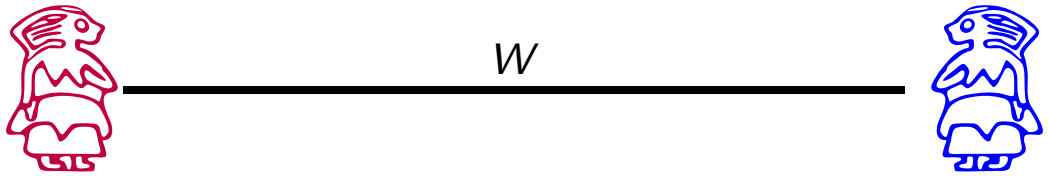
Introducción a códigos polares

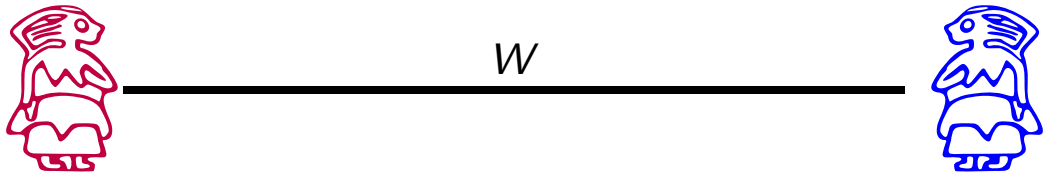
Eduardo Camps Moreno

Escuela Superior de Física y Matemáticas

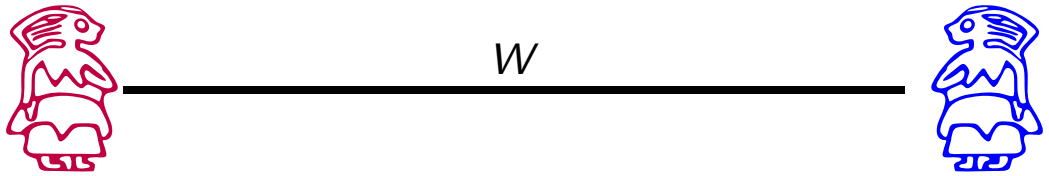
4 de marzo, 2021

Universidad de la Laguna, Tenerife

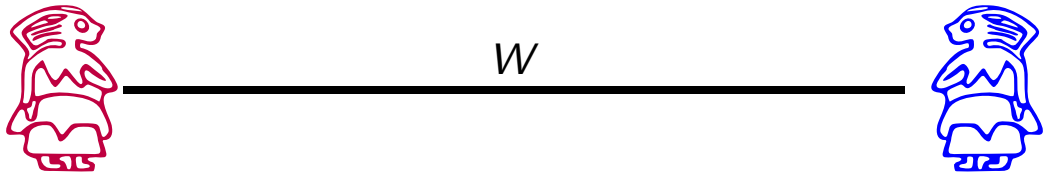

W



A

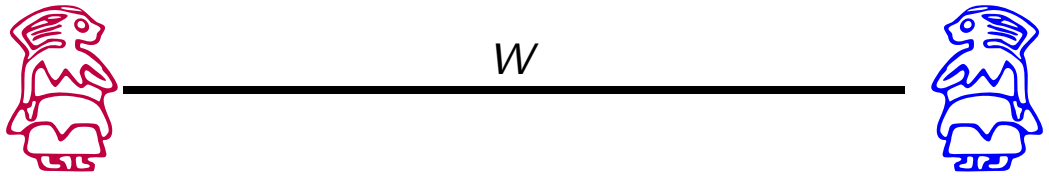


$$A \xrightarrow{W} B$$



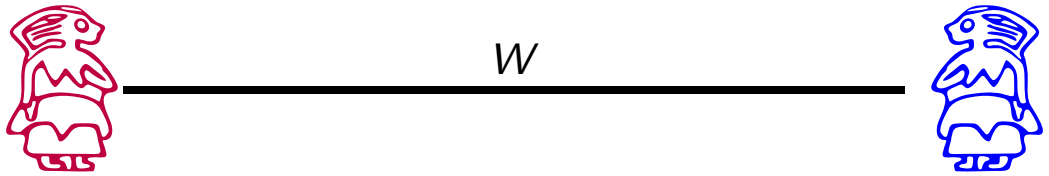
$$A \xrightarrow{W} B$$

$$0 \xrightarrow{W} 0$$



$$A \xrightarrow{W} B$$

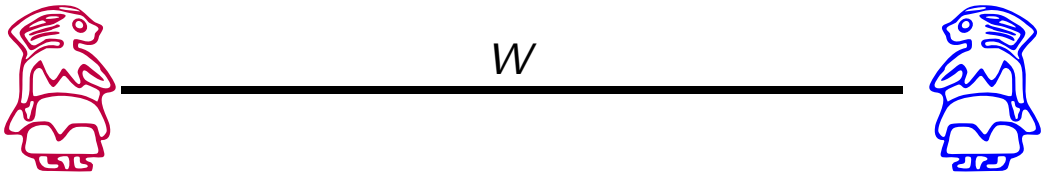
$$0 \xrightarrow{W} 0 \qquad \ddot{\smile}$$



$$A \xrightarrow{W} B$$

$$0 \xrightarrow{W} 0 \qquad \text{☺}$$

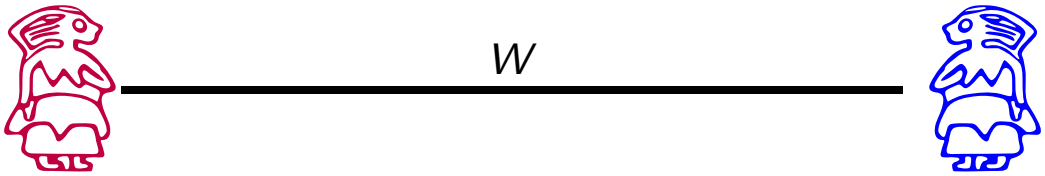
$$0 \xrightarrow{W} 1$$



$$A \xrightarrow{W} B$$

$$0 \xrightarrow{W} 0 \qquad \text{☺}$$

$$0 \xrightarrow{W} 1 \qquad \text{☹}$$

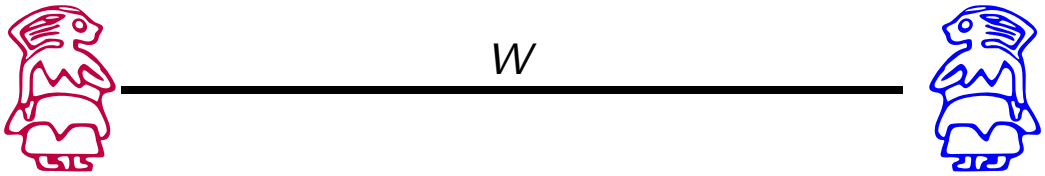


$$A \xrightarrow{W} B$$

$$0 \xrightarrow{W} 0 \qquad \text{☺}$$

$$0 \xrightarrow{W} 1 \qquad \text{☹}$$

$$W(y|x)$$



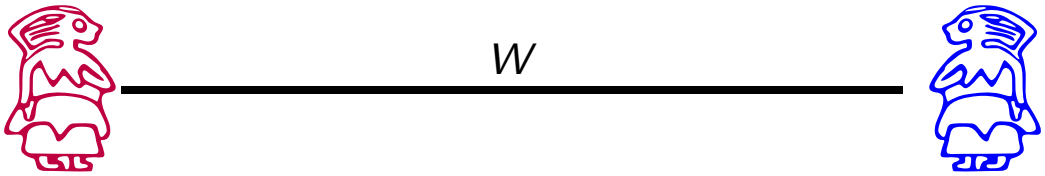
$$A \xrightarrow{W} B$$

$$0 \xrightarrow{W} 0 \qquad \text{☺}$$

$$0 \xrightarrow{W} 1 \qquad \text{☹}$$

$$W(y|x)$$

$$W(x|x) = 1, \;\; W(y|x) = 0, y \neq x$$



$$A \xrightarrow{W} B$$

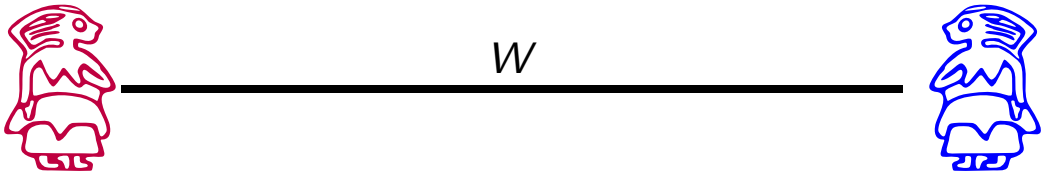
$$0 \xrightarrow{W} 0 \qquad \text{☺}$$

$$0 \xrightarrow{W} 1 \qquad \text{☹}$$

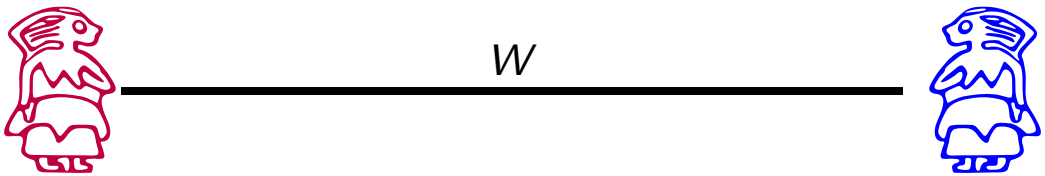
$$W(y|x)$$

$$W(x|x) = 1, \;\; W(y|x) = 0, y \neq x$$

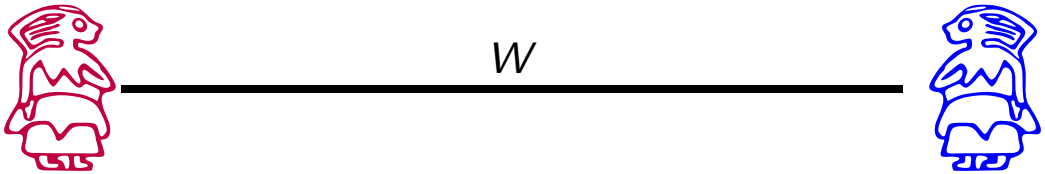
$$W(x|x) = p, \;\; W(y|x) = 1 - p, y \neq x$$



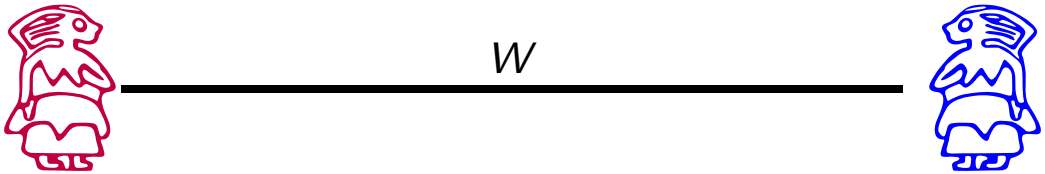
$$0 \xrightarrow{C} 0000$$



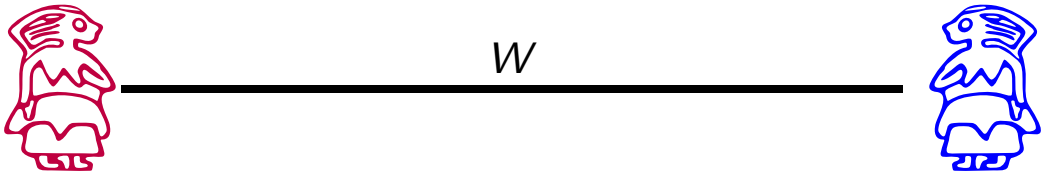
$$0 \xrightarrow{C} 0000 \xrightarrow{W} 0100$$



$$0 \xrightarrow{C} 0000 \xrightarrow{W} 0100 \xrightarrow[\substack{0000\\1111}]{}$$

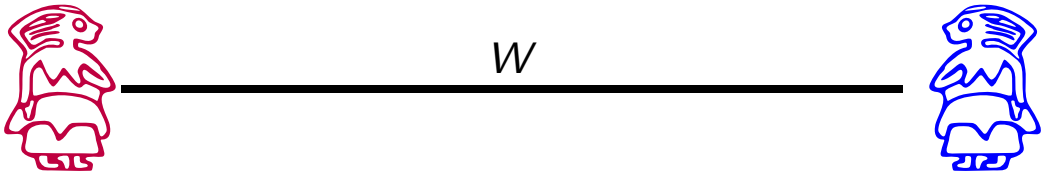


$$0 \xrightarrow{C} 0000 \xrightarrow{W} 0100 \xrightarrow[\substack{0000\\1111}]{} 0000 \xrightarrow{D} 0$$



$$0 \xrightarrow{C} 0000 \xrightarrow{W} 0100 \xrightarrow[\substack{0000\\1111}]{} 0000 \xrightarrow{D} 0$$

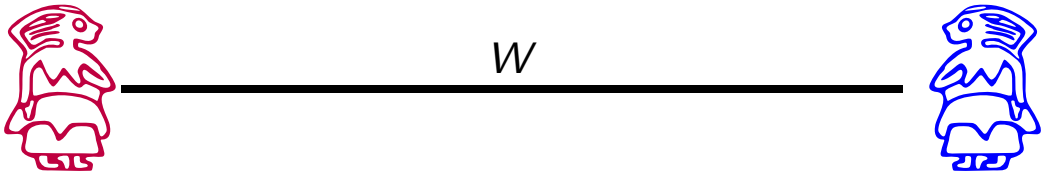
$$m \xrightarrow{C} m' \xrightarrow{W} r' \xrightarrow{D} r$$



$$0 \xrightarrow{C} 0000 \xrightarrow{W} 0100 \xrightarrow[\substack{0000\\1111}]{} 0000 \xrightarrow{D} 0$$

$$m \xrightarrow{C} m' \xrightarrow{W} r' \xrightarrow{D} r$$

$$¿m = r?$$



$$0 \xrightarrow{C} 0000 \xrightarrow{W} 0100 \xrightarrow[\substack{0000\\1111}]{} 0000 \xrightarrow{D} 0$$

$$m \xrightarrow{C} m' \xrightarrow{W} r' \xrightarrow{D} r$$

$$¿m = r?$$

$$P_e(C, W, D) = P(m \neq r)$$

Códigos lineales

$$\Sigma = \mathbb{F}_q$$

Códigos lineales

$$\Sigma = \mathbb{F}_q$$

$$C < \mathbb{F}_q^n$$

Códigos lineales

$$\Sigma = \mathbb{F}_q$$

$$C < \mathbb{F}_q^n$$

$$n \equiv \text{longitud}$$

$$k := \dim C$$

Códigos lineales

$$w(c) = |\{i \mid c_i \neq 0\}$$

Códigos lineales

$$w(c) = |\{i \mid c_i \neq 0\}$$

$$w(0111) = 3$$

Códigos lineales

$$w(c) = |\{i \mid c_i \neq 0\}$$

$$w(0111) = 3$$

$$d(c, c') = w(c - c')$$

Códigos lineales

$$w(c) = |\{i \mid c_i \neq 0\}$$

$$w(0111) = 3$$

$$d(c, c') = w(c - c')$$

$$\delta(C) = \min\{d(c, c') \mid c, c' \in C, c \neq c'\} = \min\{w(c) \mid c \in C \setminus \{0\}\}$$

- $\delta \leq n - k + 1$

- $\delta \leq n - k + 1$
- Si $e > \dfrac{\delta - 1}{2}$ entonces la decodificación puede no ser única. ☹

- $\delta \leq n - k + 1$
- Si $e > \dfrac{\delta - 1}{2}$ entonces la decodificación puede no ser única. ☹

$$0000 \to 0011 \to \begin{cases} 1111 & ? \\ 0000 & ? \end{cases}$$

- $\delta \leq n - k + 1$
- Si $e > \dfrac{\delta - 1}{2}$ entonces la decodificación puede no ser única. ☹

$$0000 \to 0011 \to \begin{cases} 1111 & ? \\ 0000 & ? \end{cases}$$

- Si $e > \delta(C) - 1$, la detección puede no ser posible.

- $\delta \leq n - k + 1$
- Si $e > \dfrac{\delta - 1}{2}$ entonces la decodificación puede no ser única. ☹

$$0000 \to 0011 \to \begin{cases} 1111 & ? \\ 0000 & ? \end{cases}$$

- Si $e > \delta(C) - 1$, la detección puede no ser posible.

$$0000 \to 1111 \xrightarrow{D} 1 \ ☺$$

$W(y|x)$ es conocida

1. $|\Sigma_X| = q$ y $\Sigma_x = \mathbb{F}_q$.
2. $|\Sigma_y| < \infty$

$W(y|x)$ es conocida

1. $|\Sigma_X| = q$ y $\Sigma_x = \mathbb{F}_q$.
2. $|\Sigma_y| < \infty$
3. $$W(y_1^n|x_1^n) = \prod_{i=1}^{n} W(y_i|x_i)$$

$W(y|x)$ es conocida

1. $|\Sigma_X| = q$ y $\Sigma_x = \mathbb{F}_q$.
2. $|\Sigma_y| < \infty$
3. $$W(y_1^n|x_1^n) = \prod_{i=1}^{n} W(y_i|x_i)$$
4. $W(y|x) = W(\sigma(y)|\psi_\sigma(x))$

$W(y|x)$ es conocida

1. $|\Sigma_X| = q$ y $\Sigma_x = \mathbb{F}_q$.
2. $|\Sigma_y| < \infty$
3. $$W(y_1^n|x_1^n) = \prod_{i=1}^{n} W(y_i|x_i)$$
4. $W(y|x) = W(\sigma(y)|\psi_\sigma(x))$

	0	1
0	2/3	1/3
1	1/3	2/3

$$m \xrightarrow{C} m' \xrightarrow{W} r' \xrightarrow{D} r$$

$$m \xrightarrow{C} m' \xrightarrow{W} r' \xrightarrow{D} r$$

1. (MDD) $D(r') = \operatorname{argmin} \{d(m', r) \mid m' \in C\}$

$$m \xrightarrow{C} m' \xrightarrow{W} r' \xrightarrow{D} r$$

1. (MDD) $D(r') = \operatorname{argmin} \{d(m', r) \mid m' \in C\}$
2. (MLD) $D(r') = \operatorname{argmax} \{P(r'|m') \mid m' \in C\}$

$$m \xrightarrow{C} m' \xrightarrow{W} r' \xrightarrow{D} r$$

1. (MDD) $D(r') = \operatorname{argmin} \{d(m', r) \mid m' \in C\}$
2. (MLD) $D(r') = \operatorname{argmax} \{P(r'|m') \mid m' \in C\}$
3. (MLDAP) $D(r') = \operatorname{argmax} \{P(m'|r') \mid m' \in C\}$.

$$m \xrightarrow{C} m' \xrightarrow{W} r' \xrightarrow{D} r$$

1. (MDD) $D(r') = \operatorname{argmin} \{d(m', r) \mid m' \in C\}$
2. (MLD) $D(r') = \operatorname{argmax} \{P(r'|m') \mid m' \in C\}$
3. (MLDAP) $D(r') = \operatorname{argmax} \{P(m'|r') \mid m' \in C\}$.

Prop.

Supongamos $W(x|x) = p$ y $W(y|x) = \dfrac{1-p}{q-1}$. Si $p > \dfrac{1}{q}$, entonces MDD coincide con MLD.

$$m \xrightarrow{C} m' \xrightarrow{W} r' \xrightarrow{D} r$$

1. (MDD) $D(r') = \operatorname{argmin} \{d(m', r) \mid m' \in C\}$
2. (MLD) $D(r') = \operatorname{argmax} \{P(r'|m') \mid m' \in C\}$
3. (MLDAP) $D(r') = \operatorname{argmax} \{P(m'|r') \mid m' \in C\}$.

Prop.

Supongamos $W(x|x) = p$ y $W(y|x) = \dfrac{1-p}{q-1}$. Si $p > \dfrac{1}{q}$, entonces MDD coincide con MLD.

$$P(y_1^n|x_1^n) = \prod_{i=1}^{n} W(y_i|x_i) = p^{n-d(x,y)} \left(\frac{1-p}{q-1}\right)^{d(x,y)}$$

$$W : X \to Y$$

$$W : X \to Y$$

$$0 \leq I(W) = \frac{1}{q} \sum_{x \in X} \sum_{y \in Y} W(y|x) \log_q \frac{W(y|x)}{W_Y(y)} \leq 1$$

$$W : X \to Y$$

$$0 \leq I(W) = \frac{1}{q} \sum_{x \in X} \sum_{y \in Y} W(y|x) \log_q \frac{W(y|x)}{W_Y(y)} \leq 1$$

Teorema de canal ruidoso [1948]

Dado cualquier canal W, para $\epsilon > 0$ y para $k < nI(W)$, si n es suficientemente grande, existe un código C de longitud n, $\dim C \geq k$ y un algoritmo de decodificación tal que la probabilidad de error de bloque es $\leq \epsilon$.

$$W : X \to Y$$

$$0 \leq I(W) = \frac{1}{q} \sum_{x \in X} \sum_{y \in Y} W(y|x) \log_q \frac{W(y|x)}{W_Y(y)} \leq 1$$

Teorema de canal ruidoso [1948]

Dado cualquier canal W, para $\epsilon > 0$ y para $k < nI(W)$, si n es suficientemente grande, existe un código C de longitud n, $\dim C \geq k$ y un algoritmo de decodificación tal que la probabilidad de error de bloque es $\leq \epsilon$.

$$m \xrightarrow{C} m' \xrightarrow{W} r' \xrightarrow{D} r$$

1. La demostración no es constructiva.
2. Para un código lineal, la complejidad de codificación es sencilla, pero la decodificación puede no serlo.

1. La demostración no es constructiva.
2. Para un código lineal, la complejidad de codificación es sencilla, pero la decodificación puede no serlo.

1. $\{C_n, D_n\}$ tales que $P_e \to 0$ cuando $n \to \infty$.
2. La complejidad de D_n es tratable.

1. La demostración no es constructiva.
2. Para un código lineal, la complejidad de codificación es sencilla, pero la decodificación puede no serlo.

1. $\{C_n, D_n\}$ tales que $P_e \to 0$ cuando $n \to \infty$.
2. La complejidad de D_n es tratable.

- Turbo codes
- LDPC
- Concatenation codes.

Códigos polares

$$G_A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Códigos polares

$$G_A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$(u_1, u_2) \rightarrow u_1^2 G_A = (u_1 + u_2, u_2) \xrightarrow{W} (y_1, y_2)$$

$$W_1(y_1 y_2 | u_1 u_2) = W(y_1 | u_1 + u_2) W(y_2 | u_2)$$

Códigos polares

$$G_A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$(u_1, u_2) \rightarrow u_1^2 G_A = (u_1 + u_2, u_2) \xrightarrow{W} (y_1, y_2)$$

$$W_1(y_1 y_2 | u_1 u_2) = W(y_1 | u_1 + u_2) W(y_2 | u_2)$$

$$W(x|x) = \frac{2}{3}$$

Códigos polares

$$G_A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$(u_1, u_2) \rightarrow u_1^2 G_A = (u_1 + u_2, u_2) \xrightarrow{W} (y_1, y_2)$$

$$W_1(y_1 y_2 | u_1 u_2) = W(y_1 | u_1 + u_2) W(y_2 | u_2)$$

$$W(x|x) = \frac{2}{3}$$

$$(10) \rightarrow (10) G_A = (1 + 0, 0) \xrightarrow{W} (01)$$

$$W_1(01|10) = W(0|1) W(1|0) = \frac{1}{9}$$

$$u_1 \rightarrow (u_1, u_2)G_A \xrightarrow{W} (y_1, y_2)$$

$$W_1^{(1)}(y_1, y_2|u_1)$$

$$u_1 \rightarrow (u_1, u_2)G_A \xrightarrow{W} (y_1, y_2)$$

$$W_1^{(1)}(y_1, y_2|u_1)$$

$$u_2 \rightarrow (u_1, u_2)G_A \xrightarrow{W} (y_1, y_2)$$

$$W_1^{(2)}(y_1, y_2, u_1|u_2)$$

$$W_1$$

$$(u_1, u_2) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \xrightarrow{W} (y_1, y_2)$$

$$W_1^{(1)}$$

$$(u_1, u_2) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \xrightarrow{W} (y_1, y_2)$$

$$W_1^{(2)}$$

$$(u_1, u_2) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \xrightarrow{W} (y_1, y_2)$$

$$W_1^{(2)}$$

$$u_2 \xrightarrow{W_1^{(2)}} (y_1, y_2, u_1) \downarrow y_2$$

$$W_1^{(2)}$$

$$u_2 \xrightarrow{W_1^{(2)}} (y_1, y_2, u_1) \downarrow y_2$$

$$P(y_2|u_2)$$

$$W_1^{(2)}$$

$$u_2 \xrightarrow{W_1^{(2)}} (y_1, y_2, u_1)$$
$$\downarrow$$
$$y_2$$

$$P(y_2|u_2) = W(y_2|u_2)$$

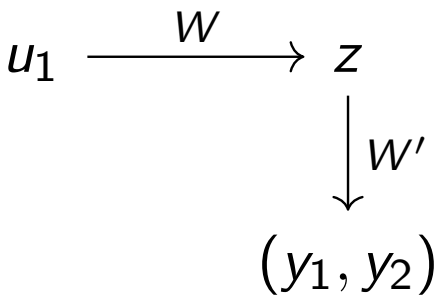
$$W_1^{(2)}$$

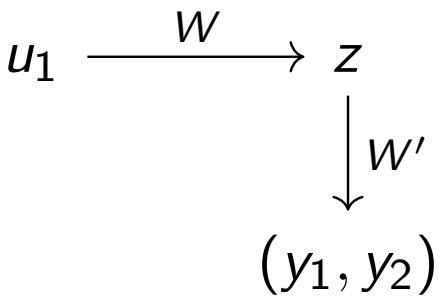
$$u_2 \xrightarrow{W_1^{(2)}} (y_1, y_2, u_1)$$
$$\downarrow$$
$$y_2$$

$$P(y_2|u_2) = W(y_2|u_2)$$

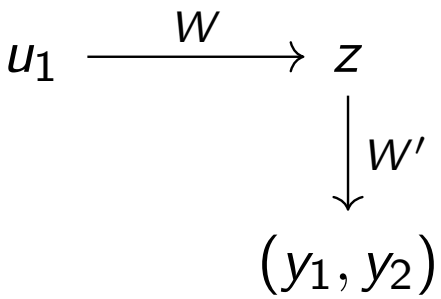
$$W \preceq W_1^{(2)}$$

$$I(W) \leq I(W_1^{(2)})$$


u_1
W
z
W'
(y_1, y_2)



$$P(y_1, y_2|u_1) = W_1^{(1)}(y_1, y_2|u_1)$$



$$P(y_1, y_2|u_1) = W_1^{(1)}(y_1, y_2|u_1)$$

$$W_1^{(1)} \preceq W \preceq W_1^{(2)}$$

$$I(W_1^{(1)}) \leq I(W) \leq I(W_1^{(2)})$$

$$(u_1, u_2) \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \xrightarrow{W} (y_1, y_2)$$

$$A \in \mathcal{M}_{m\times n},\ B \in \mathcal{M}_{m'\times n'}$$

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

$$A \in \mathcal{M}_{m\times n},\ B \in \mathcal{M}_{m'\times n'}$$

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \end{bmatrix},\ B = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

$$A \in \mathcal{M}_{m\times n},\ B \in \mathcal{M}_{m'\times n'}$$

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \end{bmatrix},\ B = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

$$A \otimes B = \begin{bmatrix} 1 & 2 & & \\ 0 & 3 & & \\ & & & \\ & & & \end{bmatrix}$$

$$A \in \mathcal{M}_{m\times n},\ B \in \mathcal{M}_{m'\times n'}$$

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \end{bmatrix},\ B = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

$$A \otimes B = \left[\begin{array}{cc|cc} 1 & 2 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ & & & \\ & & & \end{array}\right.$$

$$A \in \mathcal{M}_{m\times n},\ B \in \mathcal{M}_{m'\times n'}$$

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \end{bmatrix},\ B = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

$$A \otimes B = \left[\begin{array}{cc|cc|cc} 1 & 2 & 0 & 0 & 2 & 4 \\ 0 & 3 & 0 & 0 & 0 & 6 \\ & & & & & \\ & & & & & \end{array}\right.$$

$$A \in \mathcal{M}_{m\times n},\ B \in \mathcal{M}_{m'\times n'}$$

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \end{bmatrix},\ B = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

$$A \otimes B = \left[\begin{array}{cc|cc|cc} 1 & 2 & 0 & 0 & 2 & 4 \\ 0 & 3 & 0 & 0 & 0 & 6 \\ \hline 0 & 0 & 1 & 2 & 3 & 6 \\ 0 & 0 & 0 & 3 & 0 & 9 \end{array}\right]$$

$$G_2 = G_A^{\otimes 2} = G_A \otimes G_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$G_2 = G_A^{\otimes 2} = G_A \otimes G_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$W_1^{(1)}$$

$$(u_1, u_2, u_3, u_4) G_A \xrightarrow{W} (y_1, y_2, y_3, y_4)$$

$$G_2 = G_A^{\otimes 2} = G_A \otimes G_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$W_2^{(1)}, W_2^{(2)}$$

$$(u_1, u_2, u_3, u_4) G_A \xrightarrow{W} (y_1, y_2, y_3, y_4)$$

$$G_2 = G_A^{\otimes 2} = G_A \otimes G_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$W_2^{(1)}, W_2^{(2)}, W_2^{(3)}$$

$$(u_1, u_2, u_3, u_4) G_A \xrightarrow{W} (y_1, y_2, y_3, y_4)$$

$$G_2 = G_A^{\otimes 2} = G_A \otimes G_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$W_2^{(1)}, W_2^{(2)}, W_2^{(3)}, W_2^{(4)}$$

$$(u_1, u_2, u_3, u_4) G_A \xrightarrow{W} (y_1, y_2, y_3, y_4)$$

$$G_2 = G_A^{\otimes 2} = G_A \otimes G_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$G_2 = G_A^{\otimes 2} = G_A \otimes G_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$W_2^{(1)} = (W_1^{(1)})^{(1)}$$

$$G_2 = G_A^{\otimes 2} = G_A \otimes G_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$W_2^{(1)} = (W_1^{(1)})^{(1)}$$

$$(u_1, u_2) \to (u_1, u_2)G_A = (u_1 + u_2, u_2) \xrightarrow{W_1^{(1)}}$$

$$G_2 = G_A^{\otimes 2} = G_A \otimes G_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$W_2^{(1)} = (W_1^{(1)})^{(1)}$$

$$(u_1, u_2) \to (u_1, u_2)G_A = (u_1 + u_2, u_2) \xrightarrow{W_1^{(1)}} ((y_1 y_2), (y_3 y_4))$$

$$G_2 = G_A^{\otimes 2} = G_A \otimes G_A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$W_2^{(1)} = (W_1^{(1)})^{(1)}$$

$$(u_1, u_2) \to (u_1, u_2)G_A = (u_1 + u_2, u_2) \xrightarrow{W_1^{(1)}} ((y_1 y_2), (y_3 y_4))$$

$$W_2^{(2)} = (W_1^{(2)})^{(1)}$$

$$W_2^{(3)} = (W_1^{(1)})^{(2)}$$

$$W_2^{(4)} = (W_1^{(2)})^{(2)}$$

$$W_2^{(i)} \preceq W \preceq W_2^{(i')}$$

$$0 \leq I(W_2^{(i)}) \leq I(W) \leq I(W_2^{(i')}) \leq 1$$

$$W_2^{(i)} \preceq W \preceq W_2^{(i')}$$

$$0 \leq I(W_2^{(i)}) \leq I(W) \leq I(W_2^{(i')}) \leq 1$$

$$G_n = G^{\otimes n}$$

$$0 \leq I(W_n^{(i)}) \leq I(W) \leq I(W_n^{(i')}) \leq 1$$

$$W_2^{(i)} \preceq W \preceq W_2^{(i')}$$

$$0 \leq I(W_2^{(i)}) \leq I(W) \leq I(W_2^{(i')}) \leq 1$$

$$G_n = G^{\otimes n}$$

$$0 \leq I(W_n^{(i)}) \leq I(W) \leq I(W_n^{(i')}) \leq 1$$

$$\text{¿} \lim_{n \to \infty} I\left(W_n^{(i_n)}\right)?$$

Polarización

Teorema [Arikan, 2008]

Sea $1 > \delta > 0$. Entonces

$$\lim_{n\to\infty} \frac{|\{i \in [n] \mid I(W_n^{(i)}) \in (1-\delta, 1]\}|}{2^n} = I(W)$$

Polarización

Teorema [Arikan, 2008]

Sea $1 > \delta > 0$. Entonces

$$\lim_{n\to\infty} \frac{|\{i \in [n] \mid I(W_n^{(i)}) \in (1-\delta, 1]\}|}{2^n} = I(W)$$

$$\lim_{n\to\infty} \frac{|i \in [n] \mid I(W_n^{(i)}) \in [0, \delta)\}|}{2^n} = 1 - I(W)$$

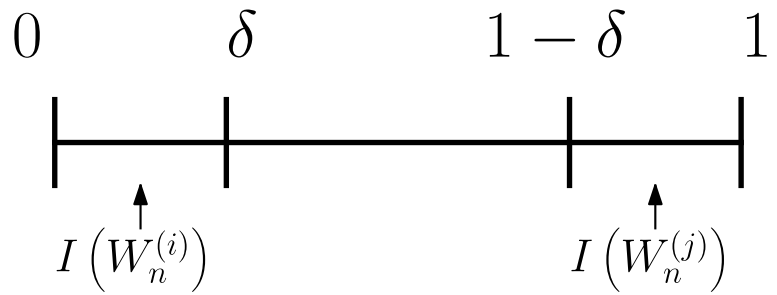
Polarización

Teorema [Arikan, 2008]

Sea $1 > \delta > 0$. Entonces

$$\lim_{n\to\infty} \frac{|\{i \in [n] \mid I(W_n^{(i)}) \in (1-\delta, 1]\}|}{2^n} = I(W)$$

$$\lim_{n\to\infty} \frac{|i \in [n] \mid I(W_n^{(i)}) \in [0, \delta)\}|}{2^n} = 1 - I(W)$$



Códigos polares

$$\mathcal{A}_n \subset [n]$$

Códigos polares

$$\mathcal{A}_n \subset [n]$$

$$i \in \mathcal{A}_n \Longrightarrow I\left(W_n^{(i)}\right) \geq I\left(W_n^{(j)}\right),\ \forall j \notin \mathcal{A}_n$$

Códigos polares

$$\mathcal{A}_n \subset [n]$$

$$i \in \mathcal{A}_n \Longrightarrow I\left(W_n^{(i)}\right) \geq I\left(W_n^{(j)}\right),\ \forall j \notin \mathcal{A}_n$$

$C_{\mathcal{A}_n}$ es el generado por los renglones de G_n indexados por $\mathcal{A}_n$

Códigos polares

$$\mathcal{A}_n \subset [n]$$

$$i \in \mathcal{A}_n \Longrightarrow I\left(W_n^{(i)}\right) \geq I\left(W_n^{(j)}\right),\ \forall j \notin \mathcal{A}_n$$

$C_{\mathcal{A}_n}$ es el generado por los renglones de G_n indexados por $\mathcal{A}_n$

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$C_{\{2,4\}} = \langle (1100), (1111) \rangle$$

Cancelación sucesiva

$$(a, b) \longrightarrow (0, a, 0, b)G_2 \xrightarrow{W} (y_1, y_2, y_3, y_4)$$

Cancelación sucesiva

$$(0, a, 0, b)G_2 \xrightarrow{W} (y_1, y_2, y_3, y_4)$$

Cancelación sucesiva

$$(0, a, 0, b)G_2 \xrightarrow{W} (y_1, y_2, y_3, y_4)$$

$$N = 2^n$$

$$u_1^N G_n \xrightarrow{W} y_1^N$$

Cancelación sucesiva

$$(0, a, 0, b)G_2 \xrightarrow{W} (y_1, y_2, y_3, y_4)$$

$$N = 2^n$$

$$u_1^N G_n \xrightarrow{W} y_1^N \xrightarrow{D} \bar{u}_1^N$$

Cancelación sucesiva

$$(0, a, 0, b)G_2 \xrightarrow{W} (y_1, y_2, y_3, y_4)$$

$$N = 2^n$$

$$u_1^N G_n \xrightarrow{W} y_1^N \xrightarrow{D} \bar{u}_1^N$$

$$\bar{u}_i = \begin{cases} 0 & i \notin \mathcal{A}_n \end{cases}$$

Cancelación sucesiva

$$(0, a, 0, b)G_2 \xrightarrow{W} (y_1, y_2, y_3, y_4)$$

$$N = 2^n$$

$$u_1^N G_n \xrightarrow{W} y_1^N \xrightarrow{D} \bar{u}_1^N$$

$$\bar{u}_i = \begin{cases} 0 & i \notin \mathcal{A}_n \\ \text{argmax} \left\{ W_n^{(i)} \left(y_1^N, u_1^{i-1} | u \right) \ | u \in \mathbb{F}_q \right\} & i \in \mathcal{A}_n \end{cases}$$

Cancelación sucesiva

$$(0, a, 0, b)G_2 \xrightarrow{W} (y_1, y_2, y_3, y_4)$$

$$N = 2^n$$

$$u_1^N G_n \xrightarrow{W} y_1^N \xrightarrow{D} \bar{u}_1^N$$

$$\bar{u}_i = \begin{cases} 0 & i \notin \mathcal{A}_n \\ \operatorname{argmax} \left\{ W_n^{(i)} \left(y_1^N, u_1^{i-1} | u \right) \ | u \in \mathbb{F}_q \right\} & i \in \mathcal{A}_n \end{cases}$$

$$O(n \log n)$$

$$\lim_{n\to\infty} P_e = 0$$

$$I(W_n^{(i)}) \geq \log_2 \frac{2}{1+2^{-n/2}},\ i \in \mathcal{A}_n$$

Teorema [Anderson, Matthews, 2014]

$$Pe = O(2^{-2^{n/2}})$$

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$0101 \rightarrow (0101)G_2 = 0011 \xrightarrow{W} 0111$$

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$0101 \rightarrow (0101)G_2 = 0011 \xrightarrow{W} 0111$$

$$\bar{u}_1 = 0$$

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$0101 \to (0101)G_2 = 0011 \xrightarrow{W} 0111$$

$$\bar{u}_1 = 0$$

$$W_2^{(2)}(0111, 0|0) = \frac{14}{648}, \quad W_2^{(2)}(0111, 0|1) = \frac{20}{648}$$

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$0101 \rightarrow (0101)G_2 = 0011 \xrightarrow{W} 0111$$

$$\bar{u}_1 = 0$$

$$W_2^{(2)}(0111, 0|0) = \frac{14}{648}, \quad W_2^{(2)}(0111, 0|1) = \frac{20}{648} \qquad \bar{u}_2 = 1$$

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$0101 \to (0101)G_2 = 0011 \xrightarrow{W} 0111$$

$$\bar{u}_1 = 0$$

$$W_2^{(2)}(0111, 0|0) = \frac{14}{648}, \quad W_2^{(2)}(0111, 0|1) = \frac{20}{648} \qquad \bar{u}_2 = 1$$

$$\bar{u}_3 = 0$$

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$0101 \to (0101)G_2 = 0011 \xrightarrow{W} 0111$$

$$\bar{u}_1 = 0$$

$$W_2^{(2)}(0111, 0|0) = \frac{14}{648}, \quad W_2^{(2)}(0111, 0|1) = \frac{20}{648} \qquad \bar{u}_2 = 1$$

$$\bar{u}_3 = 0$$

$$W_2^{(4)}(0111, 010|0) = \frac{2}{648}, \quad W_2^{(4)}(0111, 010|1) = \frac{8}{648}$$

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$0101 \to (0101)G_2 = 0011 \xrightarrow{W} 0111$$

$$\bar{u}_1 = 0$$

$$W_2^{(2)}(0111, 0|0) = \frac{14}{648}, \quad W_2^{(2)}(0111, 0|1) = \frac{20}{648} \qquad \bar{u}_2 = 1$$

$$\bar{u}_3 = 0$$

$$W_2^{(4)}(0111, 010|0) = \frac{2}{648}, \quad W_2^{(4)}(0111, 010|1) = \frac{8}{648}$$

$$\bar{u}_4 = 1$$

Anderson, S. E., Matthews, G. L. (2014). Exponents of polar codes using algebraic geometric code kernels. Designs, codes and cryptography, 73(2), 699-717.

Arikan, E. (2009). Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. IEEE Transactions on information Theory, 55(7), 3051-3073.

Shannon, C. E. (1948). A mathematical theory of communication. ACM SIGMOBILE mobile computing and communications review, 5(1), 3-55.