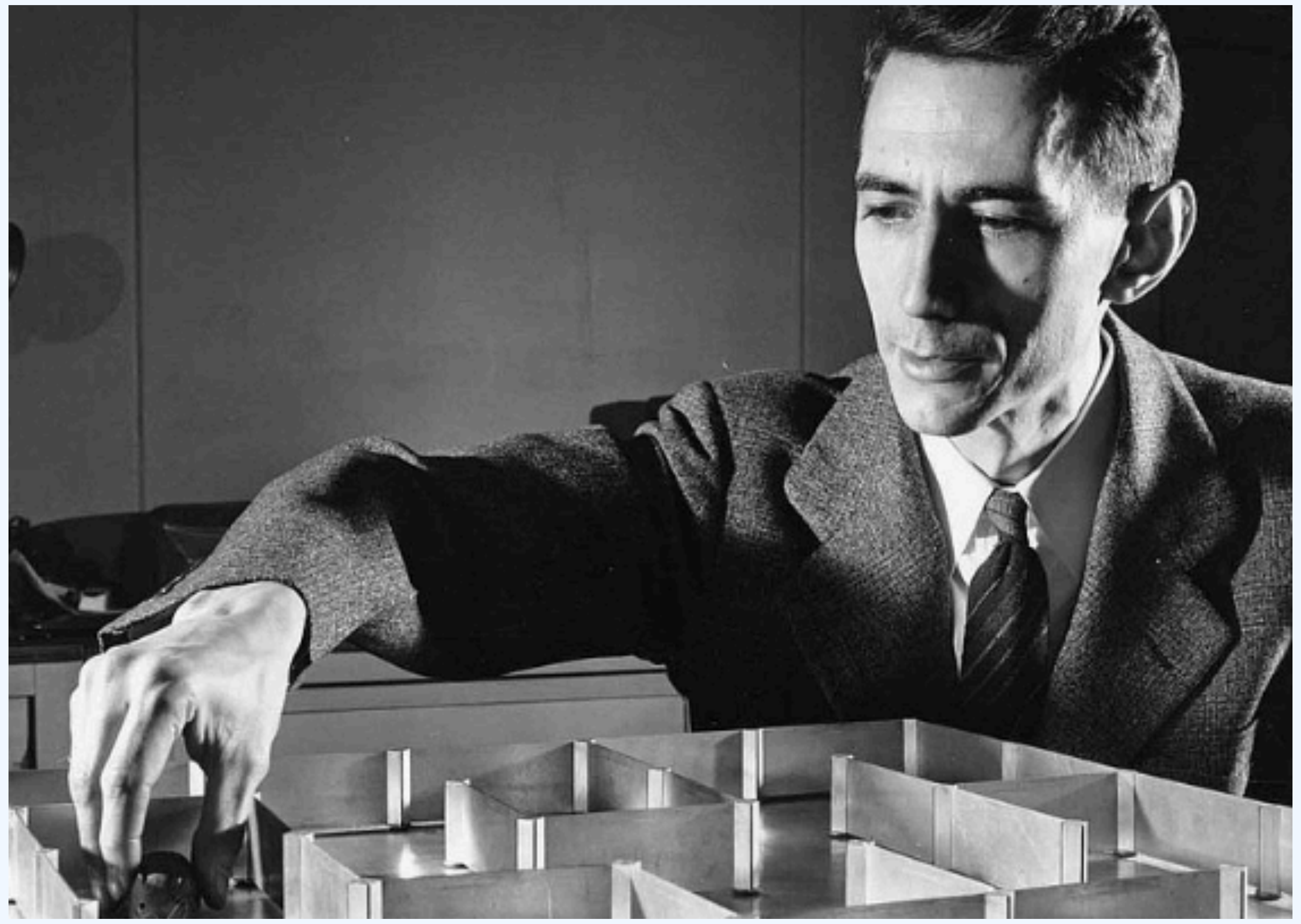
why can correct it ? »

From an interview, 3-4 February 1977

Punch cards in a punch card machine

Hamming theory of error correcting codes (Combinatorics, algebra)

Introduction

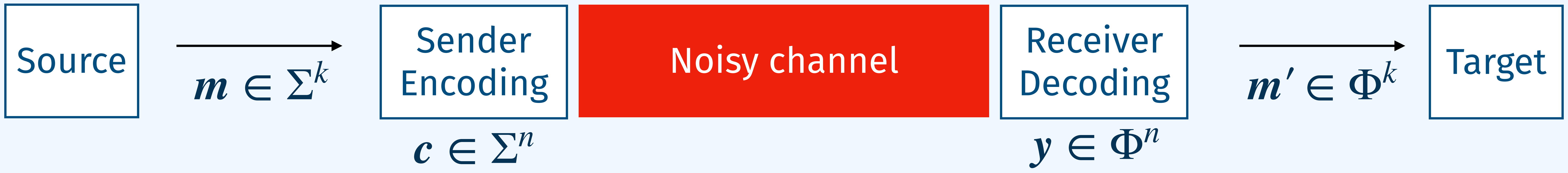


Claude E. Shannon (1916-2001)

Shannon approach : information theory

(Probability)

Shannon Channel Model

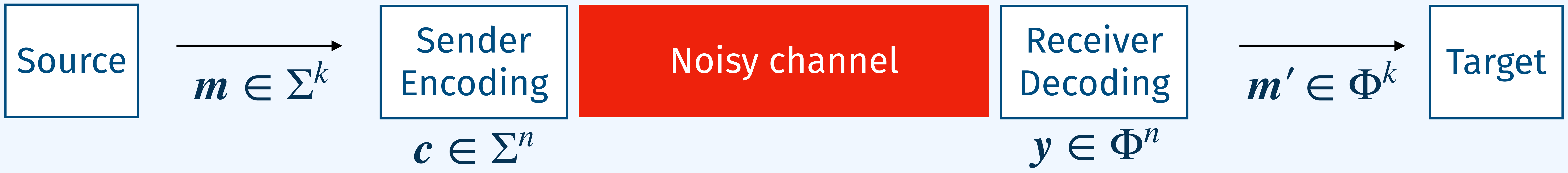


Goal: communication over a **noisy channel**

Channel : $(\Sigma, \Phi, \mathbb{P})$

- Σ, Φ are alphabets,
- and $\mathbb{P}(\boldsymbol{y}$ received $\mid \boldsymbol{c}$ sent $)$ is defined for any $\boldsymbol{c} \in \Sigma^n, \boldsymbol{y} \in \Phi^n$

Shannon Channel Model



Goal: communication over a **noisy channel**

Channel : $(\Sigma, \Phi, \mathbb{P})$

- Σ, Φ are alphabets,
- and $\mathbb{P}(\boldsymbol{y}$ received $\mid \boldsymbol{c}$ sent $)$ is defined for any $\boldsymbol{c} \in \Sigma^n, \boldsymbol{y} \in \Phi^n$

Memoryless channels:
Noise acts <u>independently</u> on each transmitted symbol

Part 1 : Hamming metric

Introduction

Channel model

- Binary Symmetric Channel
- $q-$are Symmetric Channel
- Burst channel

The channel model

Channel : $(\Sigma, \Phi, \mathbb{P})$

- Σ, Φ are alphabets,
- and $\mathbb{P}(\boldsymbol{y}$ received $\mid \boldsymbol{c}$ sent $)$ is defined for any $\boldsymbol{c} \in \Sigma^n, \boldsymbol{y} \in \Phi^n$

Memoryless channels:
Noise acts <u>independently</u> on each transmitted symbol

$$\boldsymbol{c} \in \Sigma^n \longrightarrow \boxed{\text{Noisy channel}} \longrightarrow \boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e} \in \Sigma^n$$

$$\boldsymbol{e}$$

We focus on channels that are

- **Discrete:** $|\Sigma|, |\Phi| < \infty$
- **Additive:** $\Sigma = \Phi$ and **they are finite abelian groups**

The channel model

$$\boldsymbol{c} \in \Sigma^n \longrightarrow \boxed{\text{Noisy channel}} \longrightarrow \boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e} \in \Sigma^n$$

$\boldsymbol{e}$

$E = \{i \in [n] \mid e_i \neq 0\} = \{i \in [n] \mid c_i \neq y_i\}$ **error support**

Let $\boldsymbol{x}, \boldsymbol{y} \in \Sigma^n$,

- **Hamming distance**: $d(\boldsymbol{x}, \boldsymbol{y}) := |\{i \in [n] \mid x_i \neq y_i\}|$
- **Hamming support** and **weight**: $Supp(\boldsymbol{x}) := \{i \in [n] \mid x_i \neq 0\}$, $w(\boldsymbol{x}) = |Supp(\boldsymbol{x})|$

The binary symmetric channel (BSC)

- $\Sigma = \mathbb{F}_2$
- $\forall \boldsymbol{c}, \boldsymbol{y} \in \mathbb{F}_2^n$ then $\mathbb{P}(\boldsymbol{y} \text{ received } \mid \boldsymbol{c} \text{ sent}) = \prod_{i \in [n]} \mathbb{P}(y_i \text{ received } \mid c_i \text{ sent})$

For any $a, b \in \mathbb{F}_2$

$$\mathbb{P}(b \text{ received } \mid a \text{ sent}) = \begin{cases} 1 - p & \text{if } a = b \\ p & \text{otherwise} \end{cases}$$

Memoryless channel

Each bit is flipped with probability p

- If $p = 1/2$ reliable communication is impossible (Shannon Theorem)
- We can assume $p < 1/2$

The q-ary symmetric channel

- $\Sigma = \mathbb{F}_q$, $q \geq 2$
- $\forall \boldsymbol{c}, \boldsymbol{y} \in \mathbb{F}_q^n$ then $\mathbb{P}(\boldsymbol{y} \text{ received } \mid \boldsymbol{c} \text{ sent}) = \prod_{i \in [n]} \mathbb{P}(y_i \text{ received } \mid c_i \text{ sent})$

Memoryless channel

For any $a, b \in \mathbb{F}_q$

$$\mathbb{P}(b \text{ received } \mid a \text{ sent}) = \begin{cases} 1 - p & \text{if } a = b \\ p/(q-1) & \text{otherwise} \end{cases}$$

The q-ary symmetric channel

- $\Sigma = \mathbb{F}_q$, $q \geq 2$
- $\forall \boldsymbol{c}, \boldsymbol{y} \in \mathbb{F}_q^n$ then $\mathbb{P}(\boldsymbol{y} \text{ received } \mid \boldsymbol{c} \text{ sent}) = \prod_{i \in [n]} \mathbb{P}(y_i \text{ received } \mid c_i \text{ sent})$

Memoryless channel

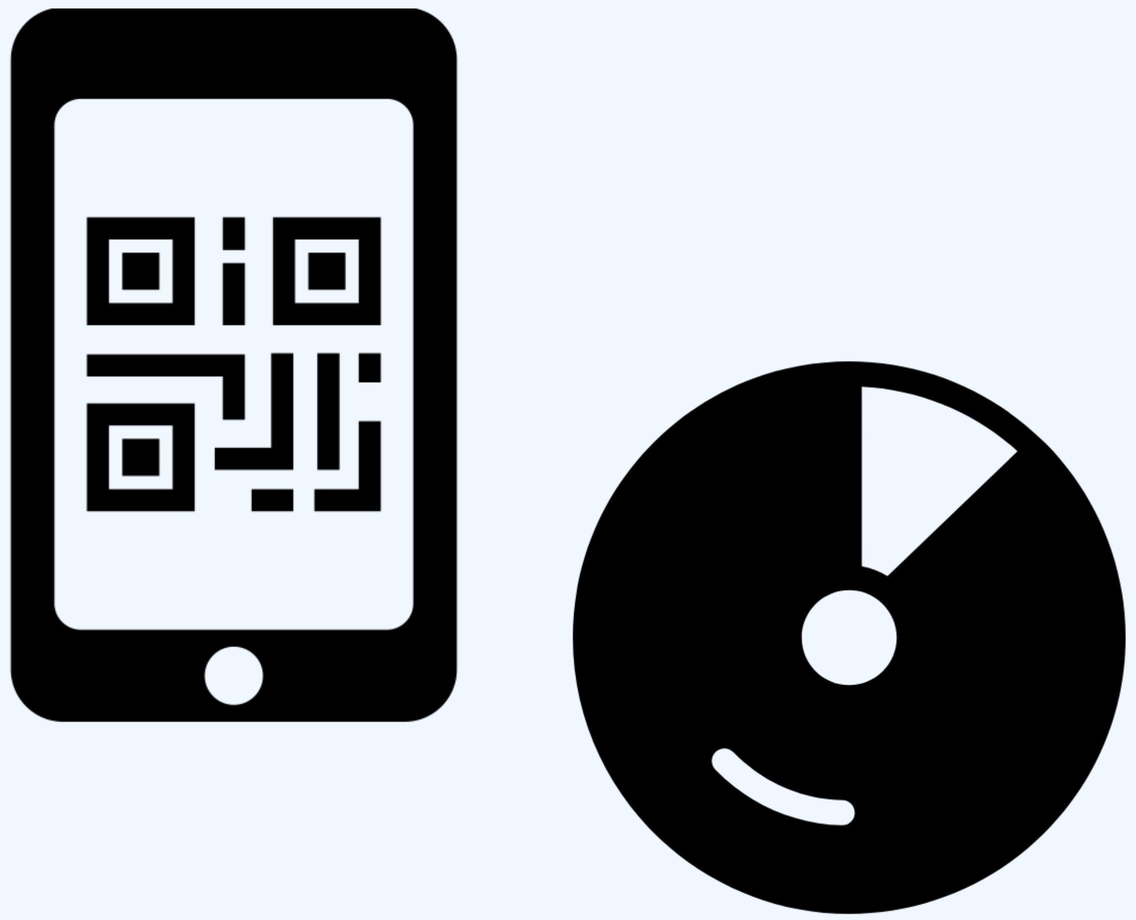
For any $a, b \in \mathbb{F}_q$

$$\mathbb{P}(b \text{ received } \mid a \text{ sent}) = \begin{cases} 1 - p & \text{if } a = b \\ p/(q-1) & \text{otherwise} \end{cases}$$

What happens if the channel is not memoryless ?

Not memoryless channels

What happens if the channel is not memoryless ?



- Errors are **correlated across time**
- **No longer a "per-symbol"** error probability
- Error patterns tend to form **burst**

The burst-noise channel

Burst-Noise Channel (Gilbert-Elliot model)

- Markov chain with two states **B** "bad", **G** "good"

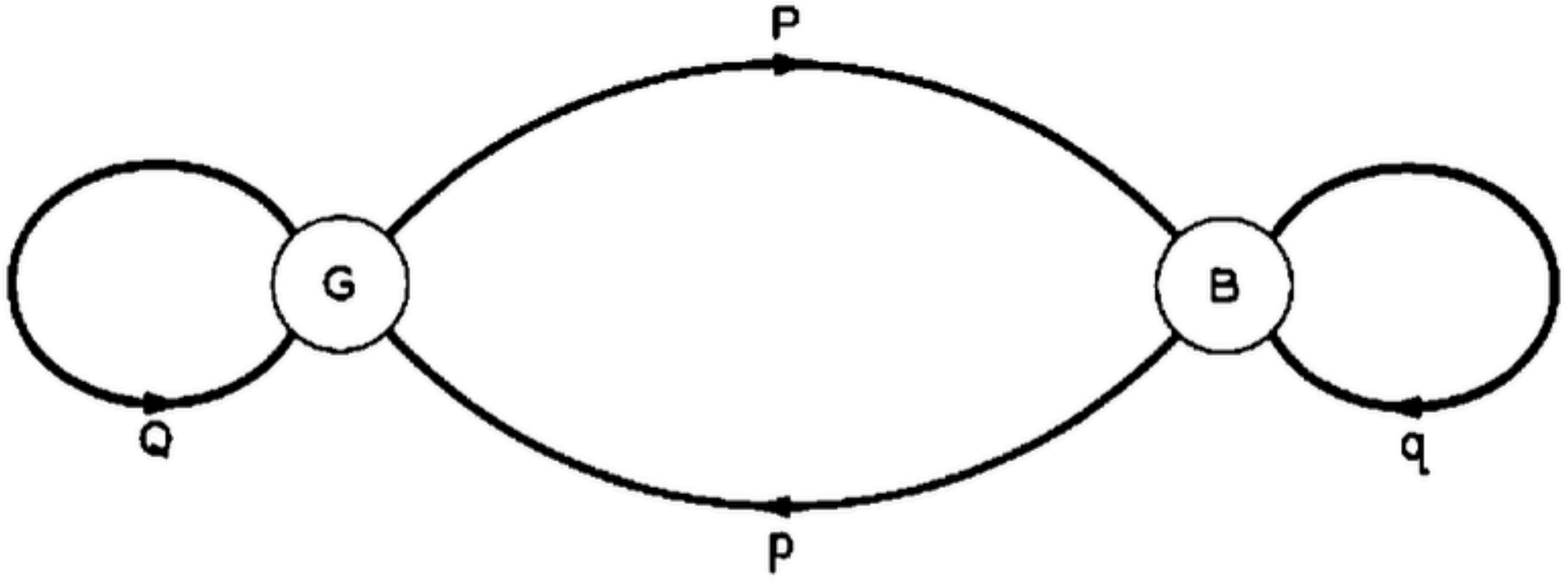


Fig. 1 — Transition diagram for the Markov chain.

E. N. Gilbert, "Capacity of a burst-noise channel," in The Bell System Technical Journal, vol. 39, no. 5, pp. 1253-1265, Sept. 1960.

The burst-noise channel

The following 500 digits form a typical sample of burst-noise with parameters $P = 0.03$, $p = 0.25$, $h = 0.5$, produced by using random numbers:

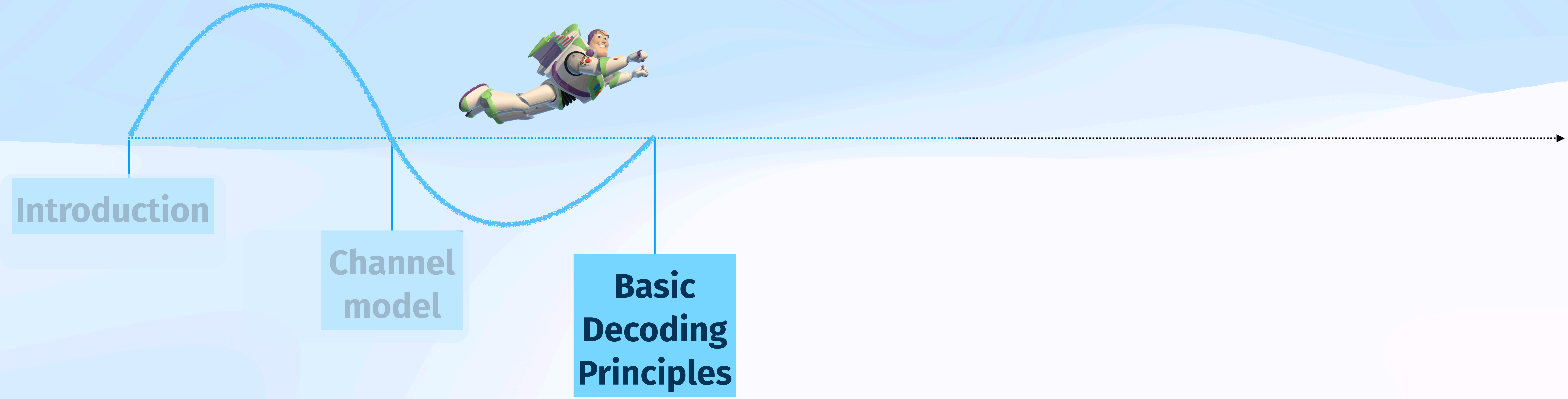
$$0^{62}110^{17}10^{46}110101110^{11}110^{15}10^{42}10^{28}110^{90}10^{37}$$

$$110^{5}10010^{35}1011010^{23}110^{4}10^{18}10^{15}1101110110110^{5}.$$

The exponents are run lengths; i.e., 0^{62} denotes a run of 62 consecutive zeros. As expected, long runs of good digits separate the bursts.

E. N. Gilbert, "Capacity of a burst-noise channel," in The Bell System Technical Journal, vol. 39, no. 5, pp. 1253-1265, Sept. 1960.

Part 1 : Hamming metric



- Maximum Likelihood - Nearest codeword - Syndrome decoding
- Bounding the radius (BMD, BD, List decoding)

Linear Block Codes

Linear (Block) Code $[n, k, d]$**:**

A linear code C is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^n$.

- $k = dim_{\mathbb{F}_q}(C)$ is the **dimension**
- n is the **length**
- $d = \min_{\boldsymbol{c}_1, \boldsymbol{c}_2 \in C, \boldsymbol{c}_1 \neq \boldsymbol{c}_2} d_H(\boldsymbol{c}_1, \boldsymbol{c}_2)$ is the **minimum distance**

- $G \in \mathbb{F}_q^{k \times n}$ the matrix whose rows are a basis of C, is a **generator matrix**
- Let $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$, the **inner product** $< \boldsymbol{x}, \boldsymbol{y} >$ the **dual code** is :

$$C^{\perp} := \{\boldsymbol{h} \mid < \boldsymbol{h}, \boldsymbol{c} > = 0, \forall \boldsymbol{c} \in C\}$$

- A generator matrix $H \in \mathbb{F}_q^{(n-k) \times n}$ of $C^{\perp}$ is called **parity check matrix**

The decoder

Let C be an $[n, k, d]$ code, a **decoder** for C is a map

$$D : \mathbb{F}_q^n \to \mathbb{F}_q^n \cup \{\,?\,\}$$

such that $D(\boldsymbol{c}) = \boldsymbol{c}$ for all $\boldsymbol{c} \in C$.

A decoder is **complete** if it **always returns a codeword.**

Maximum-Likelihood and Nearest-codeword

Maximum-Likelihood decoder

$$D_{ML} : \mathbb{F}_q^n \to C$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n, D_{ML}(\boldsymbol{y}) = \boldsymbol{c}$ which maximizes $\mathbb{P}(\boldsymbol{y}$ received $\;|\; \boldsymbol{c}$ sent$)$

If there exist two codewords for which the corresponding conditional probability is the same, the decoder arbitrarily chooses one of them.

Nearest-codeword decoder

$$D_{Nc} : \mathbb{F}_q^n \to C$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n, D_{ML}(\boldsymbol{y}) = \boldsymbol{c}$ where

$$\boldsymbol{c} \in argmin_{\boldsymbol{c} \in C}\{d_H(\boldsymbol{y}, \boldsymbol{c})\} = \{\boldsymbol{c} \in C \mid \forall \boldsymbol{c}' \in C, d_H(\boldsymbol{c}, \boldsymbol{y}) \leq d_H(\boldsymbol{c}', \boldsymbol{y})\}$$

Maximum-Likelihood and Nearest-codeword

Maximum-Likelihood decoder

$$D_{ML} : \mathbb{F}_q^n \to C$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n, D_{ML}(\boldsymbol{y}) = \boldsymbol{c}$ which maximizes $\mathbb{P}(\boldsymbol{y}$ received $\mid \boldsymbol{c}$ sent)

If there exist two codewords for which the corresponding conditional probability is the same, the decoder arbitrarily chooses one of them.

Symmetric channels

Nearest-codeword decoder

$$D_{Nc} : \mathbb{F}_q^n \to C$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n, D_{ML}(\boldsymbol{y}) = \boldsymbol{c}$ where

$$\boldsymbol{c} \in argmin_{\boldsymbol{c} \in C}\{d_H(\boldsymbol{y}, \boldsymbol{c})\} = \{\boldsymbol{c} \in C \mid \forall \boldsymbol{c}' \in C, d_H(\boldsymbol{c}, \boldsymbol{y}) \leq d_H(\boldsymbol{c}', \boldsymbol{y})\}$$

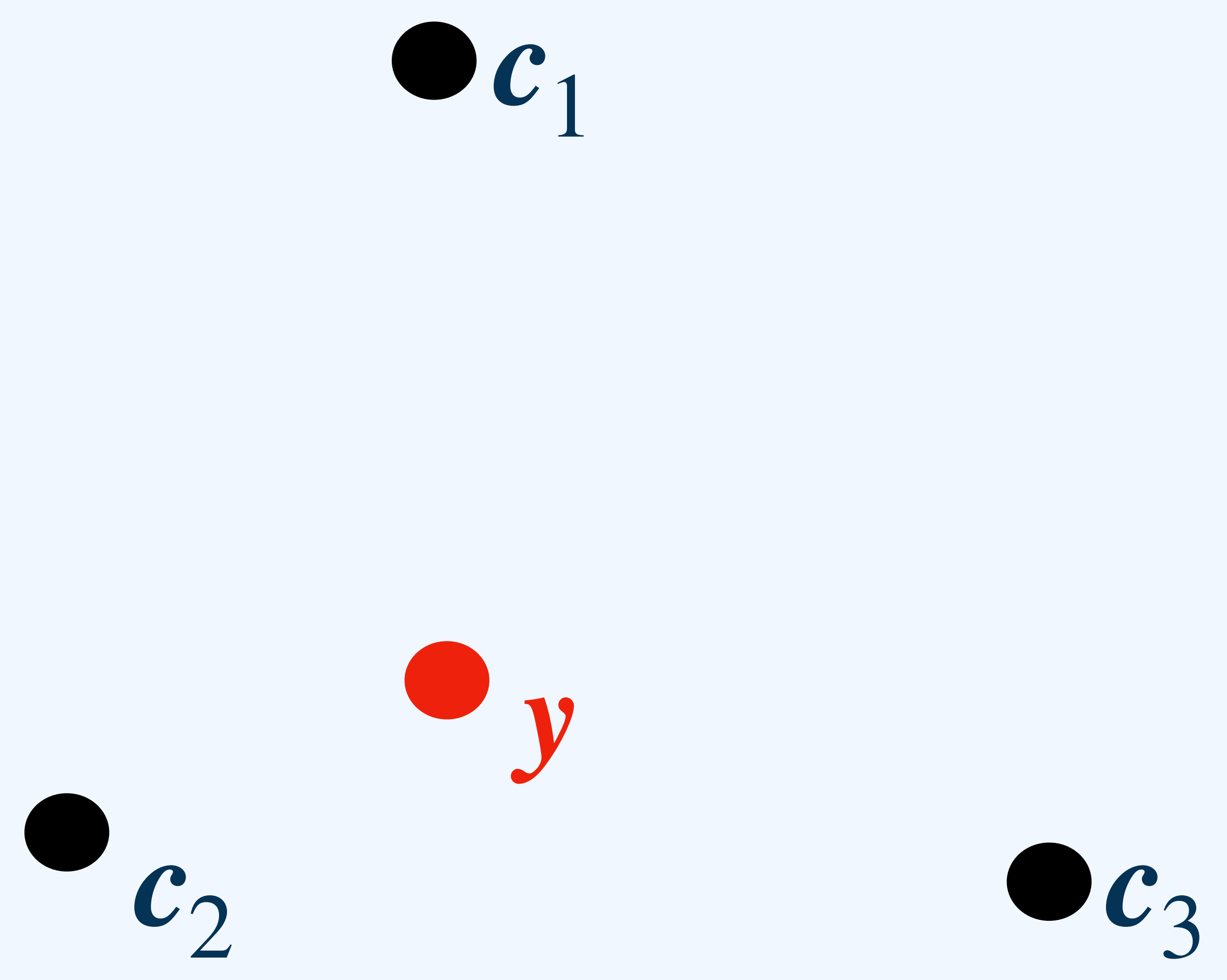
Nearest-codeword decoder, the linear case

Nearest-codeword decoder

$$D_{Nc} : \mathbb{F}_q^n \to C$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n, D_{ML}(\boldsymbol{y}) = \boldsymbol{c}$ where

$$\boldsymbol{c} \in argmin_{c \in C}\{d_H(\boldsymbol{y}, \boldsymbol{c})\} = \{\boldsymbol{c} \in C \mid \forall \boldsymbol{c}' \in C, d_H(\boldsymbol{c}, \boldsymbol{y}) \leq d_H(\boldsymbol{c}', \boldsymbol{y})\}$$



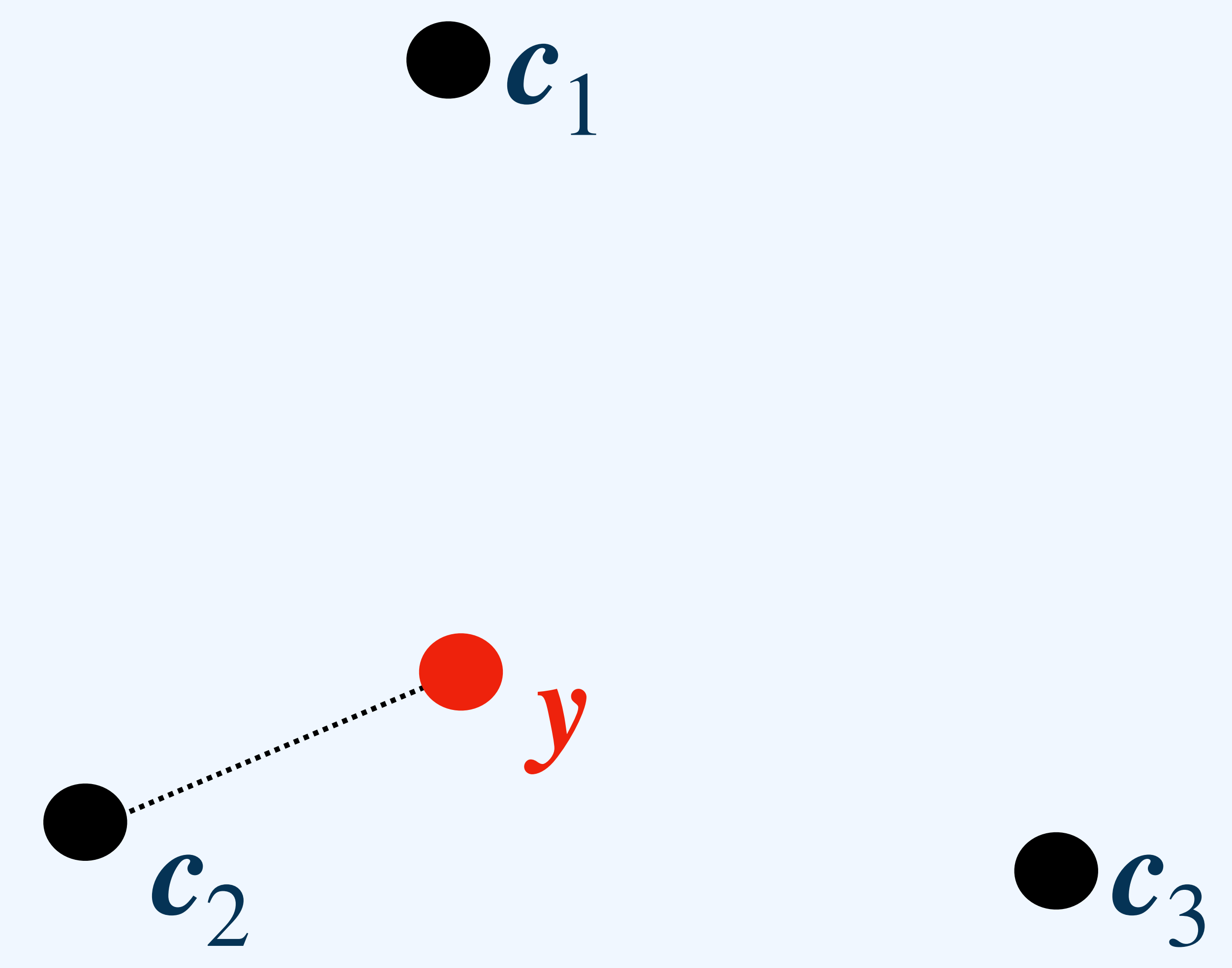
Nearest-codeword decoder, the linear case

Nearest-codeword decoder

$$D_{Nc} : \mathbb{F}_q^n \to C$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n, D_{ML}(\boldsymbol{y}) = \boldsymbol{c}$ where

$$\boldsymbol{c} \in argmin_{c \in C}\{d_H(\boldsymbol{y}, \boldsymbol{c})\} = \{\boldsymbol{c} \in C \mid \forall \boldsymbol{c}' \in C, d_H(\boldsymbol{c}, \boldsymbol{y}) \leq d_H(\boldsymbol{c}', \boldsymbol{y})\}$$



Nearest-codeword decoder, the linear case

Nearest-codeword decoding problem

Given $\boldsymbol{y}$ finding $\boldsymbol{c} \in C$ which minimizes $d(\boldsymbol{c}, \boldsymbol{y})$

Syndrome decoding problem

Let C be a linear code with parity check matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$.

Given $\boldsymbol{y} \in \mathbb{F}_q^n$ and $\boldsymbol{s} = \boldsymbol{H}\boldsymbol{y}^T$, finding $\boldsymbol{e} \in \mathbb{F}_q^n$ s.t. $\boldsymbol{H}\boldsymbol{e}^T = \boldsymbol{s}$ and it has minimum Hamming weight.

Nearest-codeword decoder, the linear case

Nearest-codeword decoding problem

Given $\boldsymbol{y}$ finding $\boldsymbol{c} \in C$ which minimizes $d_H(\boldsymbol{c}, \boldsymbol{y})$

$\Updownarrow$

Syndrome decoding problem

Let C be a linear code with parity check matrix $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$.

Given $\boldsymbol{y} \in \mathbb{F}_q^n$ and $\boldsymbol{s} = \boldsymbol{H}\boldsymbol{y}^T$, finding $\boldsymbol{e} \in \mathbb{F}_q^n$ s.t. $\boldsymbol{H}\boldsymbol{e}^T = \boldsymbol{s}$ and it has minimum Hamming weight.

Nearest-codeword decoder, the linear case

Nearest-codeword decoding problem

Given $\boldsymbol{y}$ finding $\boldsymbol{c} \in C$ which minimizes $d_H(\boldsymbol{c}, \boldsymbol{y})$

NP-complete

Syndrome decoding problem

Let C be a linear code with parity check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$.

Given $\boldsymbol{y} \in \mathbb{F}_q^n$ and $\boldsymbol{s} = \boldsymbol{H}\boldsymbol{y}^T$, finding $\boldsymbol{e} \in \mathbb{F}_q^n$ s.t. $\boldsymbol{H}\boldsymbol{e}^T = \boldsymbol{s}$ and it has minimum Hamming weight.

NP-complete

A. Vardy: *Algorithmic Complexity in Coding Theory and the Minimum Distance Problem.* STOC 1997:92-109.

E. Berlekamp, R. McEliece and H. van Tilborg, "*On the inherent intractability of certain coding problems* (Corresp.)," in IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 384-386, May 1978

Nearest-codeword decoder, the linear case

3-DIM matching problem

Given X, Y, Z finite sets with q elements and $T \subseteq X \times Y \times Z$, with $|T| = m$ decide whether there exists $M \subseteq T$, $|M| = q$ s.t. each element of X, Y, Z occurs in exactly one triple of M.

$$X = Y = Z = \{1,2,3,4\}$$

$$T = \{(1,2,1), (1,3,2), (2,1,4), (2,2,3), (3,1,1), (4,4,4)\}$$

E. Berlekamp, R. McEliece and H. van Tilborg, "*On the inherent intractability of certain coding problems* (Corresp.)," in IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 384-386, May 1978

Nearest-codeword decoder, the linear case

3-DIM matching problem

Given X, Y, Z finite sets with q elements and $T \subseteq X \times Y \times Z$, with $|T| = m$ decide whether there exists $M \subseteq T$, $|M| = q$ s.t. each element of X, Y, Z occurs in exactly one triple of M.

$$X = Y = Z = \{1,2,3,4\}$$

$$T = \{(1,2,1), (1,3,2), (2,1,4), (2,2,3), (3,1,1), (4,4,4)\}$$

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

E. Berlekamp, R. McEliece and H. van Tilborg, "*On the inherent intractability of certain coding problems* (Corresp.)," in IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 384-386, May 1978

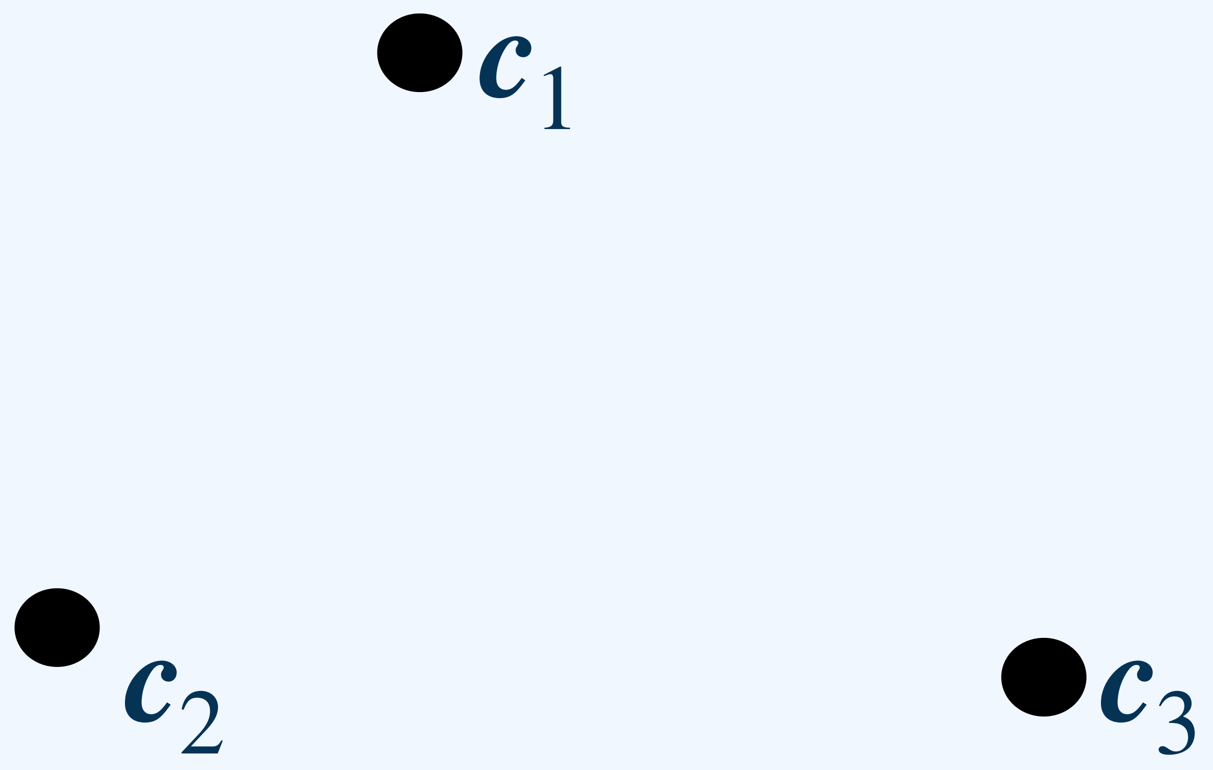
Unique Decoding Capability

Theorem (Unique Decoding Capability)

Let C be an $[n, k, d]$ code and $\tau_0 = \lfloor (d-1)/2 \rfloor$.

Then for any pair of distinct codewords $\boldsymbol{c}_1, \boldsymbol{c}_2$,

$$B^{\tau_0}(\boldsymbol{c_1}) \cap B^{\tau_0}(\boldsymbol{c_2}) = \varnothing$$



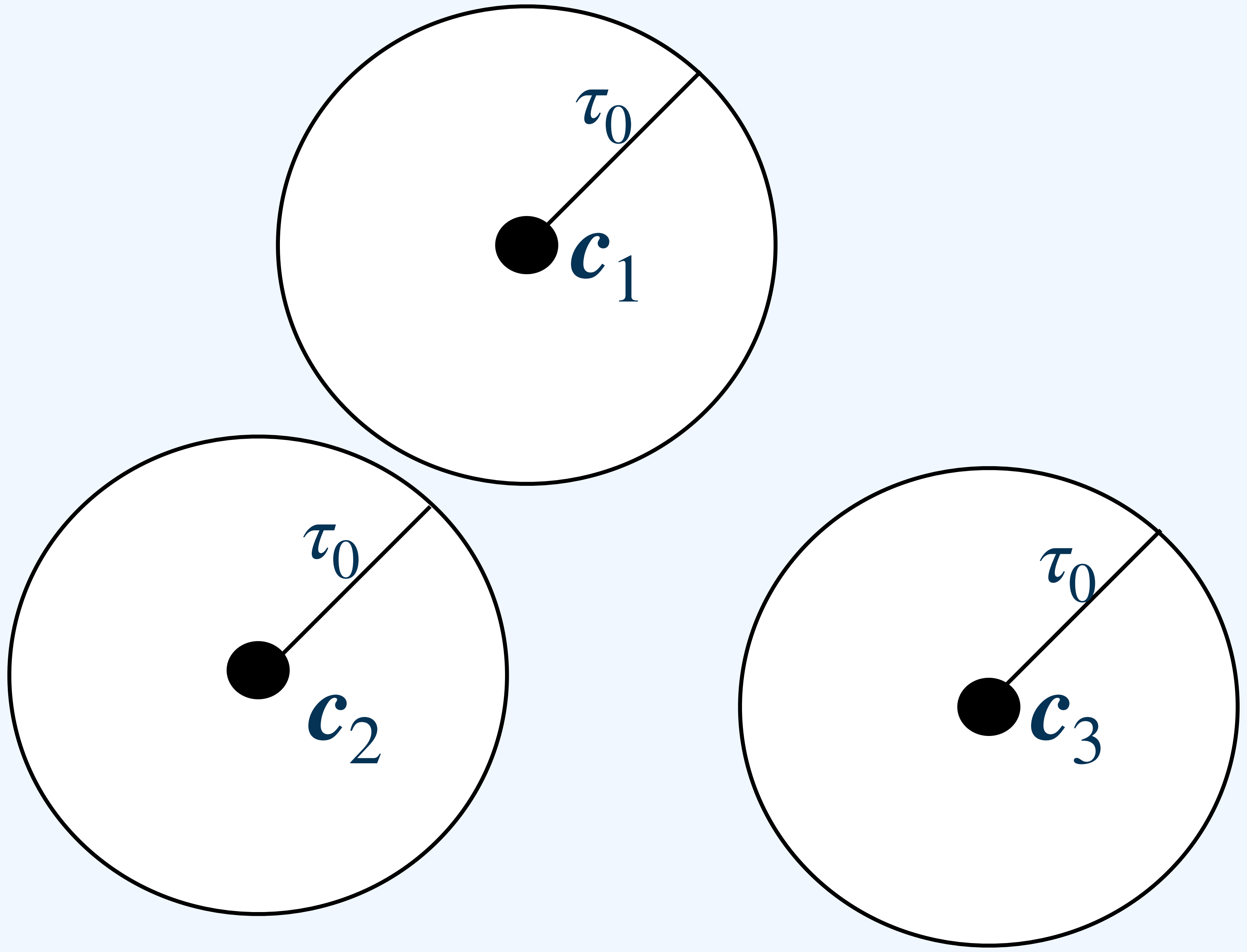
Unique Decoding Capability

Theorem (Unique Decoding Capability)

Let C be an $[n, k, d]$ code and $\tau_0 = \lfloor (d-1)/2 \rfloor$.

Then for any pair of distinct codewords $\boldsymbol{c}_1, \boldsymbol{c}_2$,

$$B^{\tau_0}(\boldsymbol{c_1}) \cap B^{\tau_0}(\boldsymbol{c_2}) = \varnothing$$



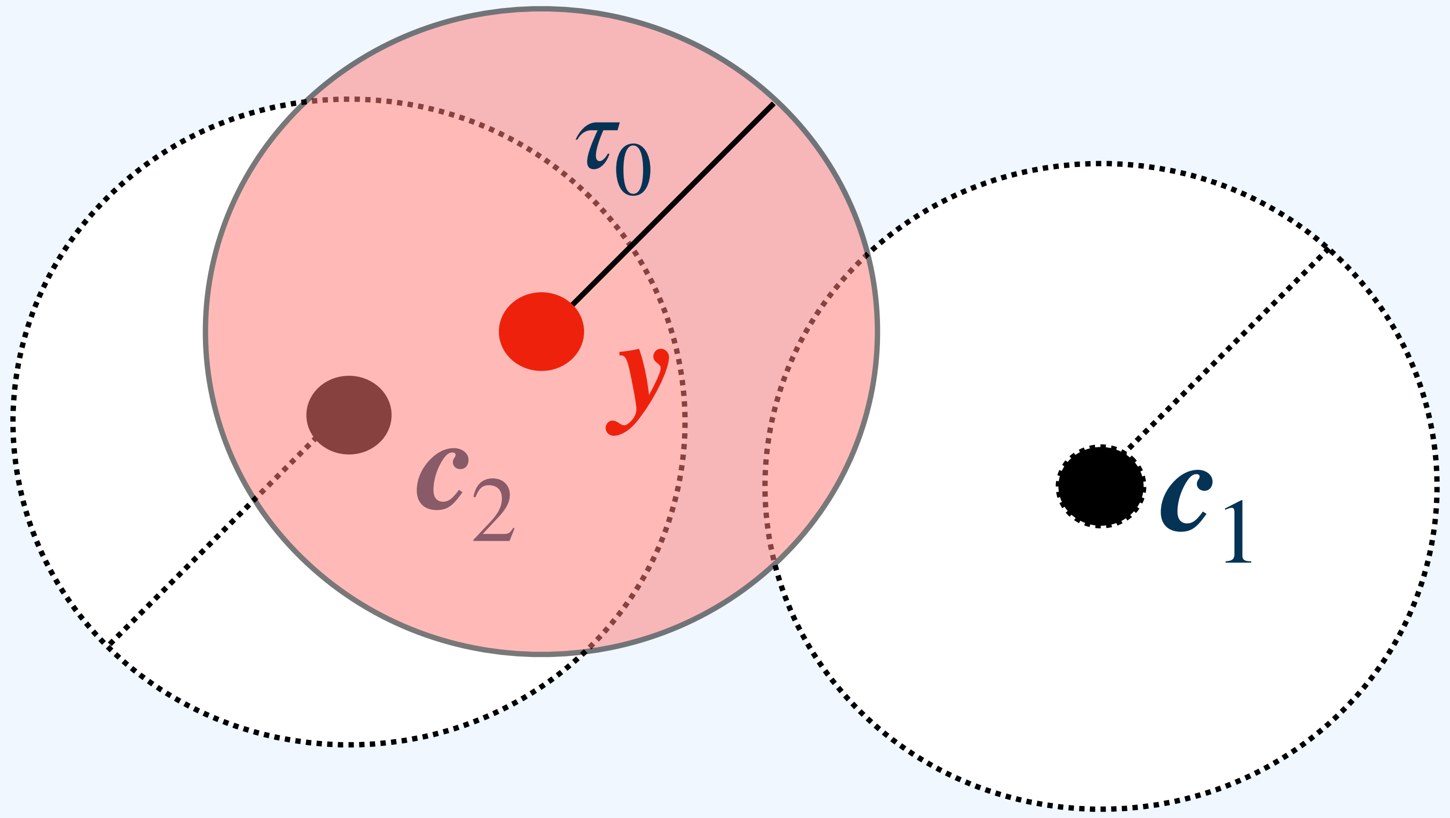
Bounded Minimum Distance decoder

Bounded Minimum Distance decoder

$$D_{BMD} : \mathbb{F}_q^n \to C \cup \{\,?\,\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n,$

$$D_{BMD}(\boldsymbol{y}) = \begin{cases} \boldsymbol{c} & \text{if } B^{\tau_0}(\boldsymbol{y}) \cap C \neq \emptyset \\ ? & \text{otherwise} \end{cases}$$



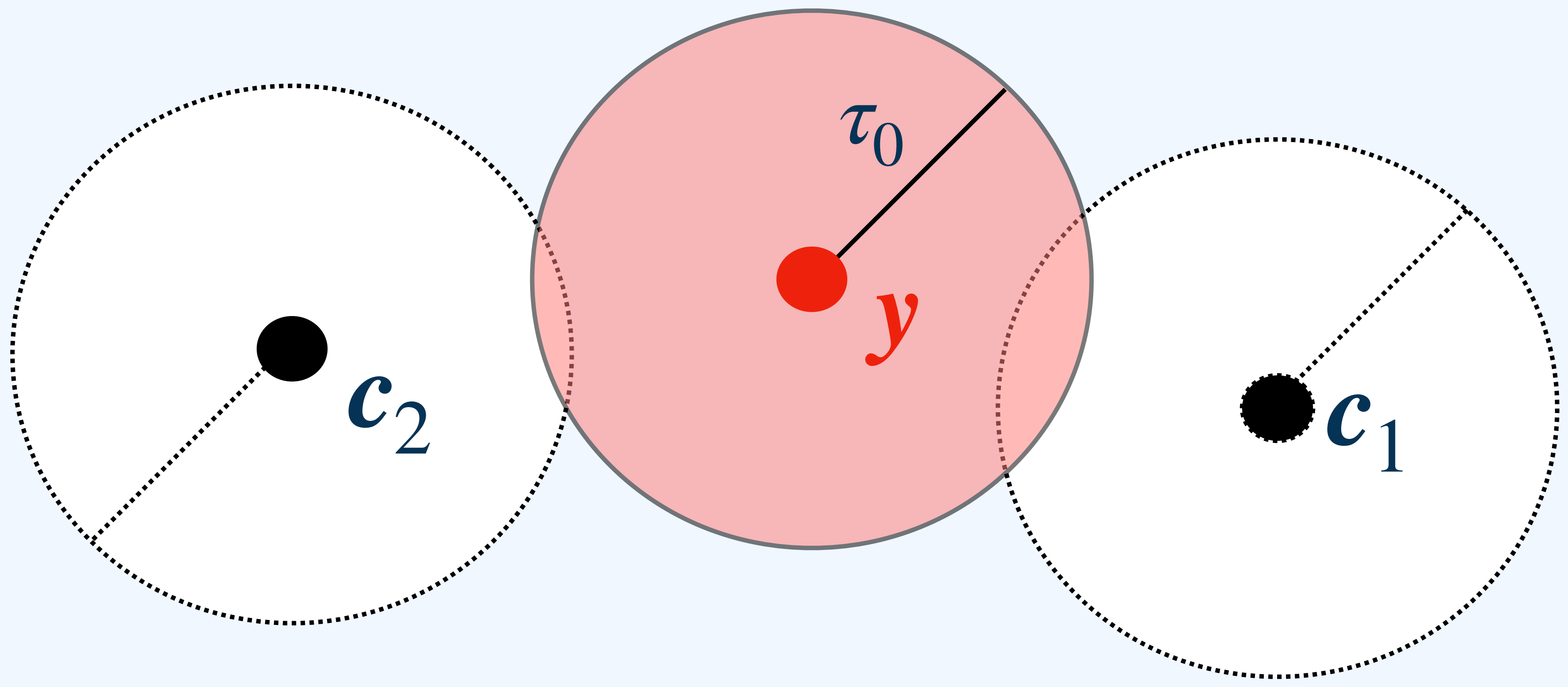
Bounded Minimum Distance decoder

Bounded Minimum Distance decoder

$$D_{BMD} : \mathbb{F}_q^n \to C \cup \{\,?\,\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n,$

$$D_{BMD}(\boldsymbol{y}) = \begin{cases} \boldsymbol{c} & \text{if } B^{\tau_0}(\boldsymbol{y}) \cap C \neq \varnothing \\ ? & \text{otherwise} \end{cases}$$



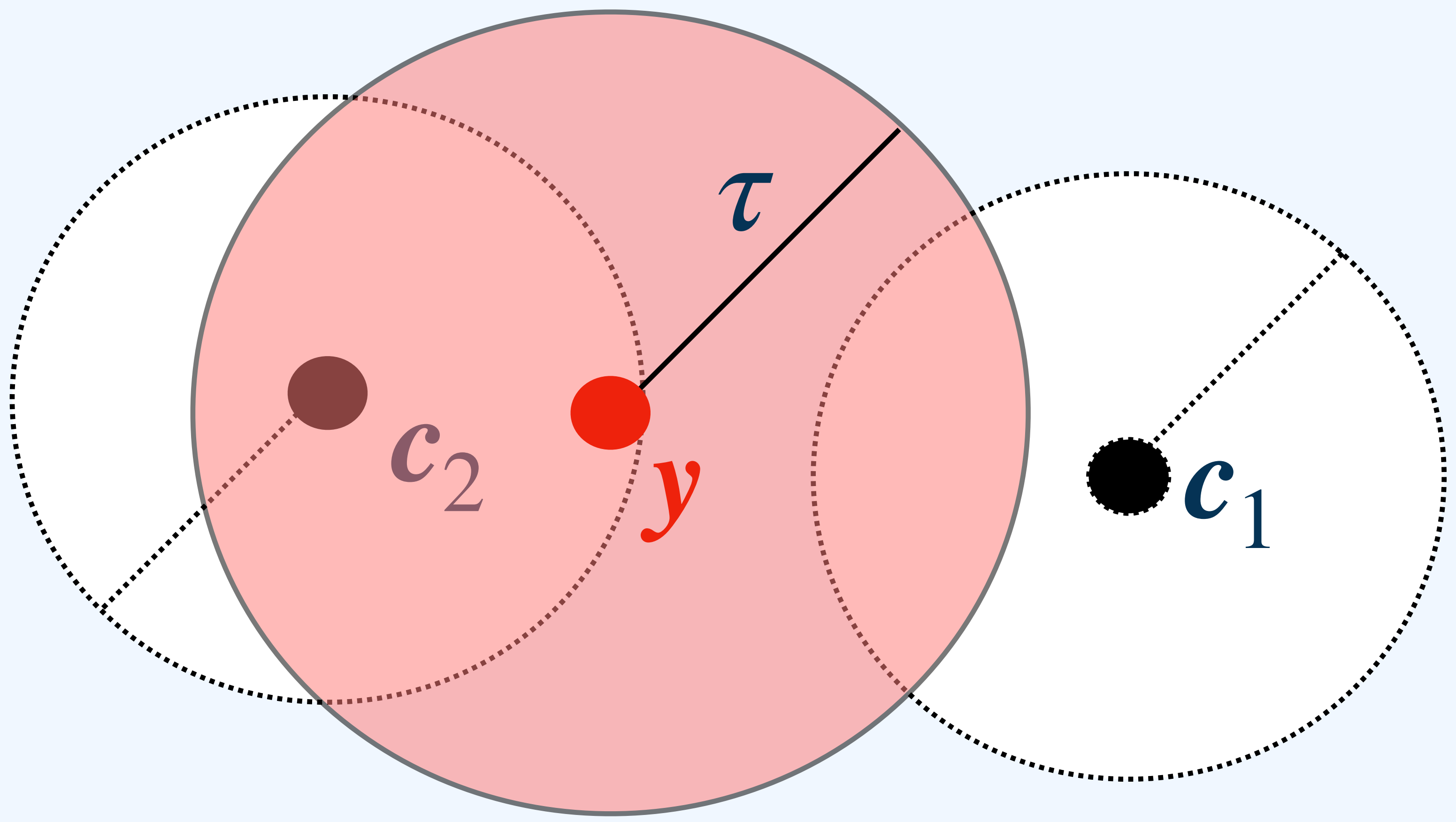
Bounded Distance decoder

Bounded Distance decoder for a general $\tau \geq \tau_0$

$$D_{BD} : \mathbb{F}_q^n \to C \cup \{?\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n$,

$$D_{BD}(\boldsymbol{y}) = \begin{cases} \boldsymbol{c} & \text{if } |B^\tau(\boldsymbol{y}) \cap C| = 1 \\ ? & \text{otherwise} \end{cases}$$



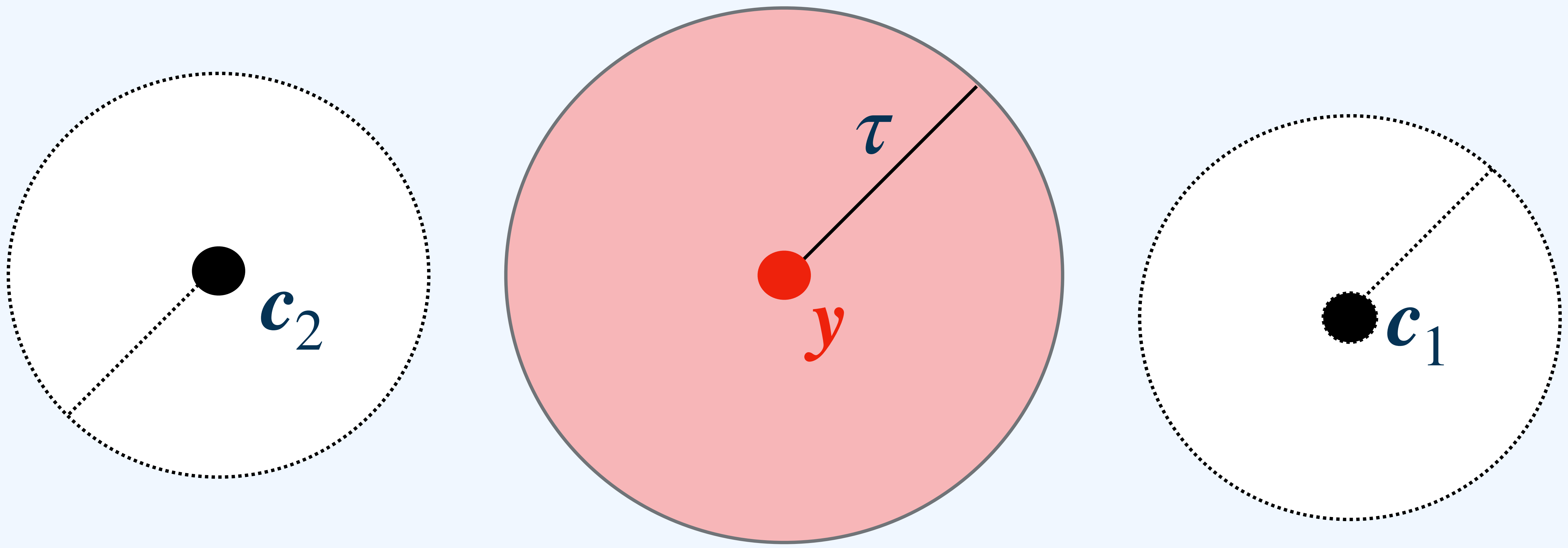
Bounded Distance decoder

Bounded Distance decoder for a general $\tau \geq \tau_0$

$$D_{BD} : \mathbb{F}_q^n \to C \cup \{?\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n,$

$$D_{BD}(\boldsymbol{y}) = \begin{cases} \boldsymbol{c} & \text{if } |B^\tau(\boldsymbol{y}) \cap C| = 1 \\ ? & \text{otherwise} \end{cases}$$



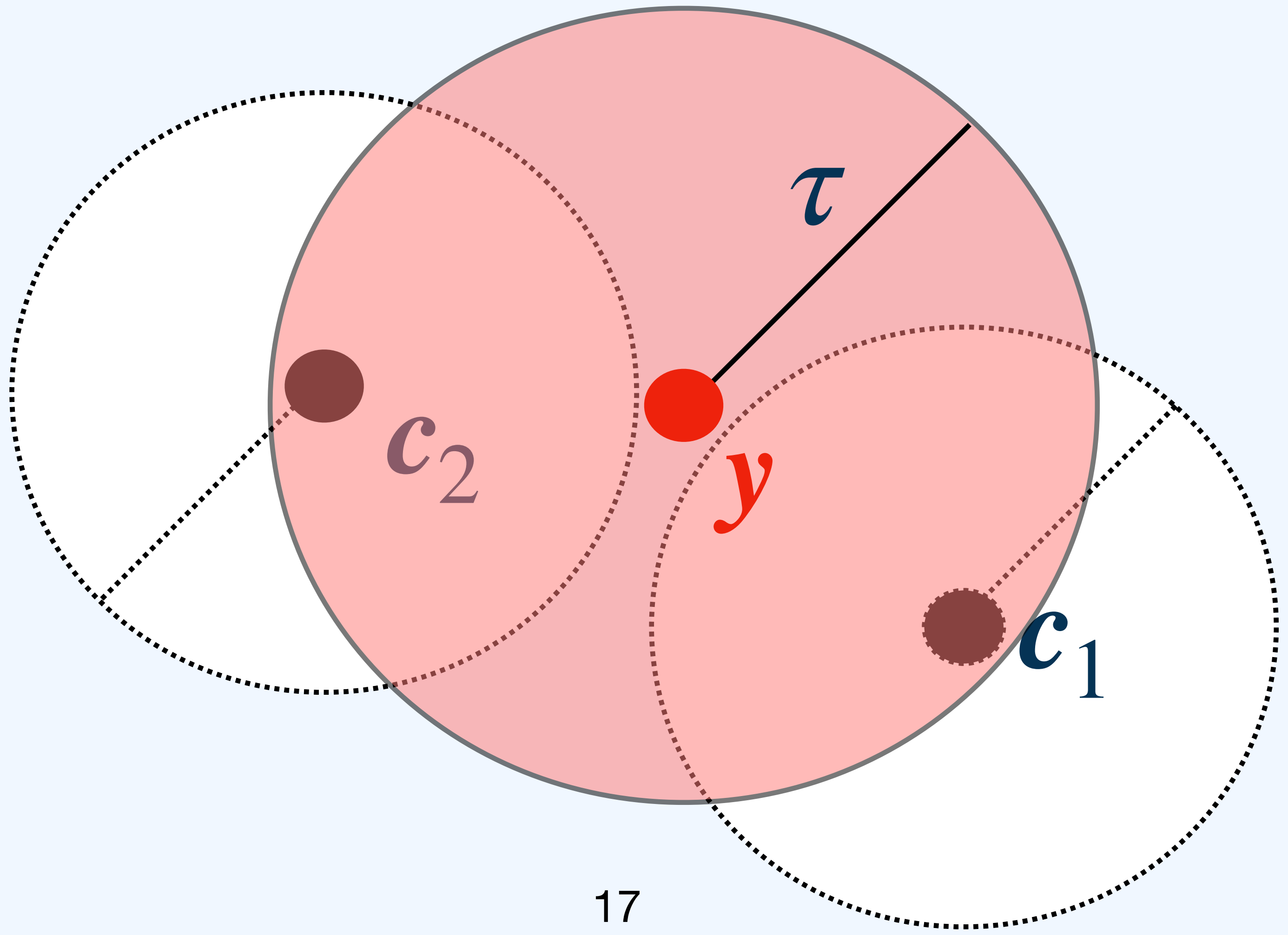
Bounded Distance decoder

Bounded Distance decoder for a general $\tau \geq \tau_0$

$$D_{BD} : \mathbb{F}_q^n \to C \cup \{?\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n,$

$$D_{BD}(\boldsymbol{y}) = \begin{cases} \boldsymbol{c} & \text{if } |B^{\tau}(\boldsymbol{y}) \cap C| = 1 \\ ? & \text{otherwise} \end{cases}$$



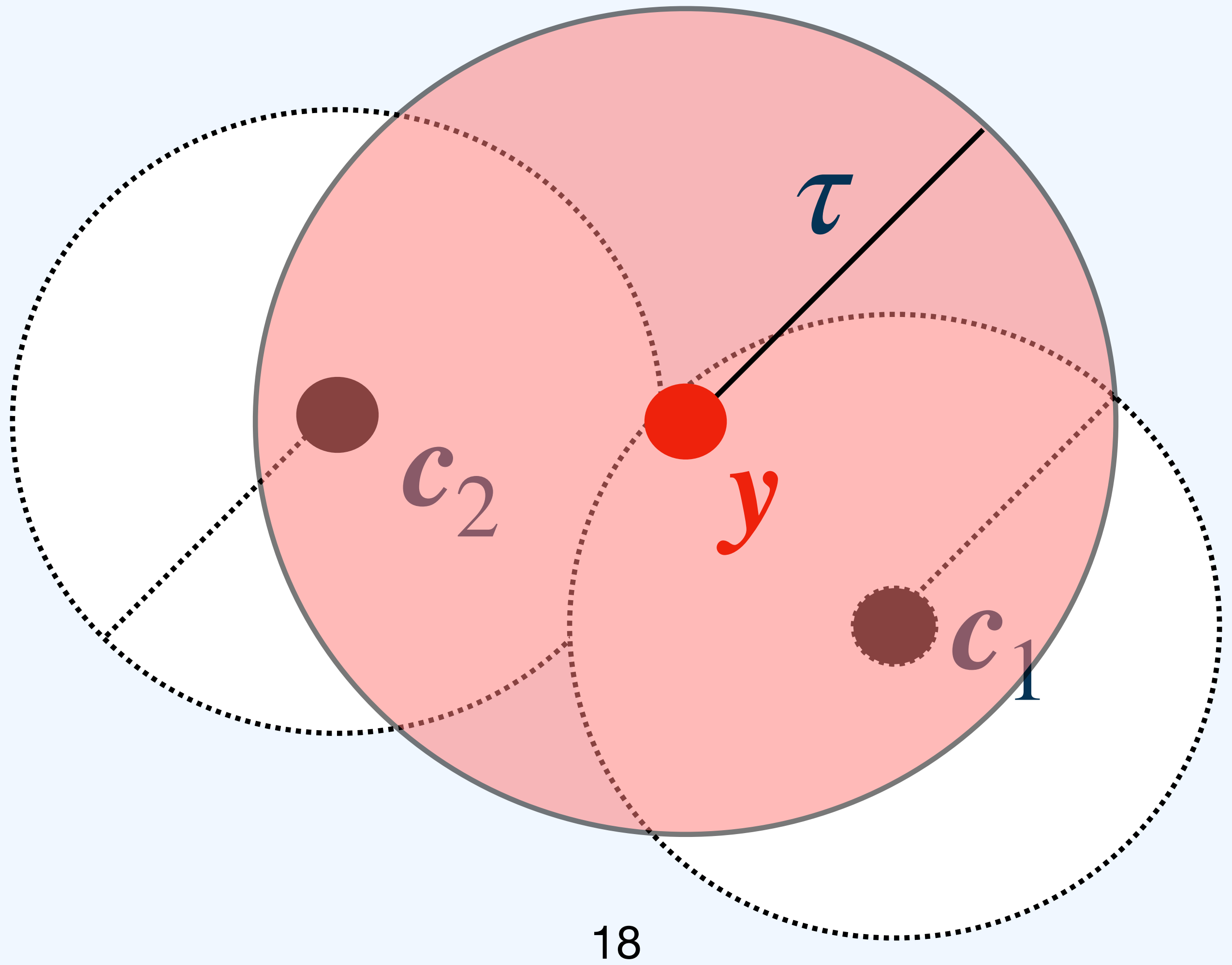
List decoder

List decoder for a general $\tau \geq \tau_0$

$$D_L : \mathbb{F}_q^n \to \mathscr{P}(C)$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n$,

$$D_L(\boldsymbol{y}) = \begin{cases} B^\tau(\boldsymbol{y}) \cap C & \text{if } B^\tau(\boldsymbol{y}) \cap C \neq \varnothing \\ ? & \text{otherwise} \end{cases}$$



List decoder

List decoder for a general $\tau \geq \tau_0$

$$D_L : \mathbb{F}_q^n \to \mathscr{P}(C)$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n$,

$$D_L(\boldsymbol{y}) = \begin{cases} B^\tau(\boldsymbol{y}) \cap C & \text{if } B^\tau(\boldsymbol{y}) \cap C \neq \varnothing \\ ? & \text{otherwise} \end{cases}$$

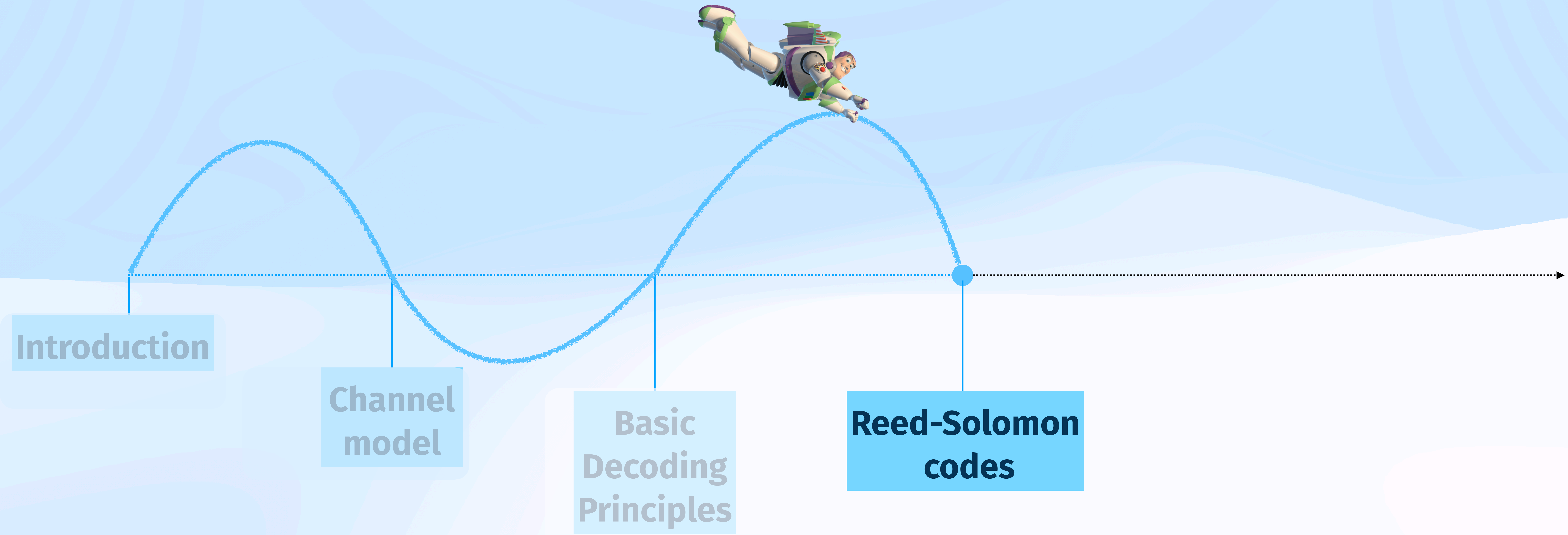
Theorem (Johnson Bound)

Let C be an $[n, k, d]$ code.

If $\tau/n < J_q(d/n)$ then C is a **list decodable code** with list size $poly(n)$ where,

$$J_q(\delta) = 1 - \frac{1}{q} - \sqrt{\left(1 - \frac{1}{q}\right)(1 - \delta)}$$

Part 1 : Hamming metric



- Generalized Reed-Solomon codes
- Reed-Solomon codes

Generalized Reed Solomon Codes

Generalized Reed Solomon codes

Let $k \leq n \leq q, \ \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^n$ where $\alpha_i \neq \alpha_j$ and $v_1, \ldots, v_n \in \mathbb{F}_q^n$ nonzero elements

$$C_{GRS}(n,k) := \{(v_1 F(\alpha_1), \ldots, v_n F(\alpha_n)) \mid F \in \mathbb{F}_q[x]_{<k}\}$$

MDS codes : $d = n - k + 1$

Theorem:

The **dual of a GRS** code **is a GRS code** where $\forall i \in [n], v_i' := \dfrac{1}{v_i \prod_{j \in [n] \setminus \{i\}} (\alpha_i - \alpha_j)}$

Reed Solomon Codes

Reed Solomon codes

Let $k \leq n \leq q$ and $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^n$ where $\alpha_i \neq \alpha_j$.

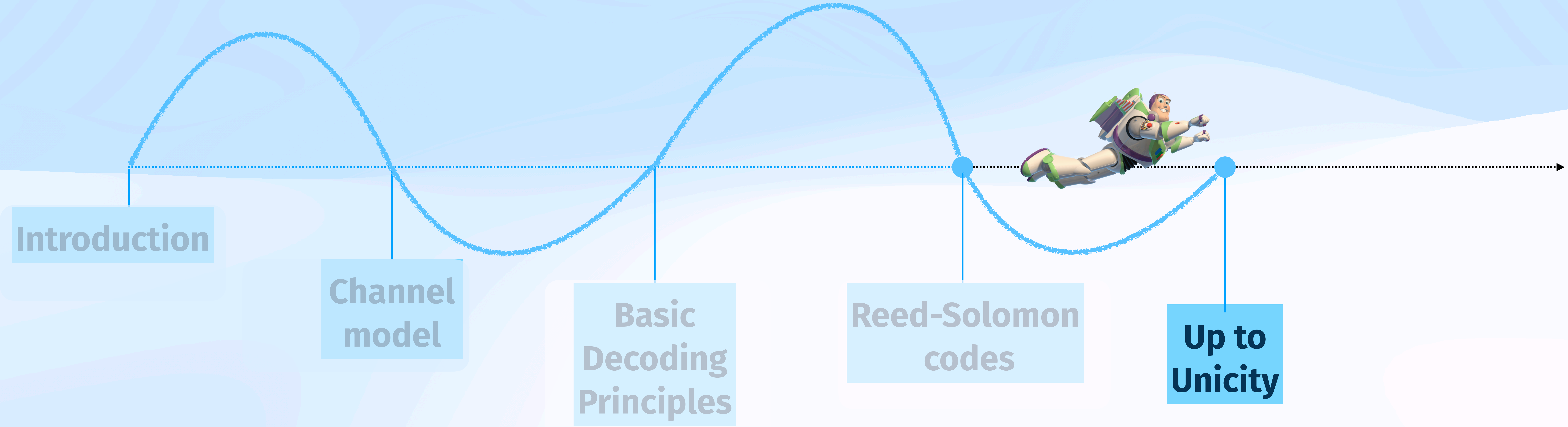
$$C_{RS}(n,k) := \{(F(\alpha_1), \ldots, F(\alpha_n) \mid F \in \mathbb{F}_q[x]_{<k}\}$$

MDS codes : $d = n - k + 1$

Corollary:

The **dual of a RS** code **is a GRS code** where $\forall i \in [n],\ \ \ell_i' := \dfrac{1}{\prod_{j \in [n] \setminus \{i\}} (\alpha_i - \alpha_j)}$

Part 1 : Hamming metric



- Welch-Berlekamp
- Syndrome-based decoding

Reed Solomon Codes

Reed Solomon codes

Let $k \leq n \leq q$ and $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^n$ where $\alpha_i \neq \alpha_j$.

$$C_{RS}(n,k) := \{(F(\alpha_1), \ldots, F(\alpha_n) \mid F \in \mathbb{F}_q[x]_{<k}\}$$

MDS codes : $d = n - k + 1$

$$D_{BMD} : \mathbb{F}_q^n \to \mathbb{F}_q[x]_{<k} \cup \{\,?\,\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_q^n$,

$$D_{BMD}(\boldsymbol{y}) = \begin{cases} F(x) \text{ s.t. } \boldsymbol{c} = (F(\alpha_1), \ldots, F(\alpha_n)) \in B^{\tau_0}(\boldsymbol{y}) & \text{if } B^{\tau_0}(\boldsymbol{y}) \cap C \neq \emptyset \\ ? & \text{otherwise} \end{cases}$$

Rational Reconstruction Problem

Rational Function Reconstruction Problem

Let $\mathbb{K}$ be a field, $A(x), Y(x) \in \mathbb{F}_q[x]$ s.t. $\deg(Y) < \deg(A)$, $v < \deg(A)$ and $d < \deg(A) - \deg(Y)$

Find $(V, D) \in \mathbb{K}[x]^2$ such that,

$$\begin{cases} V(x) = D(x)Y(x) \bmod A(x) \\ \deg(V) < v \\ \deg(D) < d \end{cases}$$

If $\deg(A) \geq v + d - 1$ the linear system admits a **unique solution**

$\downarrow$

Extended Euclidean Algorithm

Welch-Berlekamp key equation

Let $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ be a **received word**, where $\boldsymbol{c} \in C_{RS}(n, k)$

- $E := \{i \mid e_i \neq 0\}$ error support, $|E| = \varepsilon$
- $G := \prod_{i=1}^{n}(x - \alpha_i)$ and $\Lambda := \prod_{i \in E}(x - \alpha_i)$

Lagrange interpolator polynomial of $\boldsymbol{y}$

$$\boxed{V(x) = D(x)Y(x) \bmod G(x)}$$

$\deg(V) \leq \varepsilon + k - 1$ $\deg(D) \leq \varepsilon$

If $\deg(G) = n \geq (\varepsilon + k) + (\varepsilon + 1) - 1 \implies$ the rational reconstruction problem admits a unique solution, i.e. the minimal solution is $(\Lambda(x)f(x), \Lambda(x))$

Welch-Berlekamp key equation

Let $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ be a **received word**, where $\boldsymbol{c} \in C_{RS}(n, k)$

- $E := \{i \mid e_i \neq 0\}$ error support, $|E| = \varepsilon$
- $G := \prod_{i=1}^{n}(x - \alpha_i)$ and $\Lambda := \prod_{i \in E}(x - \alpha_i)$

Lagrange interpolator polynomial of $\boldsymbol{y}$

$$\boxed{V(x) = D(x)Y(x) \bmod G(x)}$$

$\deg(V) \leq \varepsilon + k - 1$

$\deg(D) \leq \varepsilon$

If $\deg(G) = n \geq (\varepsilon + k) + (\varepsilon + 1) - 1 \Longrightarrow \varepsilon \leq \dfrac{n-k}{2} = \tau_0$ then we can construct a BMD decoder

Gao Decoding Algorithm

Given $\boldsymbol{y}$ a received word,

1. Compute the Lagrange interpolator $Y(x)$ of $\boldsymbol{y}$
2. Solve the corresponding rational function reconstruction problem $\rightarrow (V, D)$
3. Perform the Euclidean division of V by D
   - if the remainder is 0 $\rightarrow$ returns $F = V/D$
   - Otherwise outputs $?$

S. Gao. *A New Algorithm for Decoding Reed-Solomon Codes*. In Communications, Information and Network Security, pg. 55-68, Springer US, 2003

Syndrome key equation

Let $C_{RS}(n,k)$ a Reed Solomon code with parity check $H = V^T_{n,n-k} \times Diag(\ell_1, \ldots, \ell_n)$

Let $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ and $E = \{i \mid e_i \neq 0\}$, where $\varepsilon = |E|$

Syndrome $\boldsymbol{s} = H\boldsymbol{y}^T = H\boldsymbol{e}^T \longrightarrow$ Syndrome polynomial $S(x) := \sum_{m \in [n-k]} s_m x^m$

- $\Lambda := \prod_{i \in E} (x - \alpha_i)$ error locator polynomial
- $\Gamma := \sum_{i \in E} e_i \ell_i \prod_{j \in E \setminus \{i\}} (x - \alpha_j)$ error evaluator polynomial

$$\boxed{V(x) = S(x)D(x) \bmod x^{n-k}}$$

$\deg(V) < \varepsilon$ $\qquad$ $\deg(D) \leq \varepsilon$

If $n - k \geq \varepsilon + (\varepsilon + 1) - 1 \Longrightarrow \varepsilon \leq \dfrac{n-k}{2} = \tau_0$ then we can construct a BMD decoder

Syndrome Decoding Algorithm

Given $\boldsymbol{y}$ a received word,

1. Compute the syndrome polynomial $S(x)$
2. Solve the corresponding Padé approximation problem $\rightarrow (V, D)$
3. Reconstruct the error locator and the error evaluator
4. **Find error locators and evaluators Forney algorithm**

$\downarrow$

This decoder never fails: it always return a codeword

Complete decoder

Part 1 : Hamming metric

Introduction

Channel model

Basic Decoding Principles

Reed-Solomon codes

Up to Unicity

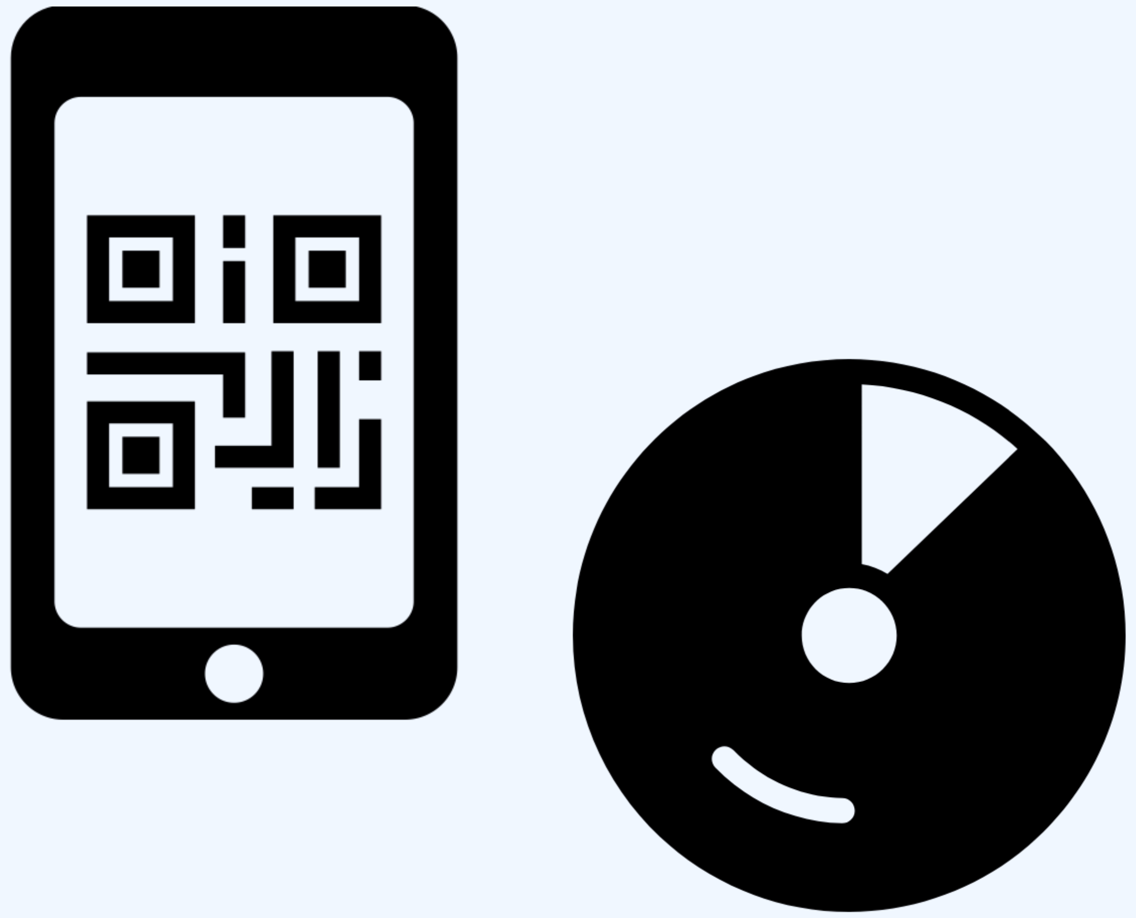
And Beyond

- Interleaving
- Power Decoding
- List Decoding

Interleaving

Burst Channel model

Goal: **dispatch** the burst errors and apply classical error correction



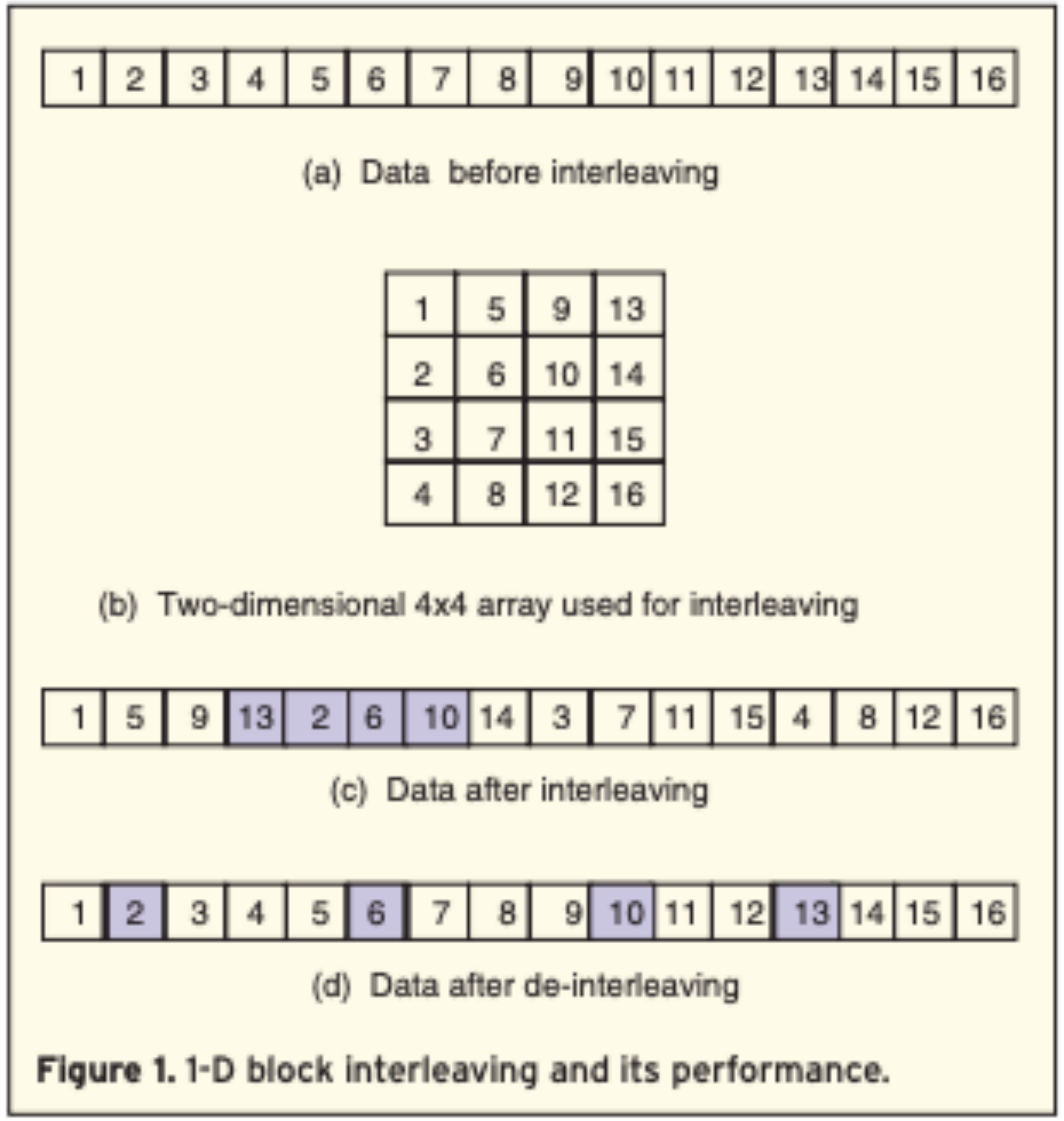


Figure 1. 1-D block interleaving and its performance.

Interleaved Reed-Solomon codes

Interleaved Reed Solomon codes

Let $k \leq n \leq q$, $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^n$ where $\alpha_i \neq \alpha_j$ and $l \geq 1$

$$C_{IRS}(n, k) := \{(\boldsymbol{f}(\alpha_1), \ldots, \boldsymbol{f}(\alpha_n))^T \mid \boldsymbol{f} \in \mathbb{F}_q[x]_{<k}^{l \times 1}\}$$

MDS code : $d = n - k + 1$

$$\begin{pmatrix} f_1(\alpha_1), f_1(\alpha_2), \ldots, f_1(\alpha_n) \\ f_2(\alpha_1), f_2(\alpha_2), \ldots, f_2(\alpha_n) \\ \vdots \\ f_l(\alpha_1), f_l(\alpha_2), \ldots, f_l(\alpha_n) \end{pmatrix}$$

Interleaved Reed-Solomon codes

Interleaved Reed Solomon codes

Let $k \leq n \leq q$, $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^n$ where $\alpha_i \neq \alpha_j$ and $l \geq 1$

$$C_{IRS}(n,k) := \{(\boldsymbol{f}(\alpha_1), \ldots, \boldsymbol{f}(\alpha_n))^T \mid \boldsymbol{f} \in \mathbb{F}_q[x]_{<k}^{l \times 1}\}$$

MDS code : $d = n - k + 1$

$$\begin{pmatrix} f_1(\alpha_1), f_1(\alpha_2), \ldots, f_1(\alpha_n) \\ f_2(\alpha_1), f_2(\alpha_2), \ldots, f_2(\alpha_n) \\ \vdots \\ f_l(\alpha_1), f_l(\alpha_2), \ldots, f_l(\alpha_n) \end{pmatrix}$$

Burst VS Interleaving algebraic channel model

Burst Channel model

Goal: **dispatch** the burst errors and apply classical error correction

$$\begin{pmatrix} f_1(\alpha_1), f_1(\alpha_2), \ldots, f_1(\alpha_n) \\ f_2(\alpha_1), f_2(\alpha_2), \ldots, f_2(\alpha_n) \\ \vdots \\ f_l(\alpha_1), f_l(\alpha_2), \ldots, f_l(\alpha_n) \end{pmatrix}$$

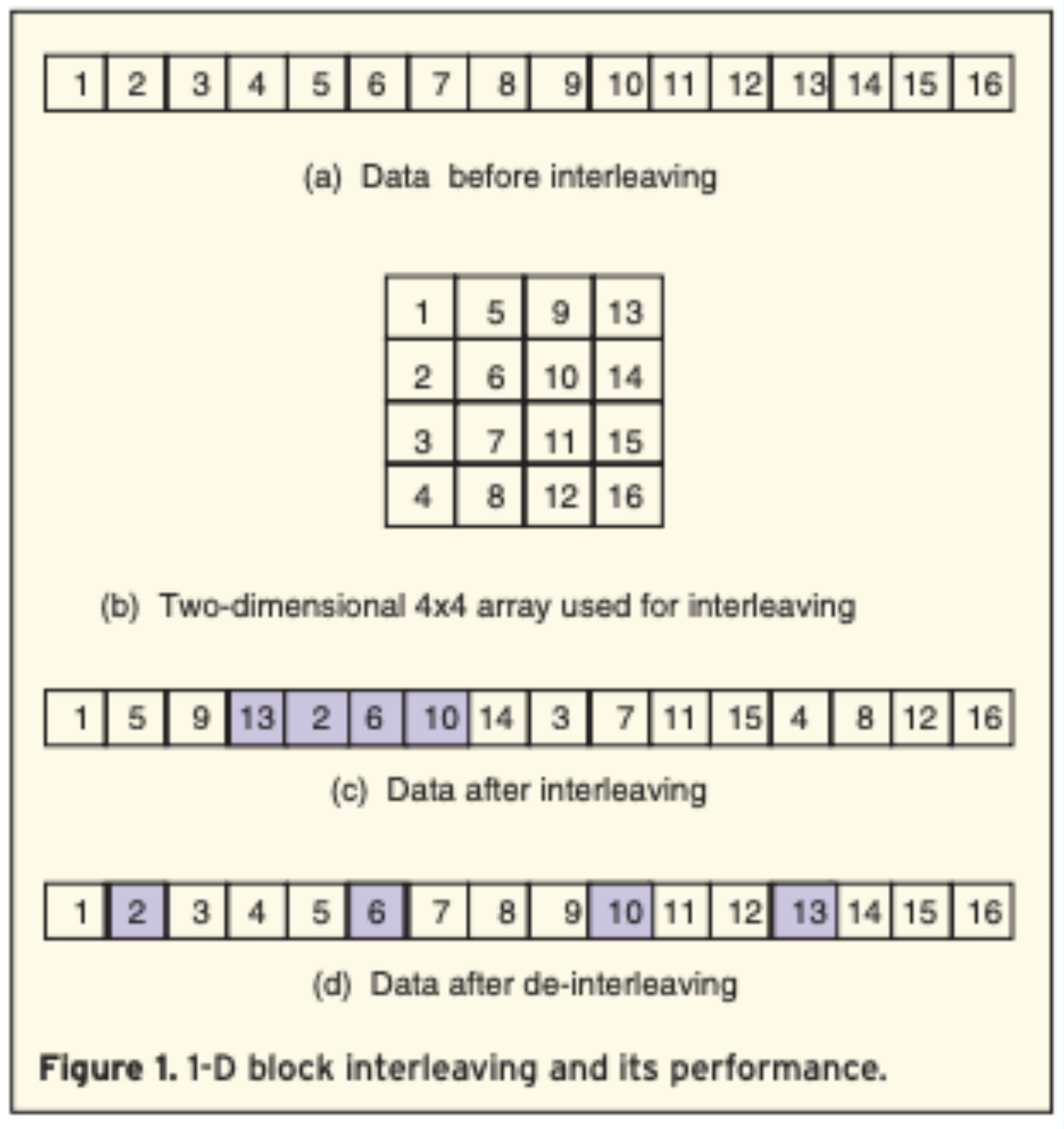


Figure 1. 1-D block interleaving and its performance.

A real burst channel is ***temporal***, while interleaving assumes ***position-aligned*** multi-symbol errors.

Interleaved Reed-Solomon codes

- Let $R = \begin{pmatrix} f_1(\alpha_1), f_1(\alpha_2), \ldots, f_1(\alpha_n) \\ f_2(\alpha_1), f_2(\alpha_2), \ldots, f_2(\alpha_n) \\ \vdots \\ f_l(\alpha_1), f_l(\alpha_2), \ldots, f_l(\alpha_n) \end{pmatrix} + \mathscr{E} \in \mathbb{F}_q^{l \times n}$ be a received matrix
- $\mathscr{E} \in \mathbb{F}_q^{l \times n}$ is the **error matrix** and $E := \{i \mid \mathscr{E}^i \neq \mathbf{0}\}$ is the **error support,** $|E| = \varepsilon$
- $\Lambda := \prod_{i \in E} (x - \alpha_i)$ **error locator** polynomial.

Lagrange interpolator polynomial of any R^i

$$\boxed{V_i(x) = D(x)Y_i(x) \bmod G(x)}$$

$\deg(V_i) \leq \varepsilon + k - 1$ $\quad$ $\deg(D) \leq \varepsilon$

Interleaved Reed-Solomon codes

- Let $R = \begin{pmatrix} f_1(\alpha_1), f_1(\alpha_2), \ldots, f_1(\alpha_n) \\ f_2(\alpha_1), f_2(\alpha_2), \ldots, f_2(\alpha_n) \\ \vdots \\ f_l(\alpha_1), f_l(\alpha_2), \ldots, f_l(\alpha_n) \end{pmatrix} + \mathscr{E} \in \mathbb{F}_q^{l \times n}$ be a received matrix
- $\mathscr{E} \in \mathbb{F}_q^{l \times n}$ is the **error matrix** and $E := \{i \mid \mathscr{E}^i \neq \mathbf{0}\}$ is the **error support**, $|E| = \varepsilon$
- $\Lambda := \prod_{i \in E} (x - \alpha_i)$ **error locator** polynomial.

Lagrange interpolator polynomial of any R^i

$$\boxed{V_i(x) = D(x)Y_i(x) \bmod G(x)}$$

Simultaneous Rational Function Reconstruction

$\deg(V_i) \leq \varepsilon + k - 1$ $\quad\quad$ $\deg(D) \leq \varepsilon$

Interleaved Reed-Solomon codes

Lagrange interpolator polynomial of any R^i

$$\boxed{V_i(x) = D(x)Y_i(x) \bmod G(x)}$$

Simultaneous Rational Function Reconstruction

$\deg(V_i) \leq \varepsilon + k - 1$

$\deg(D) \leq \varepsilon$

If $nl \geq l(\varepsilon + k) + (\varepsilon + 1) - 1 \Longrightarrow \varepsilon \leq \dfrac{l(n-k)}{l+1} = \tau_{IRS}$ then the problem admits ≥ 1 nontrivial solution

not necessarily unique

Interleaved Reed-Solomon codes

Theorem:

If $\varepsilon \leq \tau_{IRS}$, let $R \in \mathbb{F}_q^{l \times n}$ such that,

- If $j \in E$, then R_j is a uniformly distributed element of $\mathbb{F}_q^{l \times 1}$
- otherwise $R_j = \boldsymbol{f}(\alpha_j)$

Then, the key equation admits a **unique solution** with probability $\geq 1 - \tau_{IRS}/q$

$$\big\downarrow$$

$$(\Lambda \boldsymbol{f}, \Lambda)$$

IRS Decoding Algorithm

Given R a received matrix,

1. Compute the Lagrange interpolators $Y_i(x)$ of R^i
2. Compute the **solution space of the simultaneous rational reconstruction*** problem
3. If it is one-dimensional
    - perform Euclidean division
        - if the remainder is 0 returns f
        - Otherwise ?
4. Otherwise return ?

*J. Rosenkilde and A. Storjohann. *Algorithms for Simultaneous Padé Approximations*. In Proceedings of ISSAC'16

IRS Decoding Algorithm

Bounded Distance Decoder

Given R a received matrix,

1. Compute the Lagrange interpolators $Y_i(x)$ of R^i

2. Compute the **solution space of the simultaneous rational reconstruction*** problem

3. If it is one-dimensional

    - perform Euclidean division

        - if the remainder is 0 returns f

        - Otherwise ?

4. Otherwise return ?

*J. Rosenkilde and A. Storjohann. *Algorithms for Simultaneous Padé Approximations*. In Proceedings of ISSAC'16

Power Decoding

Let $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ be a **received word**, where $\boldsymbol{c} \in C_{RS}(n, k)$

Theorem:

For any $i \geq 0$, $C^i_{RS}(n, k) = C_{RS}(n, i(k-1)+1)$

Idea : consider $\boldsymbol{y}, \boldsymbol{y}^2, \ldots, \boldsymbol{y}^l$

Define $\forall i \in [l]$. $\boldsymbol{e}^{(i)} := \boldsymbol{y}^i - \boldsymbol{c}^i$

G. Schmidt, V. Sidorenko, M. Bossert. *Collaborative decoding of Interleaved Reed-Solomon codes and concatenated code designs*. IEEE Trans. Inform. Theory, 55(7): 2991-3012, 2009

J. Rosenkilde. *Power decoding of Reed-Solomon codes revisited.* In Coding Theory and Applications, 297-305, 2015, Springer

Power Decoding

Let $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ be a **received word**, where $\boldsymbol{c} \in C_{RS}(n, k)$

Theorem:

For any $i \geq 0$, $C^i_{RS}(n, k) = C_{RS}(n, i(k-1)+1)$

Idea : consider $\boldsymbol{y}, \boldsymbol{y}^2, \ldots, \boldsymbol{y}^l$

Define $\forall i \in [l].\quad \boldsymbol{e}^{(i)} := \boldsymbol{y}^i - \boldsymbol{c}^i$

Proposition: $E_{e^{(i)}} = \{j \mid e^{(i)}_j \neq 0\} \subseteq E = \{j \mid e_j \neq 0\}$

G. Schmidt, V. Sidorenko, M. Bossert. *Collaborative decoding of Interleaved Reed-Solomon codes and concatenated code designs*. IEEE Trans. Inform. Theory, 55(7): 2991-3012, 2009

J. Rosenkilde. *Power decoding of Reed-Solomon codes revisited.* In Coding Theory and Applications, 297-305, 2015, Springer

Power Decoding

Let $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ be a **received word**, where $\boldsymbol{c} \in C_{RS}(n, k)$

Theorem:

For any $i \geq 0$, $C_{RS}^{i}(n, k) = C_{RS}(n, i(k-1)+1)$

$$\begin{pmatrix} f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n) \\ f^2(\alpha_1), f^2(\alpha_2), \ldots, f^2(\alpha_n) \\ \vdots \\ f^l(\alpha_1), f^l(\alpha_2), \ldots, f^l(\alpha_n) \end{pmatrix}$$

Idea : consider $\boldsymbol{y}, \boldsymbol{y}^2, \ldots, \boldsymbol{y}^l$

Define $\forall i \in [l]$. $\boldsymbol{e}^{(i)} := \boldsymbol{y}^i - \boldsymbol{c}^i$

Proposition: $E_{e^{(i)}} = \{j \mid e_j^{(i)} \neq 0\} \subseteq E = \{j \mid e_j \neq 0\}$

G. Schmidt, V. Sidorenko, M. Bossert. *Collaborative decoding of Interleaved Reed-Solomon codes and concatenated code designs*. IEEE Trans. Inform. Theory, 55(7): 2991-3012, 2009

J. Rosenkilde. *Power decoding of Reed-Solomon codes revisited*. In Coding Theory and Applications, 297-305, 2015, Springer

Power Decoding

Let $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ be a **received word**, where $\boldsymbol{c} \in C_{RS}(n, k)$

Idea : consider $\boldsymbol{y}, \boldsymbol{y}^2, \ldots, \boldsymbol{y}^l$

Lagrange interpolator polynomial of $\boldsymbol{y}^i$

$$\boxed{V_i(x) = D(x)Y^i(x) \bmod G(x)}$$

Bounded Distance Decoder

$$\deg(V_i) \leq \varepsilon + i(k-1) \qquad \deg(D) \leq \varepsilon$$

If $nl \geq \sum_{i=1}^{n} (\varepsilon + i(k-1) + 1) + (\varepsilon + 1) - 1 \Longrightarrow \varepsilon \leq \dfrac{ln}{l+1} - \dfrac{lk}{2} + \dfrac{l(l-1)}{2(l+1)} = \tau_{PD}$

then the problem admits ≥ 1 nontrivial solution

List Decoding

Let $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ be a **received word**, where $\boldsymbol{c} \in C_{RS}(n, k)$

$\varepsilon \leq \tau_0$

$$V(\alpha_i) = y_i D(\alpha_i)$$

$\deg(V) \leq \varepsilon + k - 1$

$\deg(D) \leq \varepsilon$

Interpolation

$$Q(x, y) = yD(x) - V(x)$$

$$Q(\alpha_i, y_i) = 0$$

Root Finding

If $Y - F(x) \mid Q(x, y) \implies F$

M. Sudan. *Decoding of Reed Solomon Codes beyond the Error-Correction Bound.* J. Complexity, 13(1):180-193, 1997

List Decoding

Find $Q(x, y)$ s.t. $\deg_x Q \leq l$ and $\deg_y Q \leq n/l$

$Q(\alpha_i, y_i) = 0$

Lemma:

If $B^{\varepsilon}(\mathbf{y}) \cap C \neq \varnothing$ then $Y - f(x)$ divides $Q(x, y)$

1. Interpolation step
2. Root finding

$$\varepsilon \leq \frac{2nl - kl(l+1) + l(l+1) - 2}{2(l+1)} = \tau_S$$ at least one nontrivial solution

M. Sudan. *Decoding of Reed Solomon Codes beyond the Error-Correction Bound.* J. Complexity, 13(1):180-193, 1997

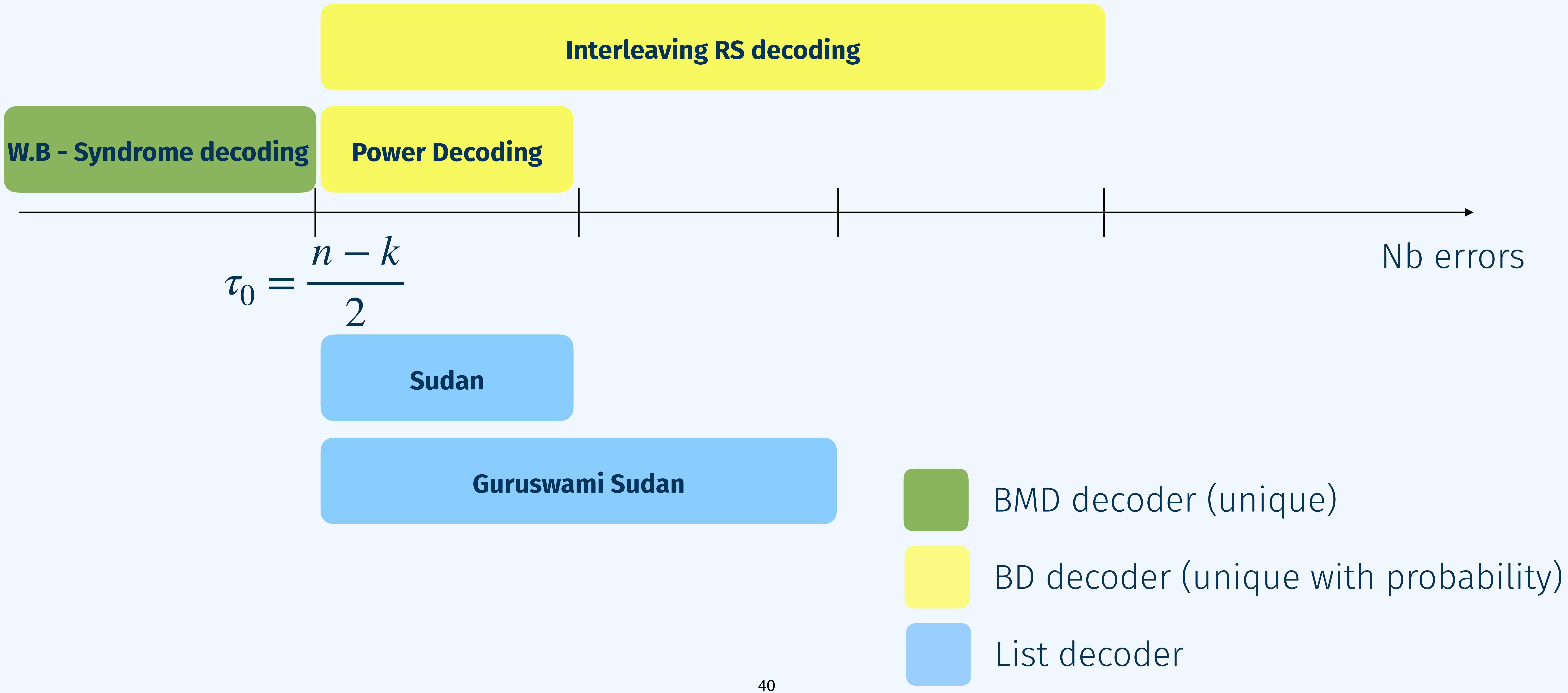
List Decoding

1. Interpolation step → Add **multiplicities** to increase the decoding radius
2. Root finding

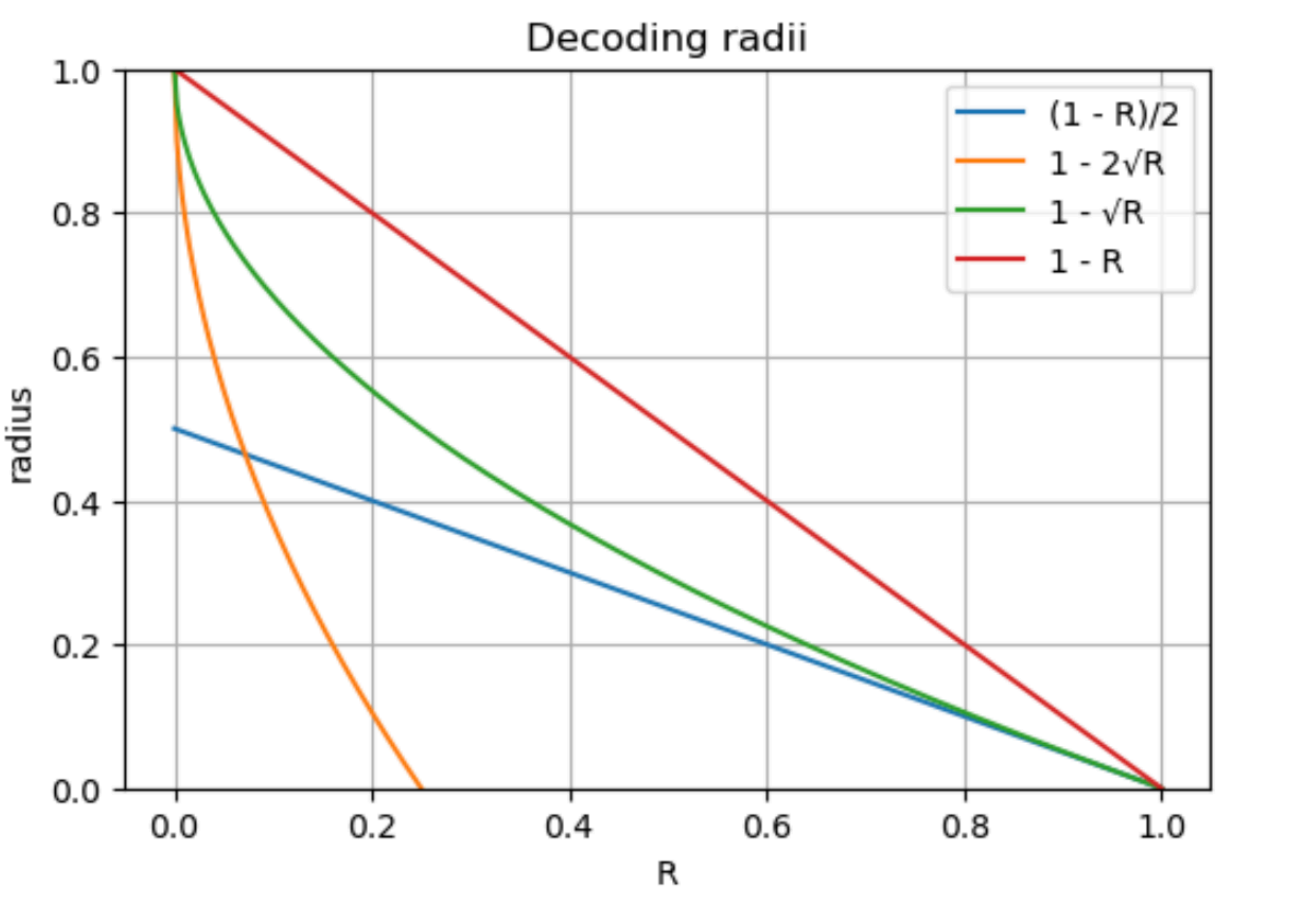
V. Guruswami, M. Sudan. *Improved decoding of Reed-Solomon codes and Algebraic-Geometry codes*. IEEE Trans. Inform. Theory, 45(6):1757-1767, 1999

S. Chatterjee, P. ,Harsha, M. Kumar. Deterministic list decoding of Reed-Solomon codes. *https://arxiv.org/abs/2511.05176*

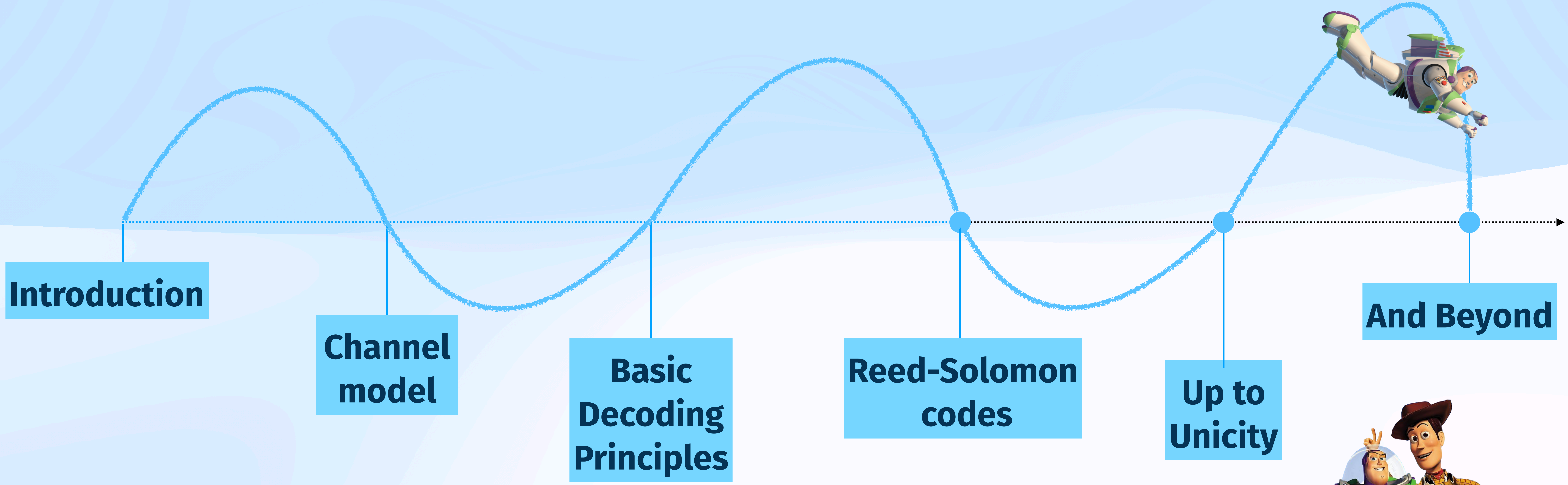
Decoding Reed Solomon codes

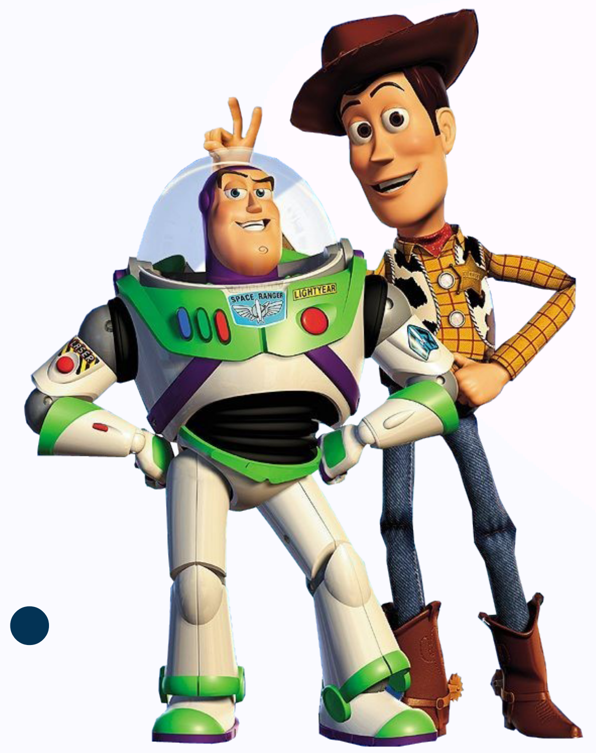


Decoding Reed Solomon codes



Part 1 : Hamming metric





Thank you.