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 2 : Rank metric

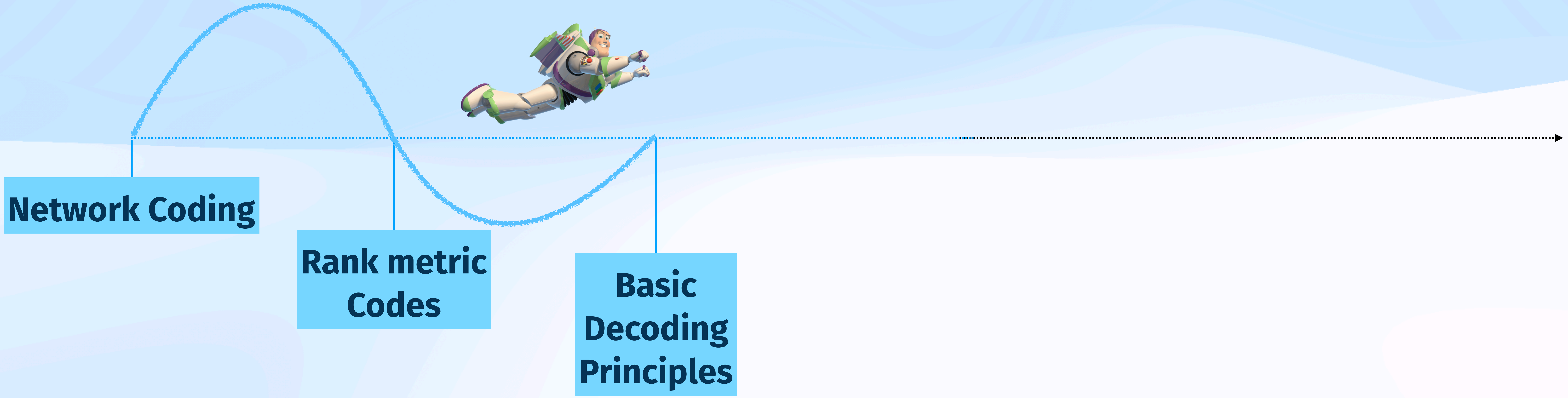
Network Coding

Part 2 : Rank metric

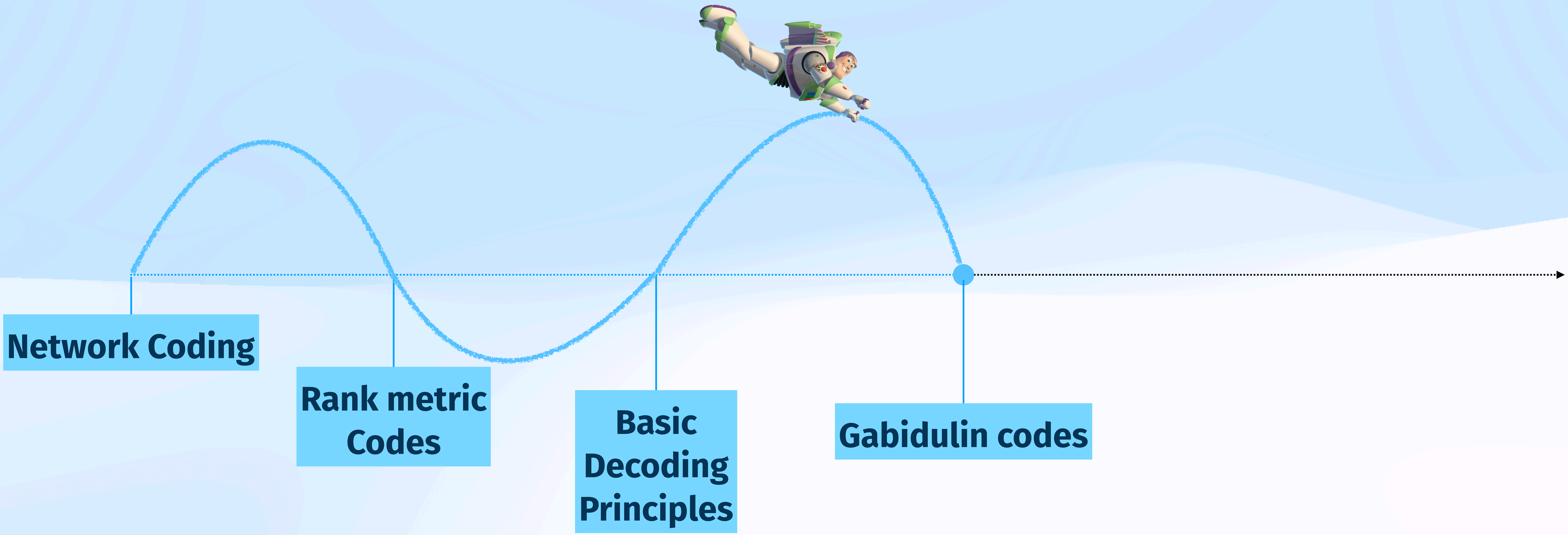
Network Coding

Rank metric Codes

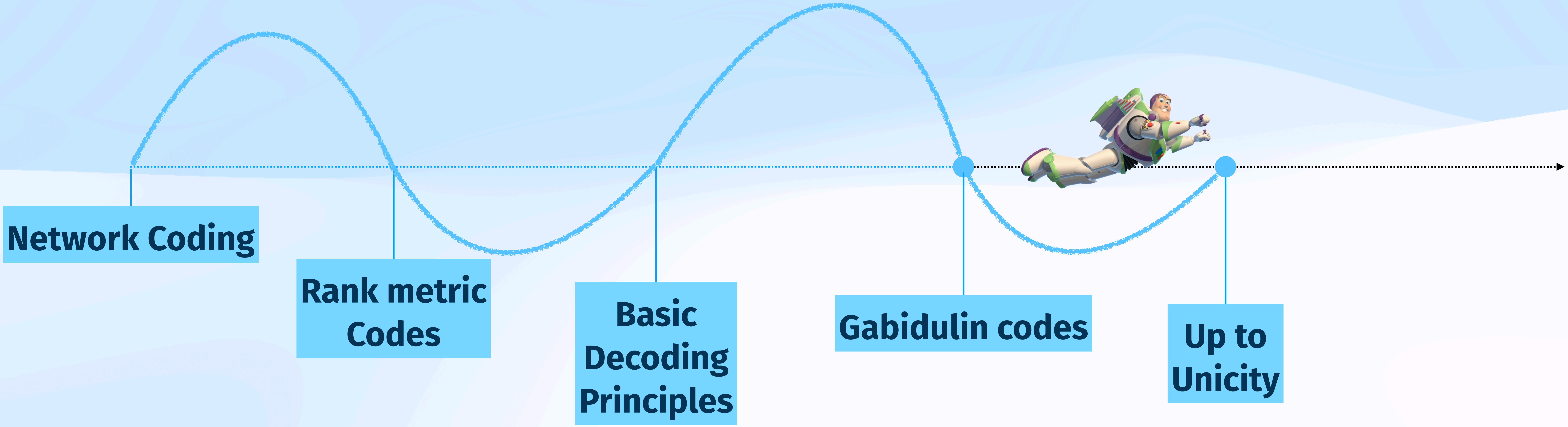
Part 2 : Rank metric



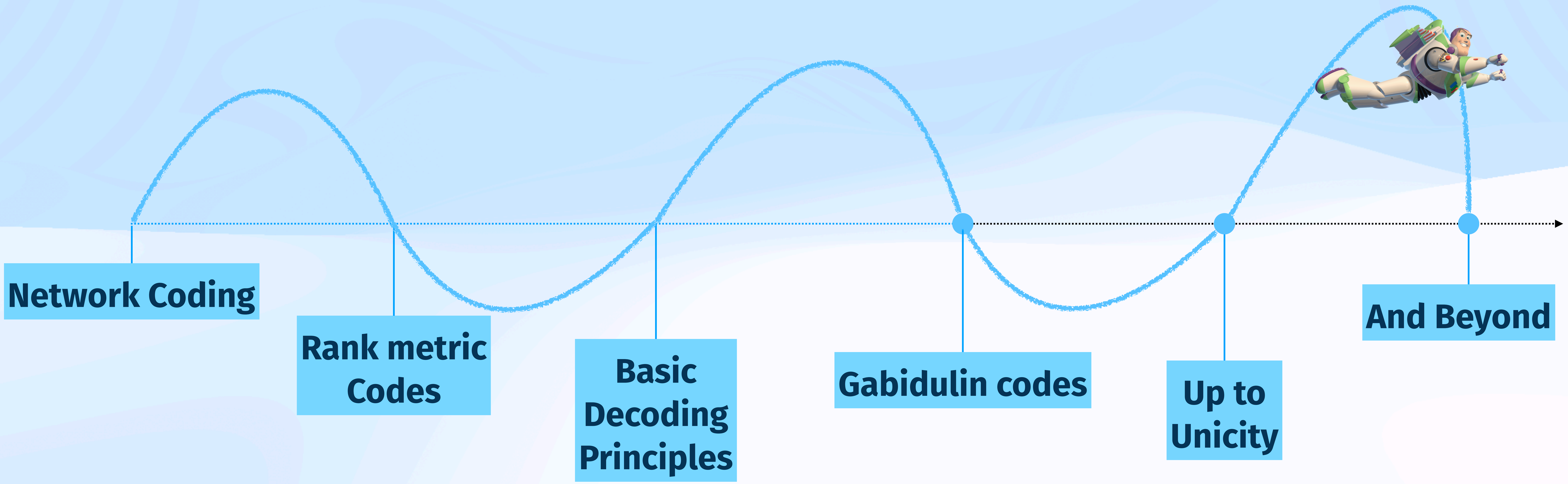
Part 2 : Rank metric



Part 2 : Rank metric



Part 2 : Rank metric



Part 2 : Rank metric

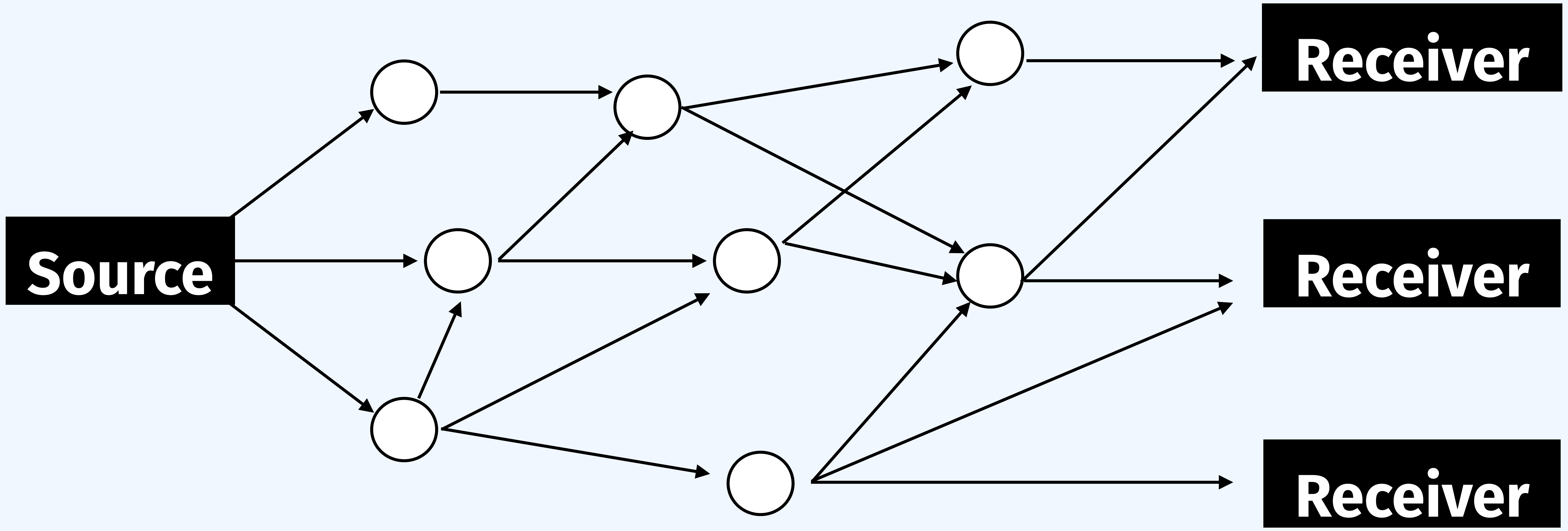
Network Coding

Network coding

Linear network communication channel model

A (single-source) multicast channel has one source or sender, several inner nodes and several receivers who want to receive the same information.

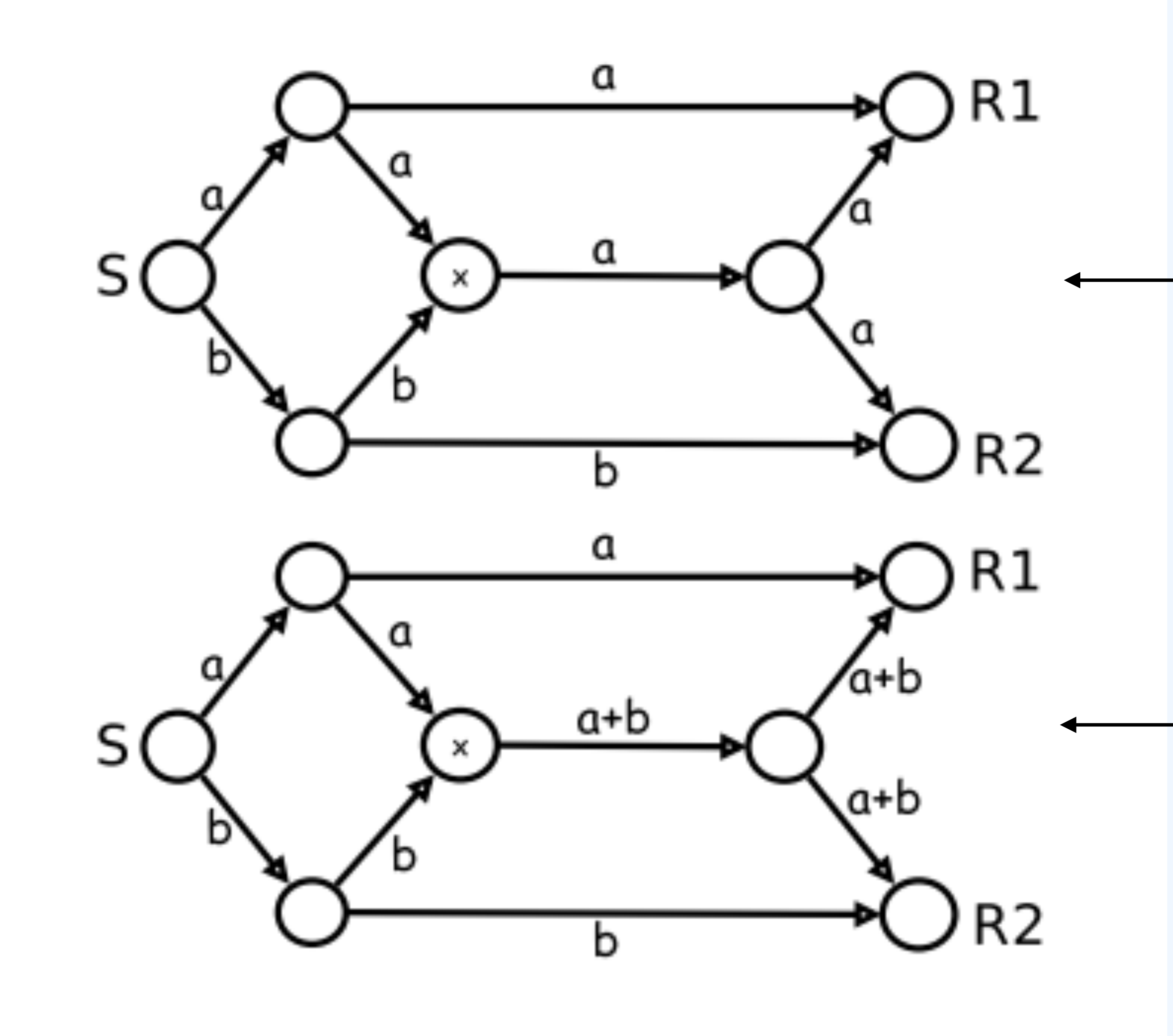
Linear network coding: the inner nodes are allowed to forward linear combinations of the information vectors.



Goal: maximize the **transmission rate**

R. Ahlswede, N. Cai, S-Y.R. Li and R..W. Yeung, *Network Information Flow*. IEEE Trans. on Inform. Theory, 46, 1204-1216, 2000.

A classical example: the butterfly network

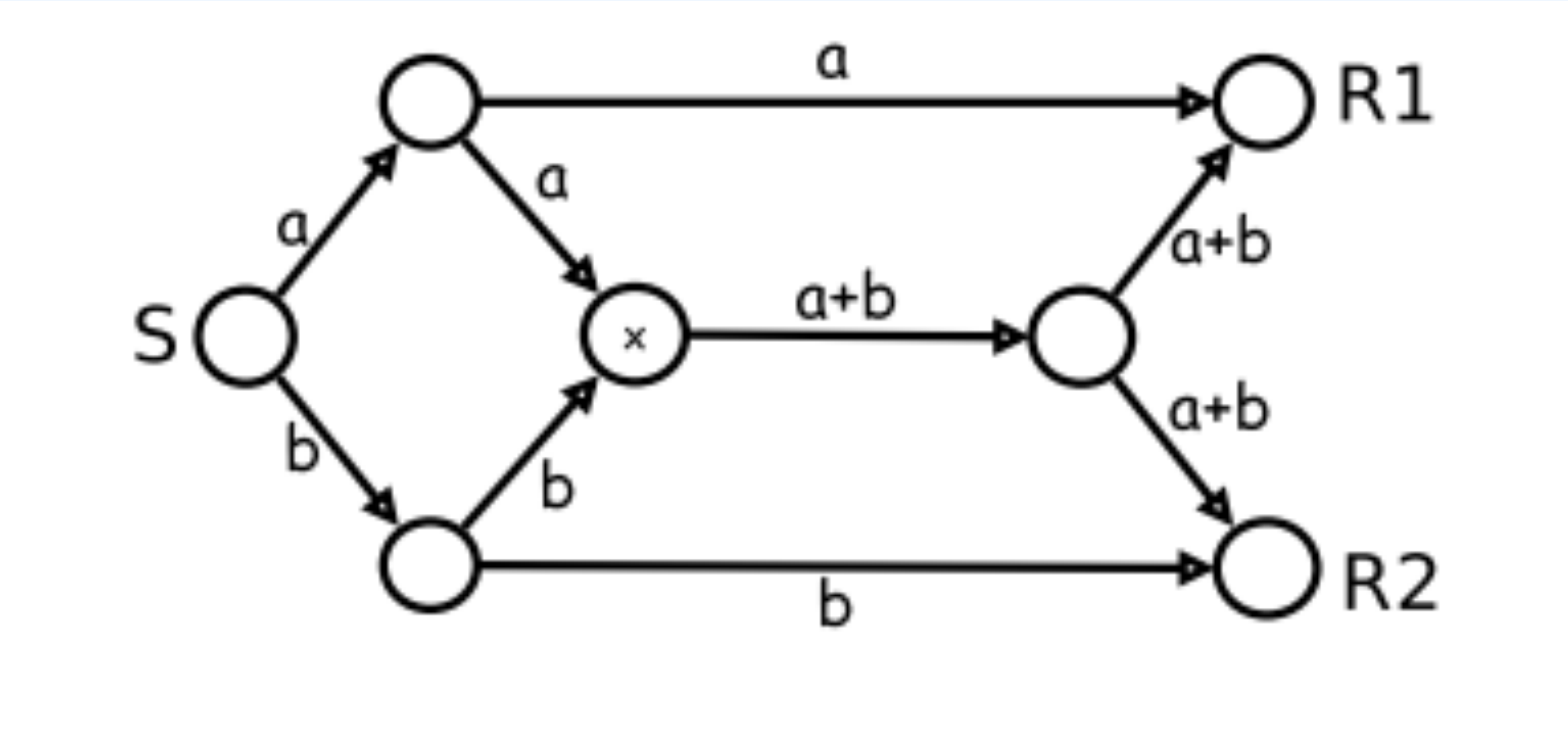


Forwarding model

Network coding model

Figure from *Lecture notes A-L. Horlemann*

The butterfly network



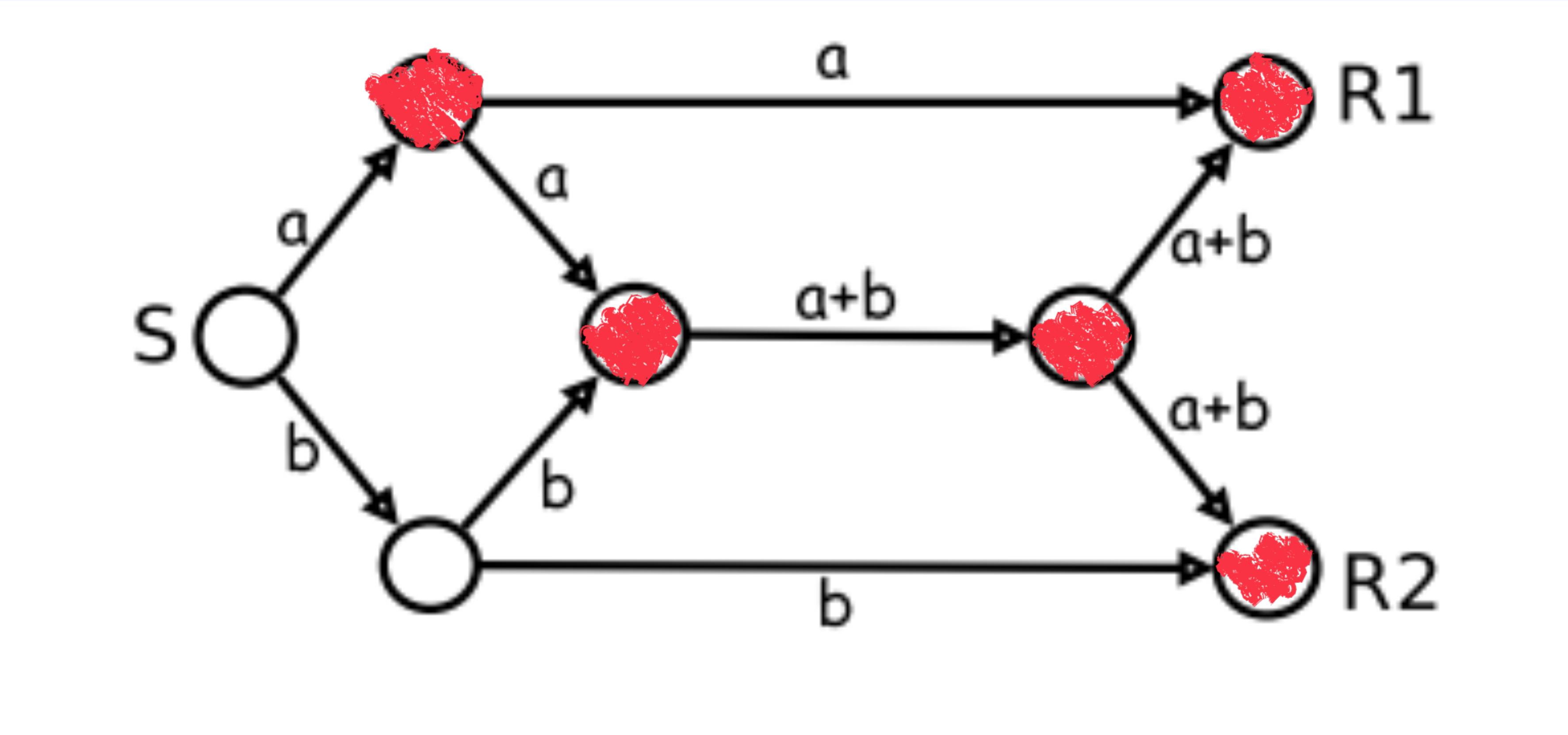
$$C = \begin{pmatrix} a \\ b \end{pmatrix} \longrightarrow Y_1 = \begin{pmatrix} a \\ a+b \end{pmatrix}, Y_2 = \begin{pmatrix} a+b \\ b \end{pmatrix}$$

Sent message

Received messages

The error propagation

Error



Error propagation

$$Y = AC + E$$

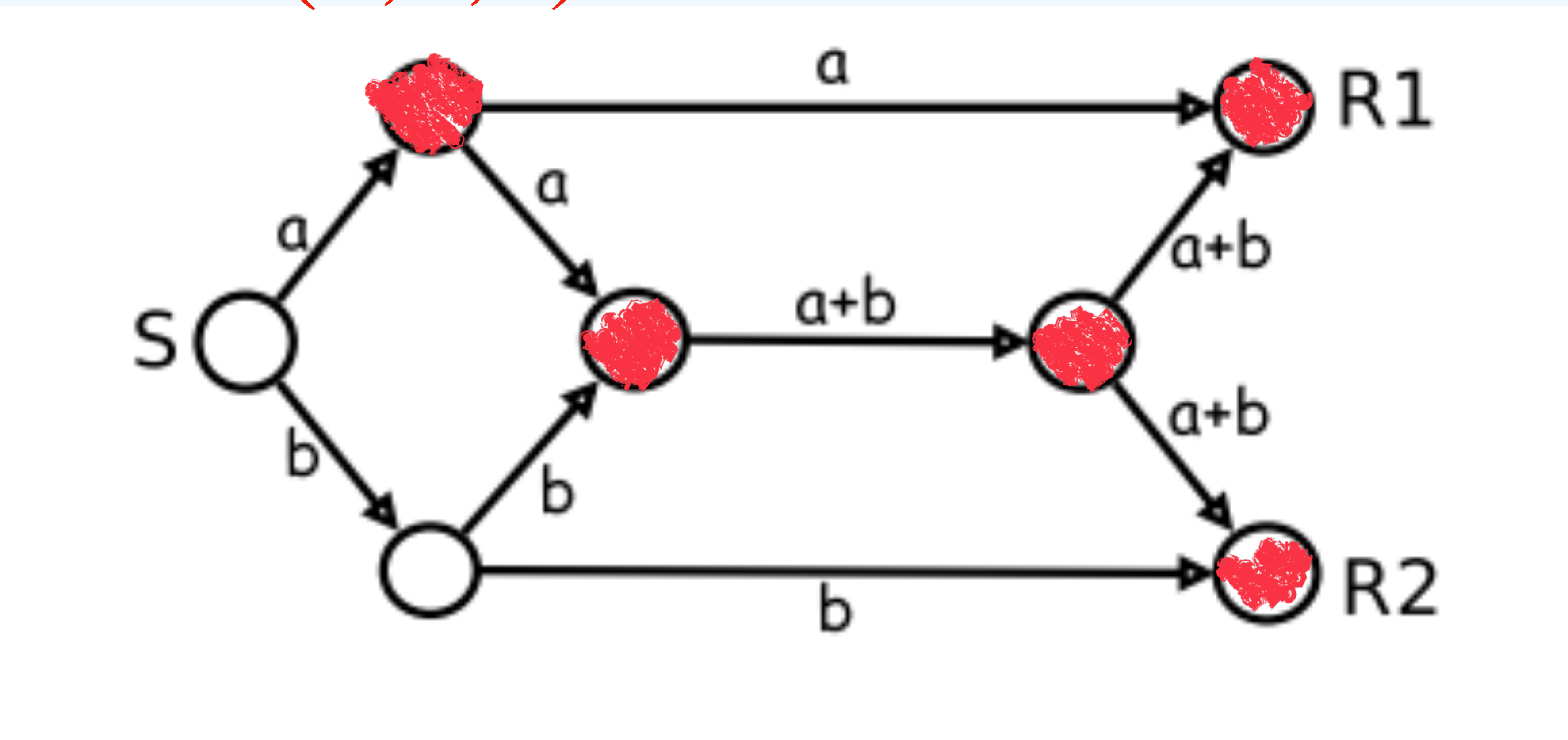
Linear channel operation matrix

Square and nonsingular

Error matrix

The error propagation : an example

(1,0,0)



$$A_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \qquad \boldsymbol{a} = (1,1,0), \boldsymbol{b} = (0,1,1) \qquad E = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$Y_1 = A_1 C + E = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$$A_1^{-1} Y_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Example from *Lecture notes A-L. Horlemann*

Part 2 : Rank metric

Rank metric

Rank support and weight

Let $A \in \mathbb{F}_q^{m\times n}$,

$$Supp_R(A) := RowSpace_{\mathbb{F}_q}(A),$$
$$w_R(A) := rk(A)$$

Rank support and weight

Let $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$,

$$Supp_R(\boldsymbol{v}) := < v_1, \dots, v_n >_{\mathbb{F}_q}$$
$$w_R(\boldsymbol{v}) = dim_{\mathbb{F}_q}(Supp_R(\boldsymbol{v}))$$

$$\mathbb{F}_q^{m\times n} \cong \mathbb{F}_{q^m}^n$$

Rank metric

Let $A, B \in \mathbb{F}_q^{m\times n}$,

$$\delta_R(A, B) = rk(A - B)$$

Rank metric

Let $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{F}_{q^m}^n$,

$$\delta_R(\boldsymbol{v}, \boldsymbol{w}) = w_R(\boldsymbol{v} - \boldsymbol{w})$$

P. Delsarte. *Bilinear forms over a finite field, with applications to coding theory.* J. Comb. Theory A, 25(3): 226-241, 1978

$\mathbb{F}_{q^m}$-linear code

$\mathbb{F}_{q^m}$- linear code $[n, k, d]_{\mathbb{F}_{q^m}}$:

An $\mathbb{F}_{q^m}$-linear code C is an $\mathbb{F}_{q^m}$-vector subspace of $\mathbb{F}_{q^m}^n$.

- $k = dim_{\mathbb{F}_{q^m}}(C)$ is the **dimension**
- n is the **length**
- $d_R = \min_{\boldsymbol{c} \in C \setminus \{\boldsymbol{0}\}} \{w_R(\boldsymbol{c})\}$ is the **minimum distance**

$\mathbb{F}_{q^m}$-linear code

$\mathbb{F}_{q^m}$- linear code $[n, k, d]_{\mathbb{F}_{q^m}}$:

An $\mathbb{F}_{q^m}$-linear code C is an $\mathbb{F}_{q^m}$-vector subspace of $\mathbb{F}_{q^m}^n$.

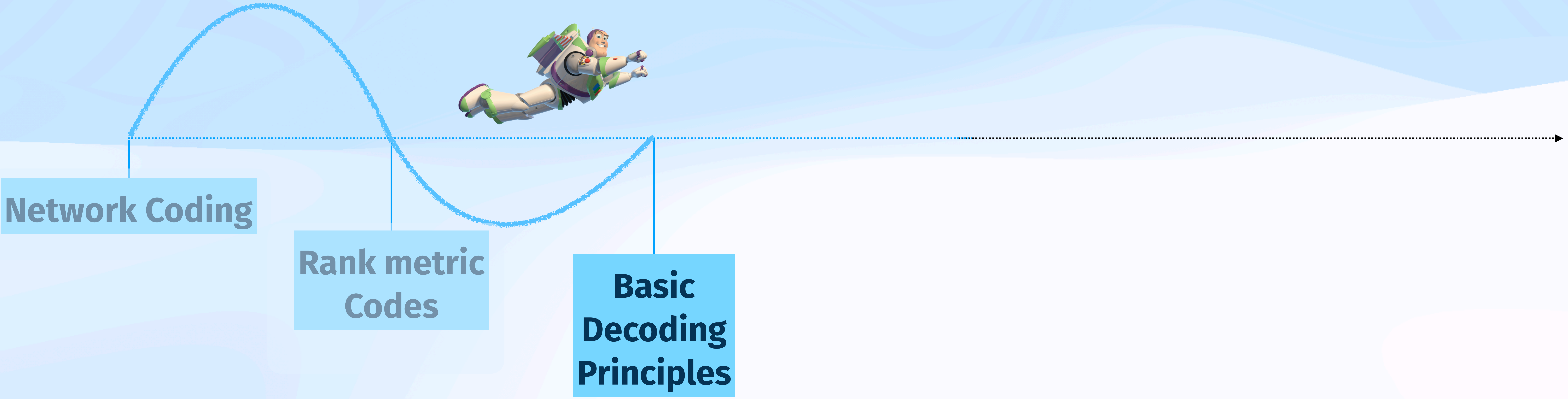
- $k = dim_{\mathbb{F}_{q^m}}(C)$ is the **dimension**
- n is the **length**
- $d_R = \min\limits_{\boldsymbol{c} \in C \setminus \{\boldsymbol{0}\}} \{w_R(\boldsymbol{c})\}$ is the **minimum distance**

- $G \in \mathbb{F}_{q^m}^{k \times n}$ the matrix whose rows are a basis of C, is a **generator matrix**
- Let $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$, 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 $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$ of $C^\perp$ is called **parity check matrix**

Part 2 : Rank metric



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

The decoder

Let C be an $[n, k, d]_{\mathbb{F}_{q^m}}$ code, a **decoder** for C is a map

$$D : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n \cup \{ ? \}$$

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

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

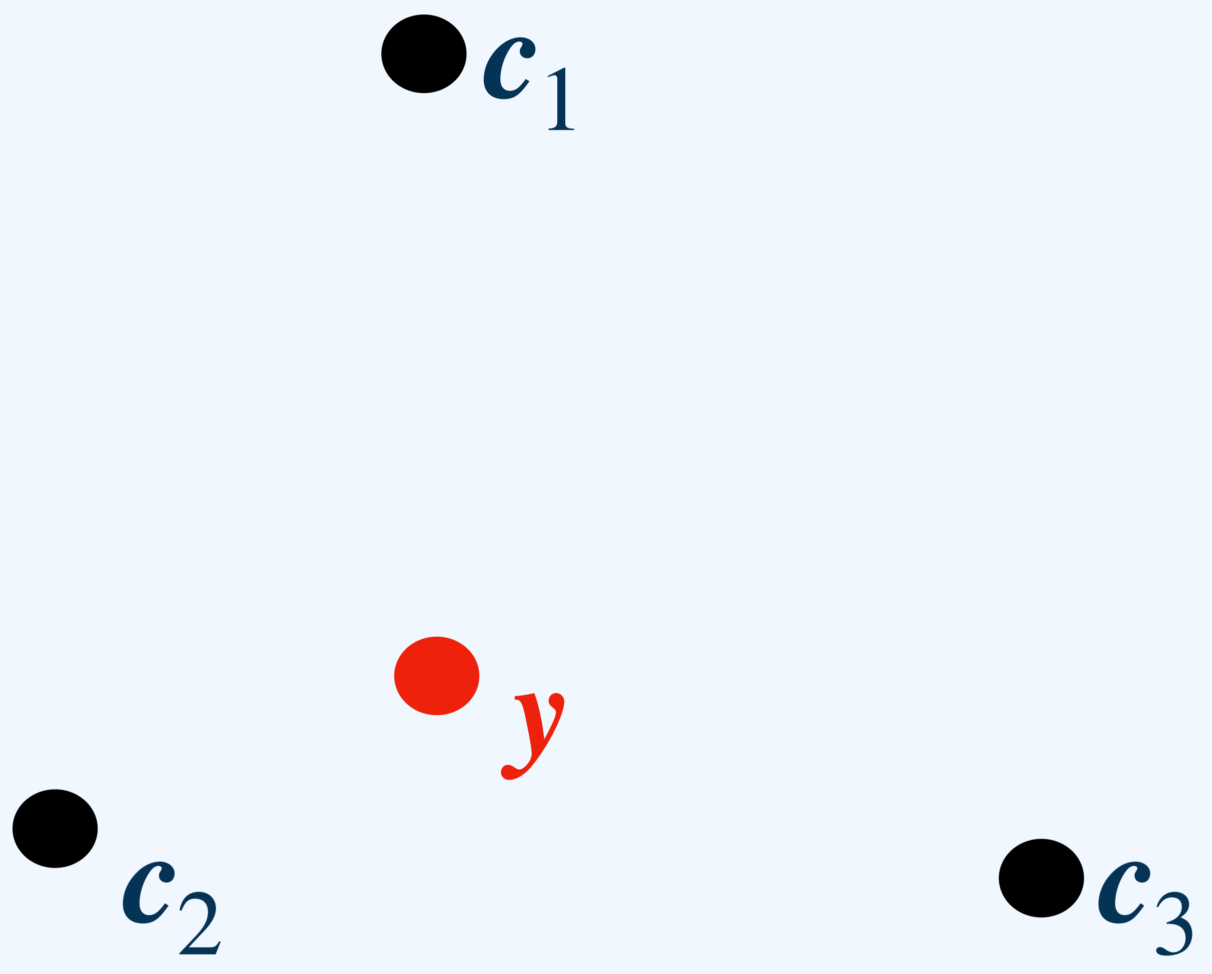
Nearest-codeword decoding

Nearest-codeword decoder

$$D_{Nc} : \mathbb{F}_{q^m}^n \to C$$

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

$$\boldsymbol{c} \in argmin_{\boldsymbol{c} \in C}\{d_R(\boldsymbol{y}, \boldsymbol{c})\}$$



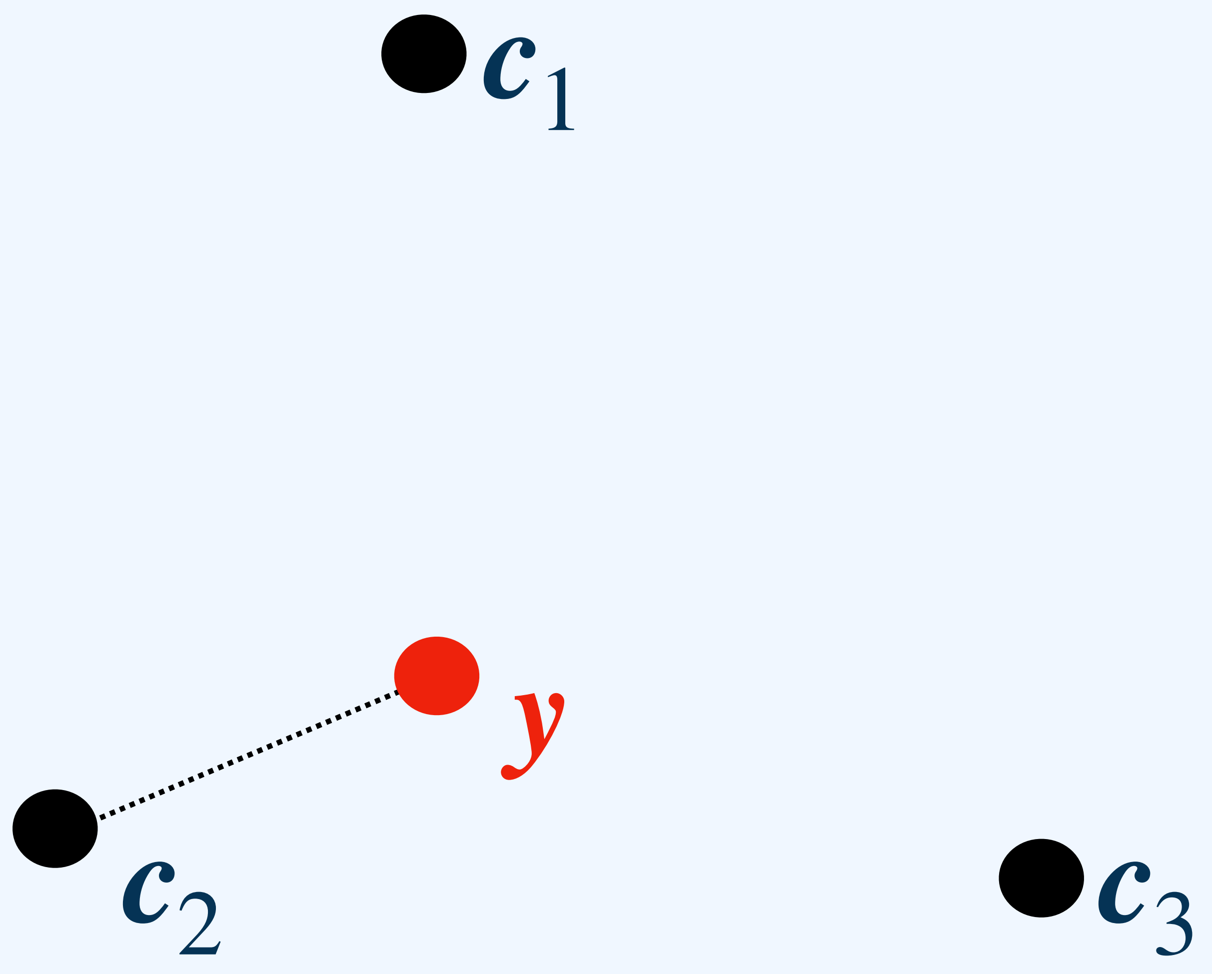
Nearest-codeword decoding

Nearest-codeword decoder

$$D_{Nc} : \mathbb{F}_{q^m}^n \to C$$

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

$$\boldsymbol{c} \in argmin_{\boldsymbol{c} \in C}\{d_R(\boldsymbol{y}, \boldsymbol{c})\}$$



Nearest-codeword decoder, the linear case

Nearest-codeword decoding problem

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

Syndrome decoding problem

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

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

Nearest-codeword decoder, the linear case

Nearest-codeword decoding problem

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

NP-hard

under randomized reductions

Syndrome decoding problem

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

NP-hard

under randomized reductions

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

P. Gaborit, G. Zémor. *On the Hardness of the decoding and the minimum distance problems for rank codes.* IEEE Trans. Inf. Theory, 62(12):1006-1019, 2016

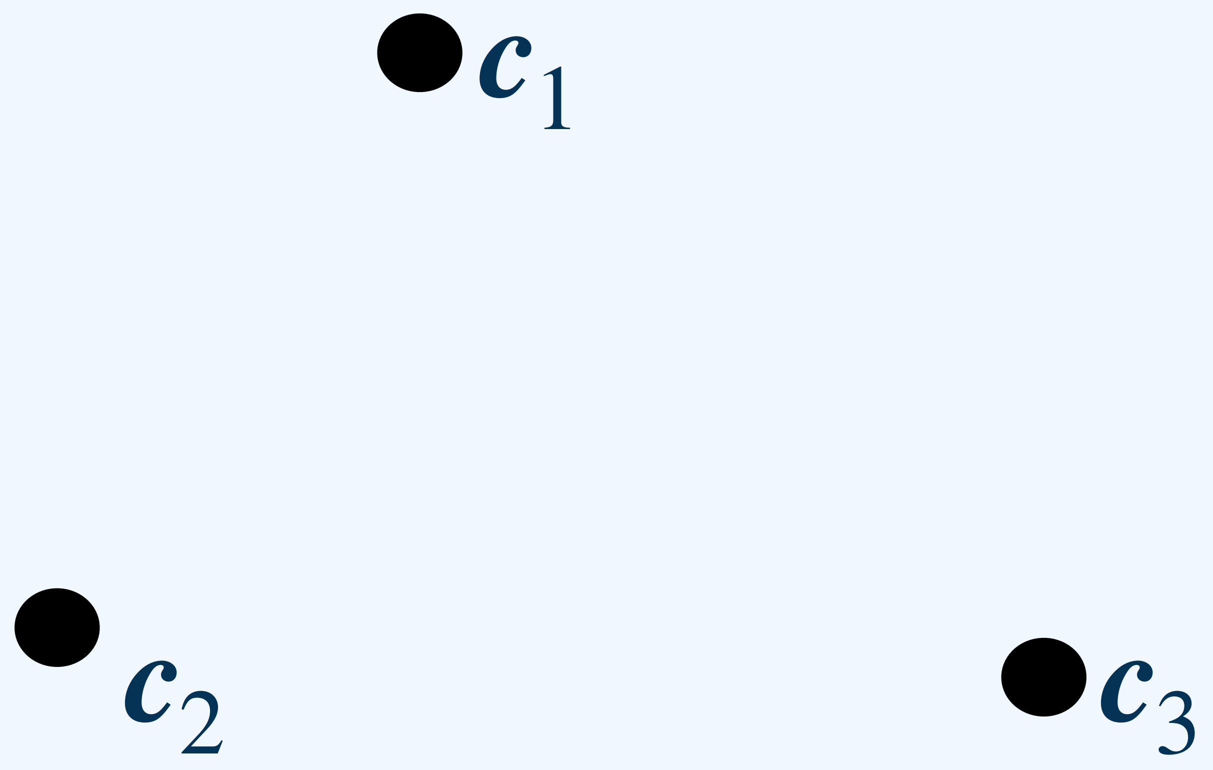
Unique Decoding Capability

Theorem (Unique Decoding Capability)

Let C be an $[n, k, d]_{\mathbb{F}_{q^m}}$ code and $\tau_0 = \lfloor (d-1)/2 \rfloor$.

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

$$B^{\tau_0}(\boldsymbol{c}_1) \cap B^{\tau_0}(\boldsymbol{c}_2) = \emptyset$$



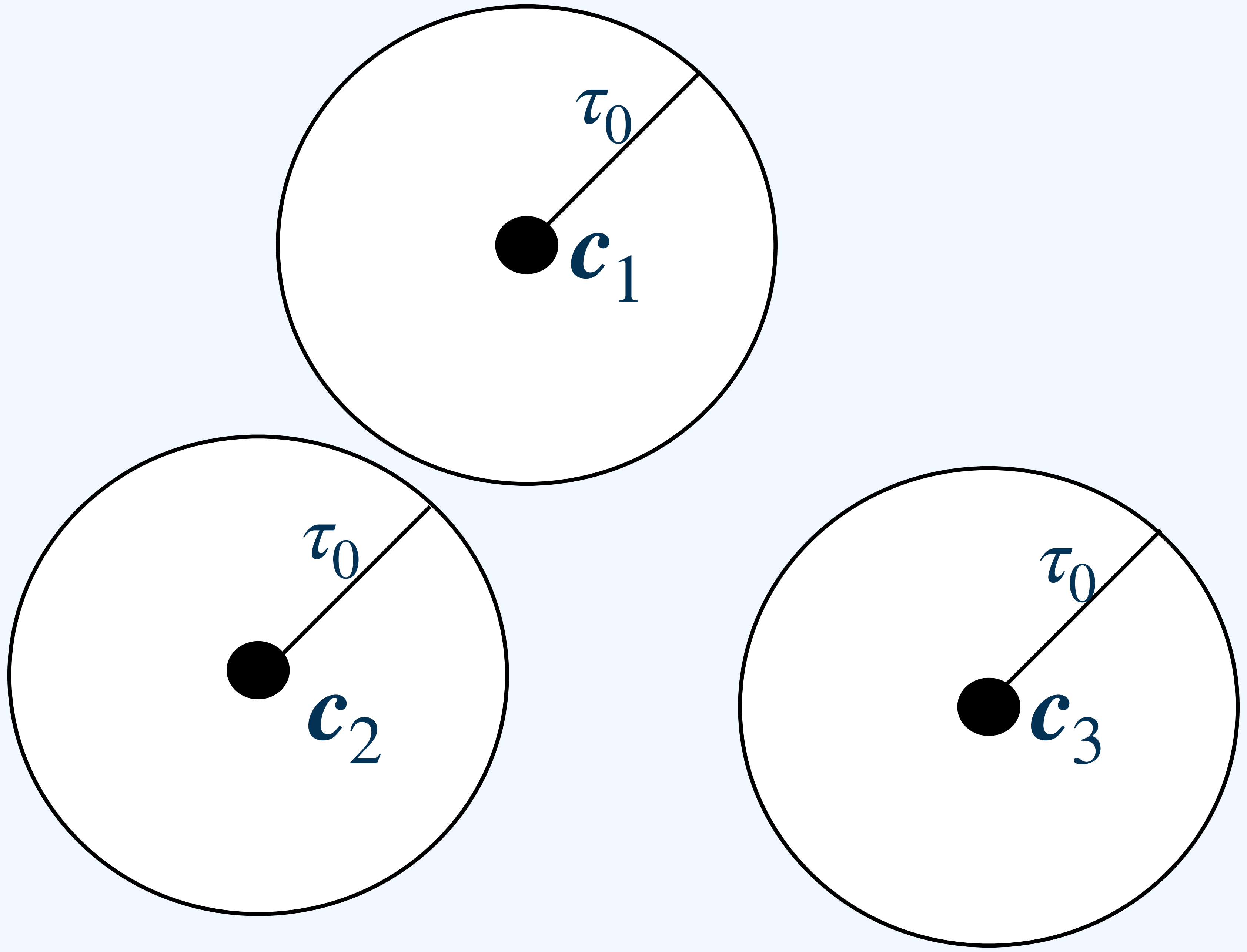
Unique Decoding Capability

Theorem (Unique Decoding Capability)

Let C be an $[n, k, d]_{\mathbb{F}_{q^m}}$ code and $\tau_0 = \lfloor (d-1)/2 \rfloor$.

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

$$B^{\tau_0}(\boldsymbol{c}_1) \cap B^{\tau_0}(\boldsymbol{c}_2) = \emptyset$$



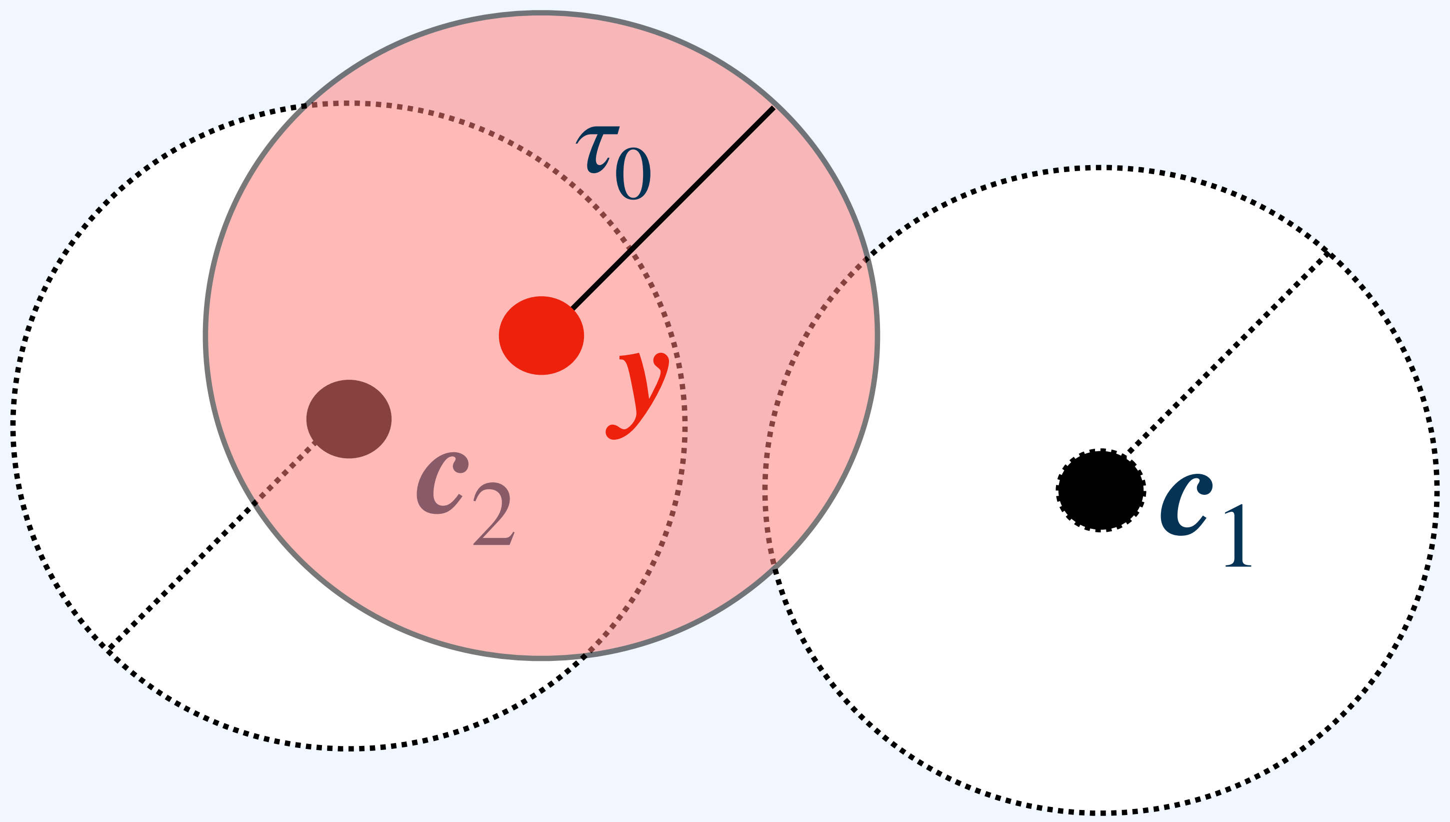
Bounded Minimum Distance decoder

Bounded Minimum Distance decoder

$$D_{BMD} : \mathbb{F}_{q^m}^n \to C \cup \{?\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_{q^m}^n$,

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



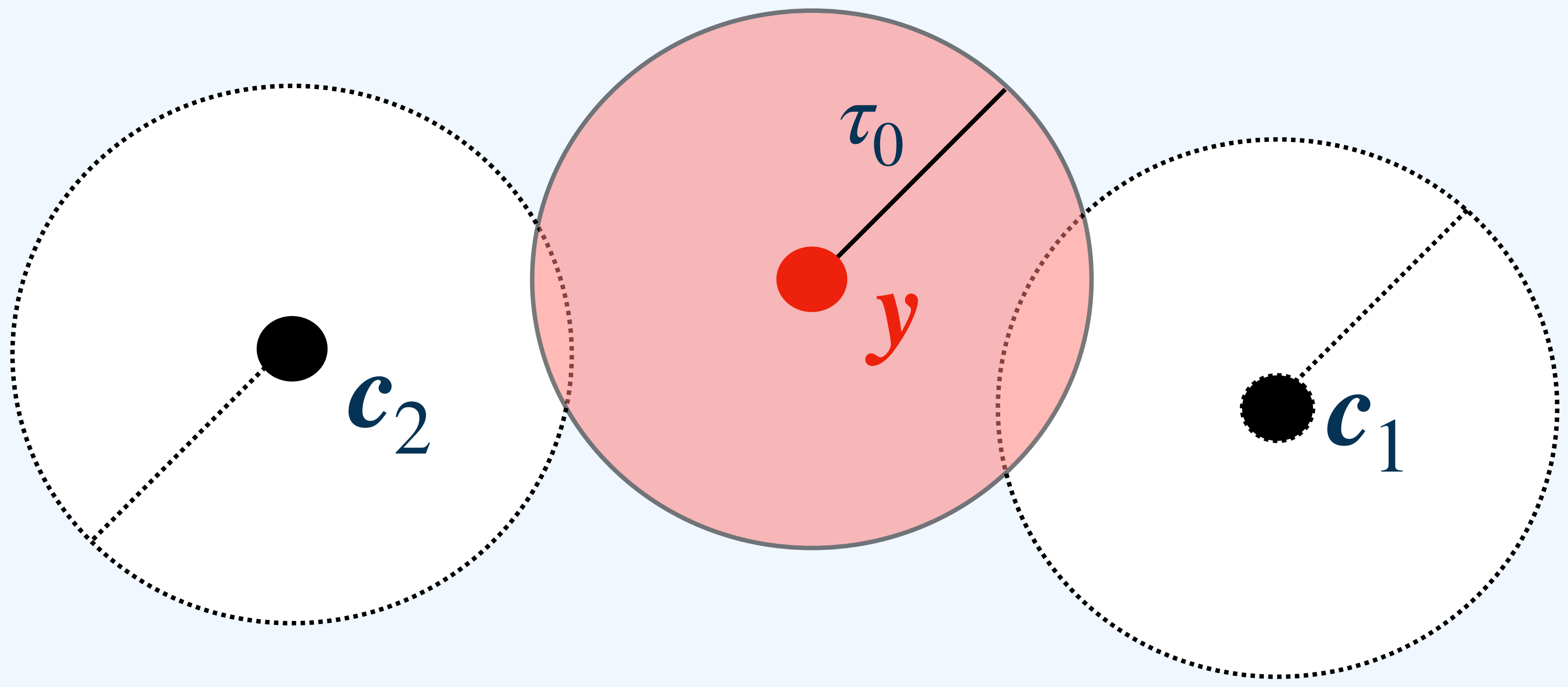
Bounded Minimum Distance decoder

Bounded Minimum Distance decoder

$$D_{BMD} : \mathbb{F}_{q^m}^n \to C \cup \{?\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_{q^m}^n$,

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



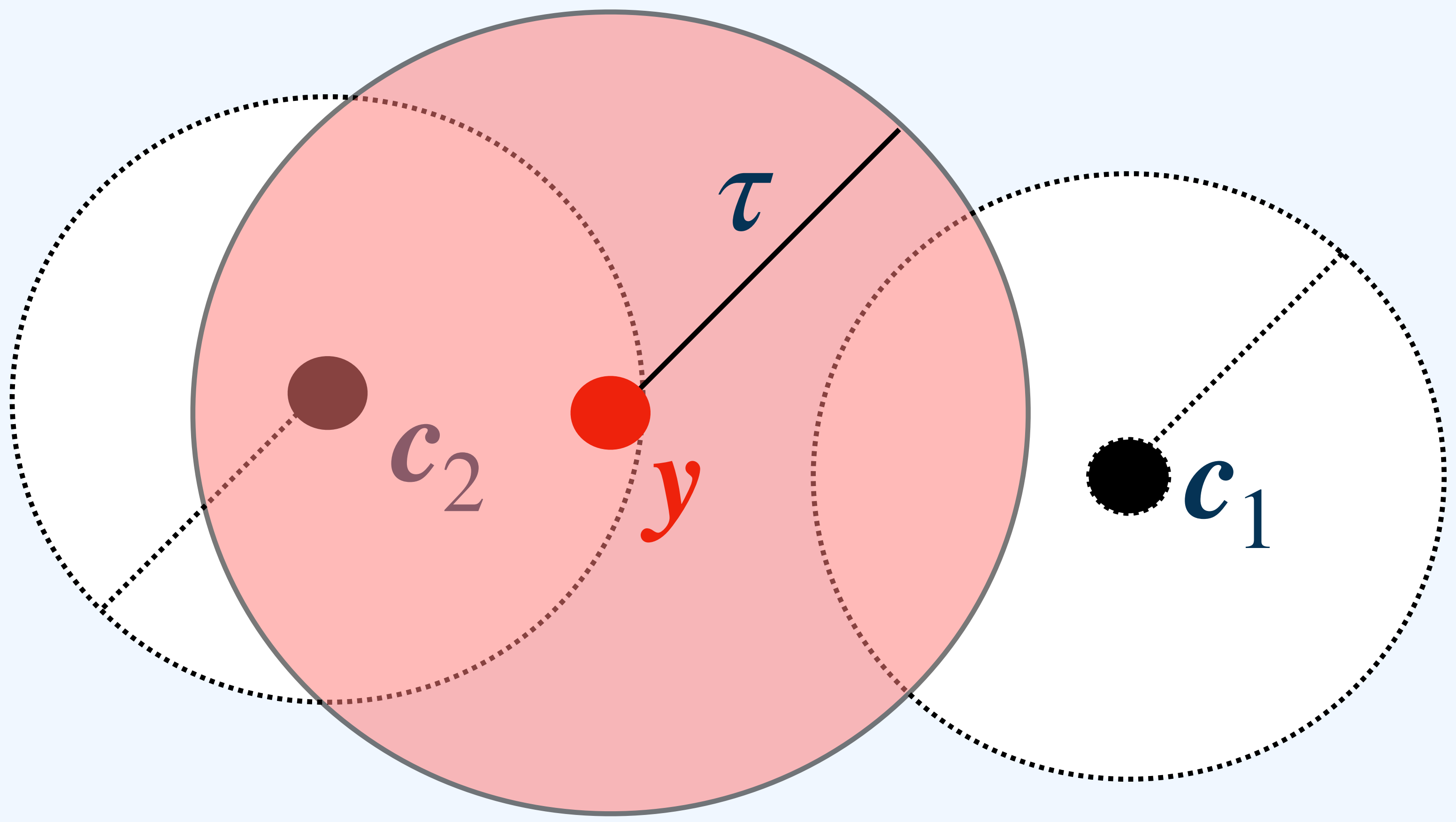
Bounded Distance decoder

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

$$D_{BD} : \mathbb{F}_{q^m}^n \to C \cup \{?\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_{q^m}^n$,

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



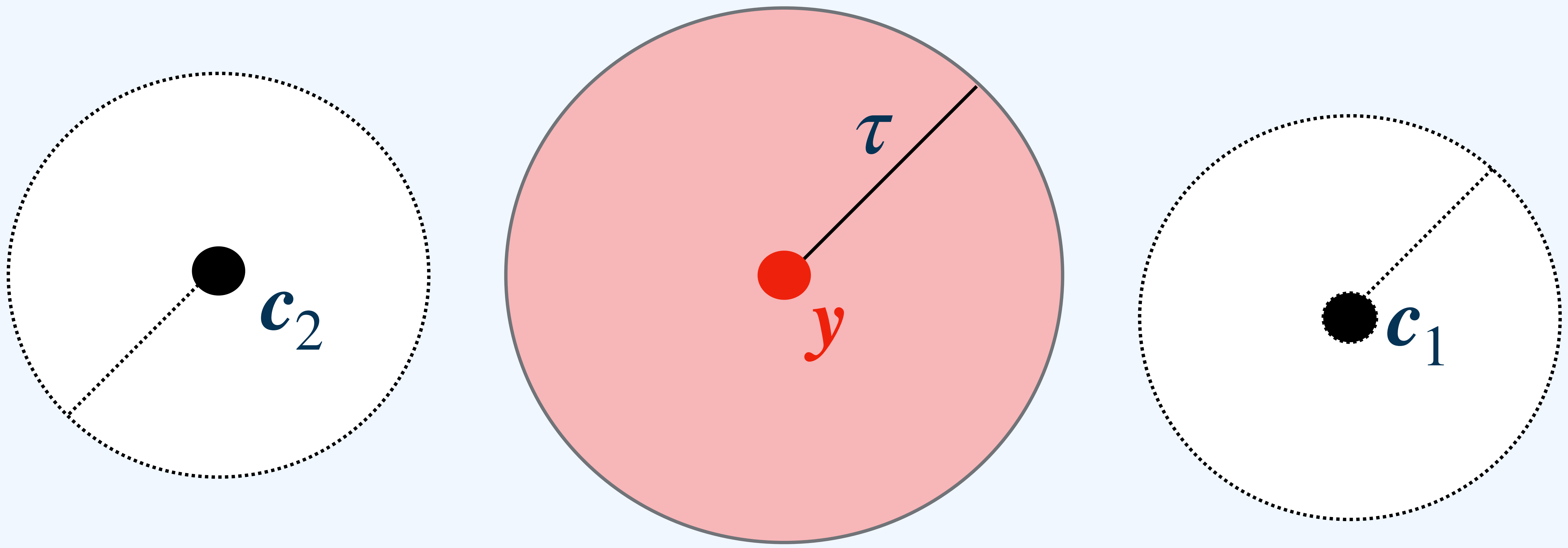
Bounded Distance decoder

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

$$D_{BD} : \mathbb{F}_{q^m}^n \rightarrow C \cup \{?\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_{q^m}^n$,

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



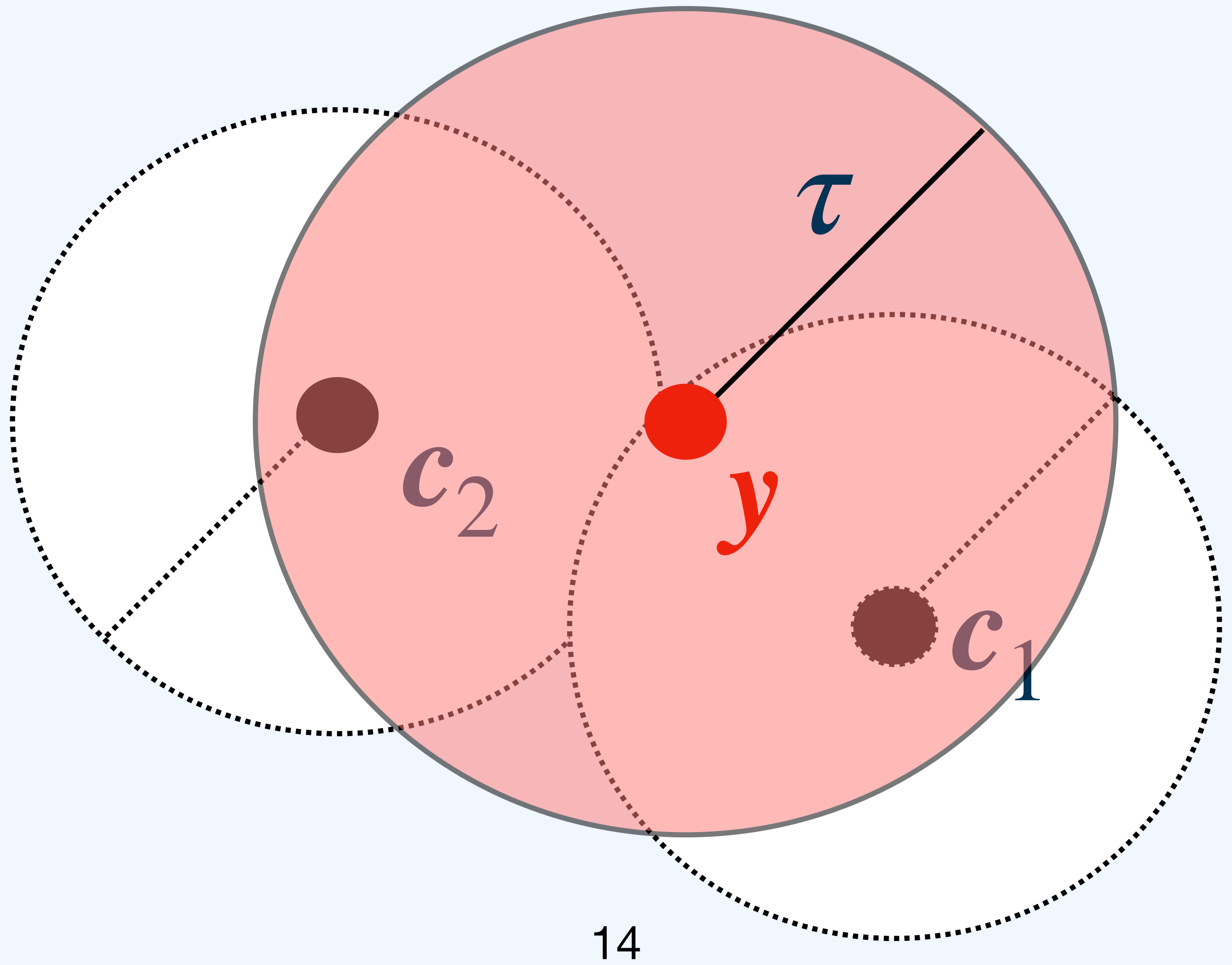
Bounded Distance decoder

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

$$D_{BD} : \mathbb{F}_{q^m}^n \to C \cup \{?\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_{q^m}^n$,

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



List decoder

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

$$D_L : \mathbb{F}_{q^m}^n \to \mathscr{P}(C) \cup \{\,?\,\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_{q^m}^n$,

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

A. Wachter-Zeh. *Bounds on list decoding of rank-metric codes*. IEEE Trans. Inform. Theory 59(11), 7628-7276, 2013

N. Raviv, A. Wachter-Zeh. *Some Gabidulin codes cannot be list decoded efficiently at any radius*. IEEE Trans. Inform. Theory 62(4), 1606-1615, 2016

List decoder

A. Wachter-Zeh. *Bounds on list decoding of rank-metric codes.* IEEE Trans. Inform. Theory 59(11), 7628-7276, 2013

Gabidulin codes cannot be decoded beyond the Johnson radius

Y. Ding. O*n list-decodability of random rank metric codes and subspace codes*. IEEE Transactions on Information Theory. 61(1): 51–59, 2015

Rank metric codes cannot be decoded beyond the Johnson radius

V. Guruswami, C. Wang, and C. Xing. *Explicit list-decodable rank-metric and subspace codes via subspace designs.* IEEE Transactions on Information Theory. 62(5): 2707–2718, 2016.

Explicit subcode of a Gabidulin code efficiently list decodable

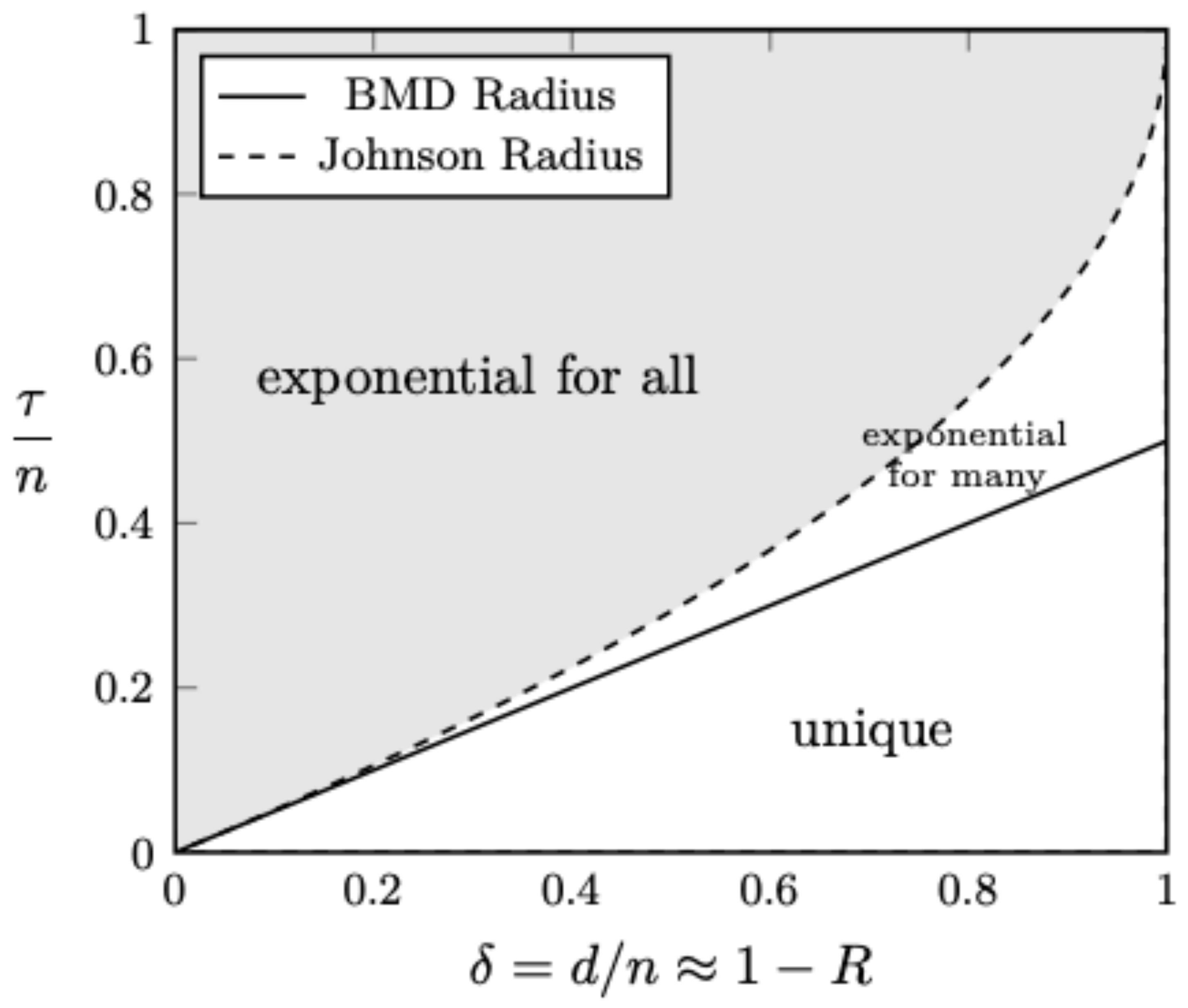
N. Raviv, A. Wachter-Zeh. *Some Gabidulin codes cannot be list decoded efficiently at any radius.* IEEE Trans. Inform. Theory 62(4), 1606-1615, 2016

Families of Gabidulin codes for which some received words have exponential list size for $\tau_0 + 1$

R. Trombetti, F. Zullo *On the list decodability of rank metric codes.* IEEE Transactions on Information Theory. 66(9): 5379–5386, 2020.

Generalization for some classes of MRD codes

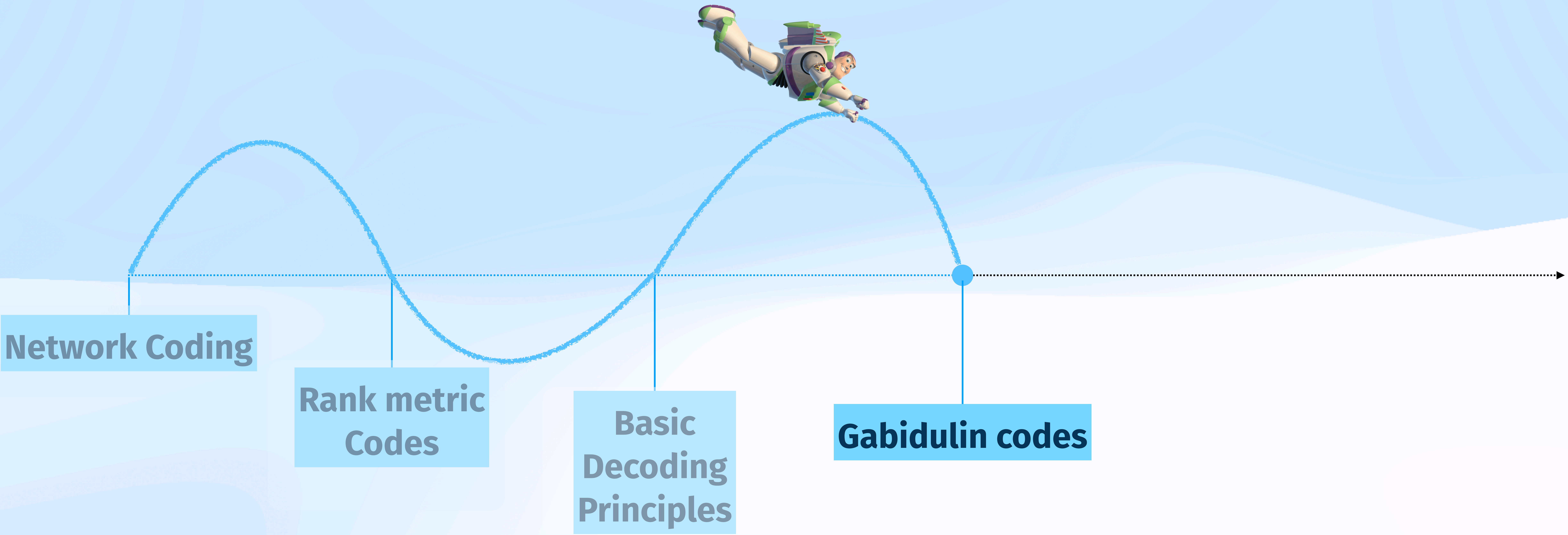
List decoder



(b) Gabidulin codes

Figure from Rank-Metric Codes and Their Applications

Part 2 : Rank metric



- The ring of linearized polynomials
- Gabidulin codes

The ring of Linearized Polynomials

Linearized Polynomials

$$F(x) = \sum_{i=0}^{d} f_i x^{q^i} = \sum_{i=0}^{d} f_i x^{[i]}, \text{ with } f_d \neq 0$$

The $q-$degree $\deg_q(F) = d$

$(\mathbb{F}_{q^m}\langle x^q \rangle, + , \circ)$ is a **non commutative ring**

- $+$ is the termwise addition of polynomials
- $\circ$ is the composition

O. Ore *On a special class of polynomials.* Trans. Of the American Mathematical Society 35(3): 559-584, 1933

The ring of Linearized Polynomials

Linearized Polynomials

$$F(x) = \sum_{i=0}^{d} f_i x^{q^i} = \sum_{i=0}^{d} f_i x^{[i]}, \text{ with } f_d \neq 0$$

The $q-$degree $\deg_q(F) = d$

$(\mathbb{F}_{q^m}\langle x^q \rangle, + , \circ)$ is a **left (right) euclidean domain**

$\downarrow$

Euclidean left (right) division

O. Ore *On a special class of polynomials*. Trans. Of the American Mathematical Society 35(3): 559-584, 1933

The ring of Linearized Polynomials

Lemma:

Let V an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ with a basis $\mathscr{B} = \{v_1, \ldots, v_d\}$. There exists a unique monic polynomial $P_V \in \mathbb{F}_{q^m}\langle x \rangle$ with $\deg_q(P_V) = d$ such that $P_V(v_i) = 0$.

Annihilator polynomial

O. Ore *On a special class of polynomials*. Trans. Of the American Mathematical Society 35(3): 559-584, 1933

Gabidulin codes

Gabidulin codes:

Let $k < n \leq m$, $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ where $w_R(\boldsymbol{g}) = n$

$$Gab(n,k) := \{(F(g_1), \ldots, F(g_n)) \mid F \in \mathbb{F}_{q^m}\langle x \rangle_{<k}\}$$

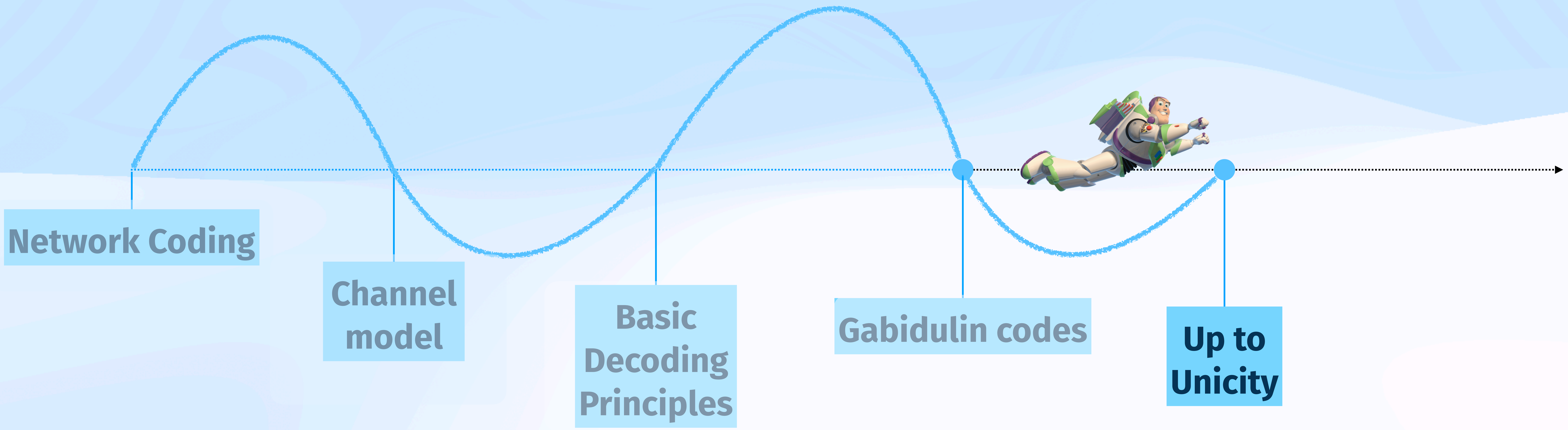
MRD codes : $d = n - k + 1$

$$D_{BMD} : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}\langle x \rangle_{<k} \cup \{?\}$$

such that $\forall \boldsymbol{y} \in \mathbb{F}_{q^m}^n$,

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

Part 2 : Rank metric



- Welch Berlekamp
- Loidreau’s algorithm

Welch-Berlekamp key equation

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

- $E := Supp(\boldsymbol{e})$ error support, $\varepsilon := w_R(\boldsymbol{e})$
- Λ the annihilator of E

$$\boxed{V(g_i) = D(y_i)}$$

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

If $n \geq (\varepsilon + k) + (\varepsilon + 1) - 1 \implies$ the (left) rational reconstruction problem

admits a unique solution, i.e. the minimal solution is $(\Lambda(x) \circ f(x), \Lambda(x))$

Welch Berlekamp-like Algorithm

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

1. Solve the corresponding **rational function reconstruction problem** $\rightarrow (V, D)$
2. Perform the left Euclidean division of V by D
   - if the remainder is 0 $\rightarrow$ outputs $F = V/_l D$
   - Otherwise outputs $?$

A. Wachter-Zeh, V. Afanassiev, V. Sidorenko. *Fast decoding of Gabidulin codes.*. Design, Codes and Cryptography, 66: 55-73, 2013

The Loidreau's algorithm

Goal : solving the left rational function reconstruction

$$\boxed{V(g_i) = D(y_i)}$$

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

Idea : iteratively construct (V_0^i, D_0^i) and (V_1^i, D_1^i), with $i \leq n$, such that

$$\forall j \leq i, . \quad \begin{cases} D_0(y_j) - V_0(g_j) = 0 \\ D_1(y_j) - V_1(g_j) = 0 \end{cases} \longrightarrow \text{Interpolation problems}$$

In the end either (V_0^n, D_0^n) or (V_1^n, D_1^n) satisfy the degree constraints

P. Loidreau. *A Welch-Berlekamp like algorithm for decoding Gabidulin codes.* WCCC 2005, 36-45

The Loidreau's algorithm

Regularity and Predictable Control Flow

- At each iteration, the $q-$degrees of (V_j^i, D_j^i) **increases by at most 1**.
- The algorithm performs a **fixed number of iterations**
- No early stopping, no data-dependent branching → **constant-time behavior**.

↓

Suitable in cryptography

To prevent **timing attacks** and **side-channel leakage**

N. Aragon, C. Baïsse, A. Fraga, P. Gaborit, I. Z. *Constant-time decoding of Gabidulin codes and their generalizations with applications to RQC*, Submitted, 2025

L. Bidoux, P. Briaud, M. Bros, P. Gaborit. *RQC revisited and more cryptanalysis for rank-based cryptography.* IEEE Trans. Inf. Theory 70(3):2271-2286

Another useful property of Gabidulin codes

$$\boxed{V(g_i) = D(y_i)}$$

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

Remark: $V(g_i) \in Gab(n, k + \varepsilon)$

$$\boxed{D(y_i) \in Gab(n, k + \varepsilon)}$$

$\deg_q(D) \leq \varepsilon$

A. Couvreur, I. Z. *An extension of Overbeck's attack with an application to cryptanalysis of Twisted Gabidulin-based schemes.* PQ Crypto 2023.

Another useful property of Gabidulin codes

$$\boxed{D(y_i) \in Gab(n, k+\varepsilon)}$$

$\deg_q(D) \leq \varepsilon$

Lemma:

$$\Lambda_t(Gab(n,k)) = Gab(n, k+t)$$

Find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{y} - \boldsymbol{e} \in Gab(n,k)$

A. Couvreur, I. Z. *An extension of Overbeck's attack with an application to cryptanalysis of Twisted Gabidulin-based schemes.* PQ Crypto 2023.

Another useful property of Gabidulin codes

$$\boxed{D(y_i) \in Gab(n, k + \varepsilon)}$$

$\deg_q(D) \leq \varepsilon$

Lemma:

$$\Lambda_t(Gab(n,k)) = Gab(n, k+t)$$

Find $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{y} - \boldsymbol{e} \in Gab(n,k)$

Gabidulin codes can be decoded solely from the knowledge of a generator matrix

A. Couvreur, I. Z. *An extension of Overbeck's attack with an application to cryptanalysis of Twisted Gabidulin-based schemes.* PQ Crypto 2023.

Syndrome key equation

Let $Gab(n, k)$ a Gabidulin code with parity check H

Let $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ and $E = Supp(\boldsymbol{e})$, where $\varepsilon := w_R(\boldsymbol{e})$

Syndrome $\boldsymbol{s} = H\boldsymbol{y}^T = H\boldsymbol{e}^T$

$$\boxed{V(x) = D(x) \circ S(x) \operatorname{mod}_{left} x^{[n-k]}}$$

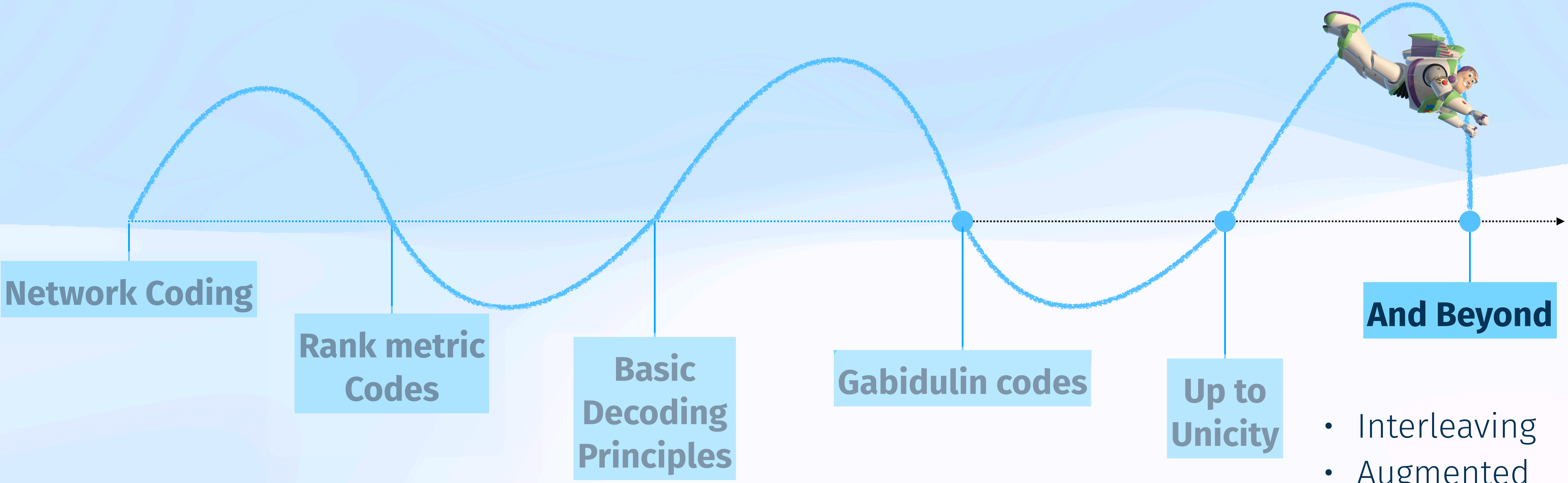
$\deg_q(V) < \varepsilon$

$\deg_q(D) \leq \varepsilon$

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

M. Gadouleau, Z. Yan *Complexity of decoding Gabidulin codes*. 2nd Annual Conference on Information Sciences and Systems, 1081-1085, 2008

Part 2 : Rank metric



- Interleaving
- Augmented Gabidulin codes

Interleaved Gabidulin codes

Interleaved Gabidulin codes

Let $k < n \leq m$, $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ where $w_R(\boldsymbol{g}) = n$ and $l \geq 1$

$$IGab(n,k) := \{(\boldsymbol{f}(g_1), \ldots, \boldsymbol{f}(g_n))^T \mid \boldsymbol{f} \in \mathbb{F}_{q^m}\langle x^q \rangle_{<k}^{l \times 1}\}$$

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

$$\begin{pmatrix} f_1(g_1), f_1(g_2), \ldots, f_1(g_n) \\ f_2(g_1), f_2(g_2), \ldots, f_2(g_n) \\ \vdots \\ f_l(g_1), f_l(g_2), \ldots, f_l(g_n) \end{pmatrix}$$

P. Loidreau, R. Overbeck *Decoding errors beyond the error-correction capability.* ACCT-10, 168-190 (2006)

Interleaved Gabidulin codes

Interleaved Gabidulin codes

Let $k < n \leq m$, $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ where $w_R(\boldsymbol{g}) = n$ and $l \geq 1$

$$IGab(n,k) := \{(\boldsymbol{f}(g_1), \ldots, \boldsymbol{f}(g_n))^T \mid \boldsymbol{f} \in \mathbb{F}_{q^m}\langle x^q \rangle_{<k}^{l \times 1}\}$$

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

$$R = \begin{pmatrix} f_1(g_1), f_1(g_2), \ldots, f_1(g_n) \\ f_2(g_1), f_2(g_2), \ldots, f_2(g_n) \\ \vdots \\ f_l(g_1), f_l(g_2), \ldots, f_l(g_n) \end{pmatrix} + \mathscr{E} \in \mathbb{F}_{q^m}^{l \times n} \Longrightarrow Supp(\mathscr{E}^1) = \ldots = Supp(\mathscr{E}^l)$$

Interleaved Gabidulin codes

- Let $R = \begin{pmatrix} f_1(\alpha_1), f_1(\alpha_2), \ldots, f_1(\alpha_n) \\ f_2(\alpha_1), f_2(\alpha_2), \ldots, f_2(\alpha_n) \\ \vdots \\ f_l(\alpha_1), f_l(\alpha_2), \ldots, f_l(\alpha_n) \end{pmatrix} + \mathscr{E} \in \mathbb{F}_{q^m}^{l \times n}$ be a received matrix
- $\mathscr{E} \in \mathbb{F}_{q^m}^{l \times n}$ is the **error matrix,** $E := Supp(\mathscr{E}^i)$ is the **error support,** $\varepsilon = w_R(\mathscr{E}^i)$
- Λ **error annihilator** polynomial.

$$\boxed{V_j(g_i) = D(y_i)}$$

$\deg_q(V_j) \leq \varepsilon + k - 1$ $\quad$ $\deg_q(D) \leq \varepsilon$

Interleaved Gabidulin codes

$$\boxed{V_j(g_i) = D(y_i)}$$

$\deg_q(V_j) \leq \varepsilon + k - 1$ $\qquad$ $\deg_q(D) \leq \varepsilon$

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 $\longrightarrow$ **unique with high probability**

P. Loidreau, R. Overbeck *Decoding errors beyond the error-correction capability.* ACCT-10, 168-190 (2006)

The power of adding zeros in rank metric : augmented Gabidulin

Augmented Gabidulin codes:

Let $k < n' < m < n$, $\boldsymbol{g} \in \mathbb{F}_{q^m}^{n'}$ where $w_R(\boldsymbol{g}) = n'$

$$AGab(n,k) := \{(F(g_1), \ldots, F(g_{n'}), 0, \ldots, 0) \mid F \in \mathbb{F}_{q^m}\langle x \rangle_{<k}\} \subseteq \mathbb{F}_{q^m}^n$$

Minimum distance : $d = n' - k + 1$

These codes **admit a BD decoder** allowing to correct up to $\tau_{AUG} := \lfloor \frac{n' - k + t}{2} \rfloor$ with probability

$$1 - \frac{1}{\tau_{\mathrm{AUG}}(n-n')} \sum_{i=t}^{\tau_{\mathrm{AUG}}-1} \prod_{j=0}^{t-1} \frac{(q^{\tau_{\mathrm{AUG}}} - q^j)(q^{n-n'} - q^j)}{q^t - q^j}$$

L. Bidoux, P. Briaud, M. Bros, P. Gaborit. *RQC revisited and more cryptanalysis for rank-based cryptography*. IEEE Trans. Inf. Theory 70(3):2271-2286

The power of adding zeros in rank metric : augmented Gabidulin

Augmented Gabidulin codes:

Let $k < n' < m < n$, $\boldsymbol{g} \in \mathbb{F}_{q^m}^{n'}$ where $w_R(\boldsymbol{g}) = n'$

$$AGab(n,k) := \{(F(g_1), \ldots, F(g_{n'}), 0, \ldots, 0) \mid F \in \mathbb{F}_{q^m}\langle x \rangle_{<k}\} \subseteq \mathbb{F}_{q^m}^n$$

Minimum distance : $d = n' - k + 1$

These codes **admit a BD decoder** allowing to correct up to $\tau_{AUG} := \lfloor \frac{n' - k + t}{2} \rfloor$ with high probability

Based on Loidreau's algorithm

N. Aragon, C. Baïsse, A. Fraga, P. Gaborit, I. Z. *Constant-time decoding of Gabidulin codes and their generalizations with applications to RQC*, Submitted, 2025

Interleaved VS Augmented

Interleaved Gabidulin

- Multiple received words
- Same error support
- More words $\Rightarrow$ more constraints on the error support
- Decoding radius $\tau_{IRS} = \dfrac{l(n-k)}{l+1}$

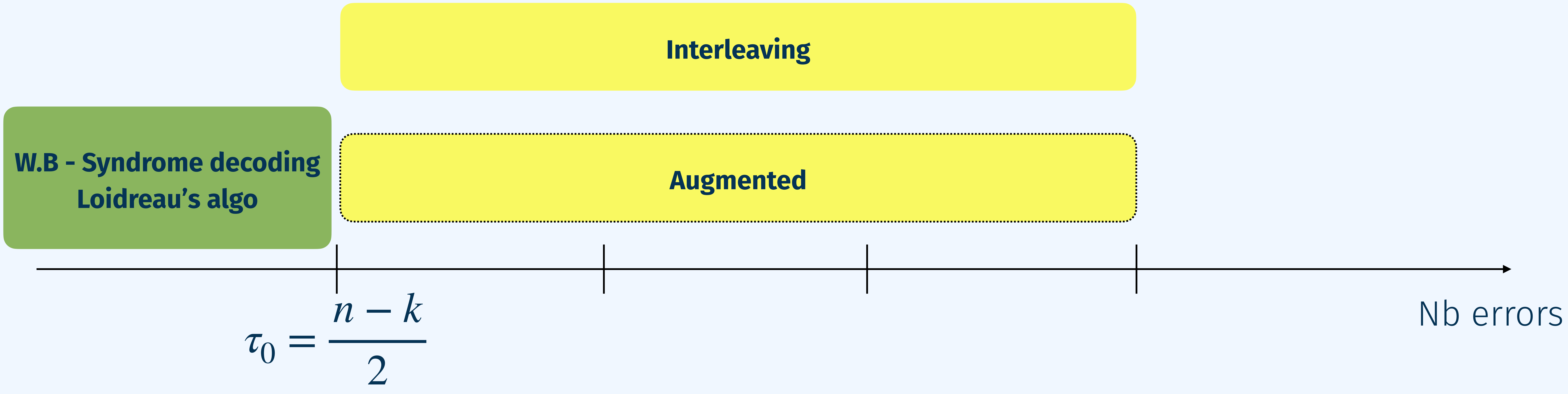
Augmented Gabidulin

- Single received word, zeros in the codeword at fixed positions
- Those positions provide direct info on the error
- More information $\Rightarrow$ partial information of the error support
- Decoding radius $\tau_{AUG} = \dfrac{(n' - k + t)}{2}$

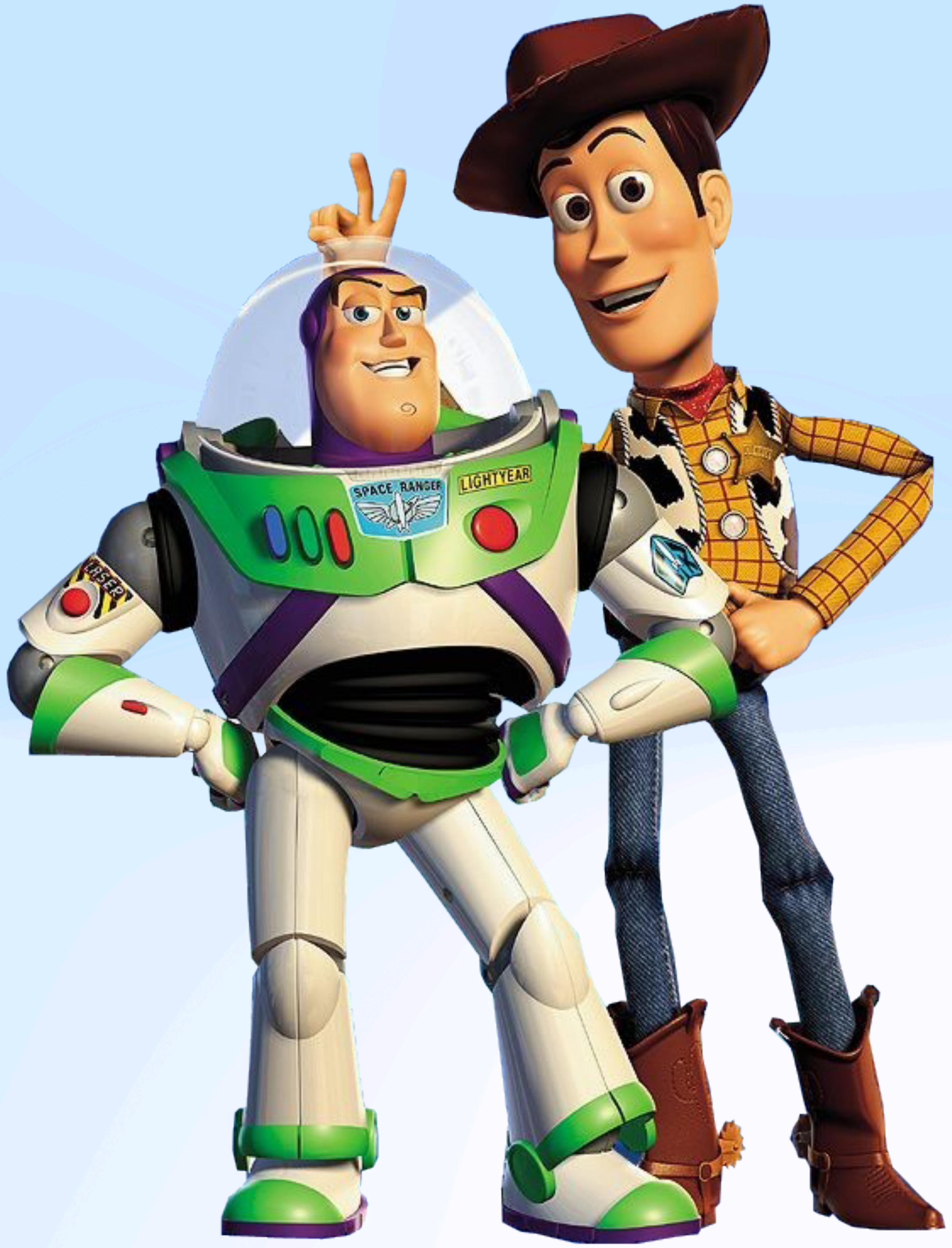
Both give extra independent information about the same error support

Conclusions

Decoding Gabidulin codes



- BMD decoder (unique)
- BD decoder (unique with probability)
- List decoder $\longrightarrow$?



Thank you.