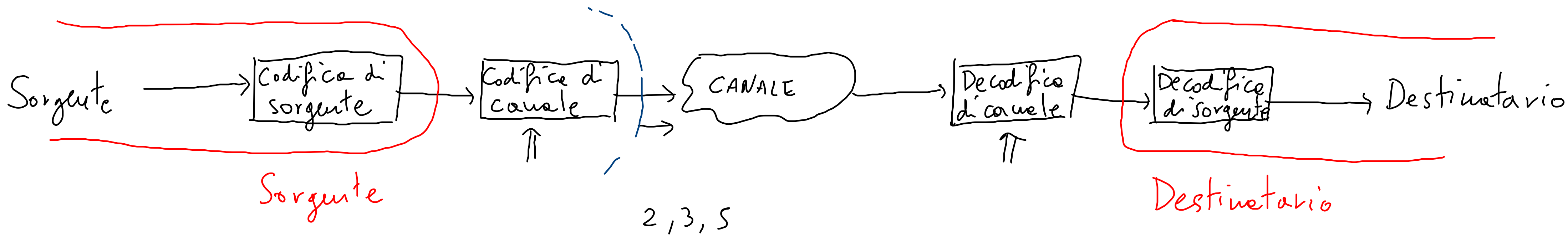
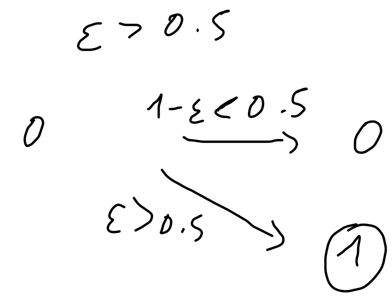
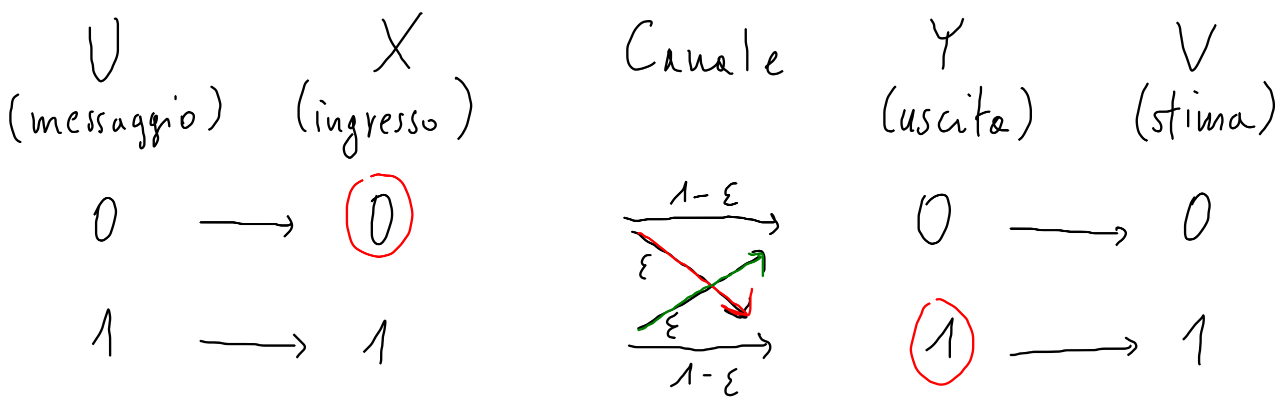


Codifica di Canale (cap. 4 e 6)





Canale simmetrico binario.

$\boxed{\varepsilon = 0.1}$

Vogliamo bassa probabilità di errore: $P_{err} = P_r[V \neq U] = P_r[(U=0 \wedge V=1) \vee (U=1 \wedge V=0)]$

$$= P_r[U=0 \wedge V=1] + P_r[U=1 \wedge V=0] = P_r[X=0 \wedge Y=1] + P_r[X=1 \wedge Y=0]$$

$$= P_r[X=0] \cdot \underbrace{P_r[Y=1 \mid X=0]}_{\varepsilon} + P_r[X=1] \cdot \underbrace{P_r[Y=0 \mid X=1]}_{\varepsilon} = \varepsilon\,(\underbrace{P_r[X=0] + P_r[X=1]}_{1}) = \varepsilon.$$

Codificare sequenze più lunghe per rilevare e/o correggere errori

Es. $n=2$ $\{00, \cancel{01}, \cancel{10}, 11\}$: Se $u=0$, codifico $x=00$; se ricevo $\overset{y}{00}$ decodifico in $\overset{v}{0}$
Se $u=1$, codifico $x=11$; se ricevo 11 decodifico in 1
se ricevo $\underline{01}$ o 10 rilevo errore.

$00 \to 01$
$11 \to 01$

Es. $n=3$ $u=0 \to x=\boxed{000}$
$u=1 \to x=\boxed{111}$

$\varepsilon = 10^{-1}$ 10^{-1}

Decodifico a maggioranza

$\varepsilon^3 + 3\varepsilon^2(1-\varepsilon)$

Se $y \in \{000, 001, 010, 100\} \to$ decodifico $v=0$

$10^{-3} + \underbrace{3 \cdot 10^{-2}(0.9)}_{} \simeq 3 \cdot 10^{-2}$

Se $y \in \{111, 110, 101, 011\} \to$ decodifico $v=1$. Quanto vale P_{err} ?

$\to$ $Pr[V=1 | U=0] = Pr[Y \in \{111, 110, 101, 011\} \mid X=000] = Pr[Y=111 \mid X=000] + Pr[Y=110 | X=000] + Pr[Y=101 | X=000] +$
$+ Pr[Y=011 | X=000] = \varepsilon^3 + \varepsilon \cdot \varepsilon \cdot (1-\varepsilon) + \varepsilon(1-\varepsilon)\varepsilon + (1-\varepsilon)\varepsilon\varepsilon = \varepsilon^3 + 3\varepsilon^2(1-\varepsilon)$.

$\to$ $Pr[V=0 | U=1] = Pr[Y \in \{000, 001, 010, 100\} | X=111] = \varepsilon^3 + 3\varepsilon^2(1-\varepsilon)$.

Quindi $P_{err} = Pr[V=1 \wedge U=0] + Pr[V=0 \wedge U=1] = Pr[U=0] \cdot Pr[V=1 | U=0] + Pr[U=1] \cdot Pr[V=0 | U=1]$
$= (\cancel{Pr[U=0] + Pr[U=1]})(\varepsilon^3 + 3\varepsilon^2(1-\varepsilon)) < \varepsilon$
per ogni $\varepsilon < 0.5$

Codici di canale

Un codice di canale (codice blocco q-ario) $\mathcal{C}$ è un sottoinsieme di $\mathcal{A}^n$ ($\mathcal{C} \subseteq \mathcal{A}^n$)

$q = |\mathcal{A}|$

Ogni $\vec{x} \in \mathcal{C}$ è detta parola di codice. (n è la lunghezza delle parole di codice)

(Nell'ultimo esempio: $\mathcal{A} = \{0,1\}$, $q=2$, $\mathcal{C} = \{\overset{\xleftrightarrow{n}}{000}, 111\} \subseteq \mathcal{A}^3$ $(n=3)$)

codice blocco binario con $n=3$

Se $M = |\mathcal{C}|$ è la cardinalità del codice $\qquad \log_q M \leq n$

Per rilevare errori occorre che $M < q^n$ (si ha sempre $M \leq q^n$)

Tasso di trasmissione del codice: $R \triangleq \frac{1}{n} \log_q M \leq 1$

$0 \to 0$

$1 \to 1$

$n=1 \quad k=1$

$q=2$

$M=2 \quad k = \log_2 2 = 1$

$R=1$

Se $\log_q M$ è intero: $k = \log_q M$ sono q-it di informazione $\Rightarrow R = \frac{1}{n} k = \frac{k}{n}$

$n-k$ sono q-it di controllo

$|\mathcal{A}^n| = q^n \qquad \overset{M}{\overset{\shortparallel}{|\mathcal{C}|}} = q^{Rn}$

Vogliamo un tasso alto (ma una probabilità di errore). Notiamo anche

$$\log_q M = nR \to M = q^{(nR)}$$

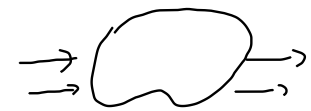
Descrizione del canale

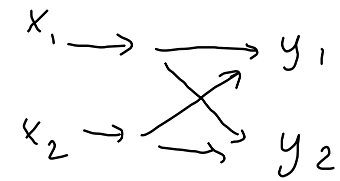
$\mathcal{X} = \{x_1, \dots, x_i, \dots\}$

$\mathcal{Y} = \{y_1, \dots, y_j, \dots\}$

Canale stazionario e senza memoria:

$$\Pr(\vec{y} \mid \vec{x}) = \prod_{r=1}^{n} p(y_{j_r} \mid x_{i_r})$$





$x_i \in \mathcal{X}$ simbolo in ingresso

$y_j \in \mathcal{Y}$ simbolo in uscita

Il canale è descritto dalle probabilità condizionate $p(y_j \mid x_i)$ $\forall i \; \forall j$

Matrice di transizione del canale Γ

$$\Gamma = \underbrace{\begin{bmatrix} p(y_1|x_1) & p(y_2|x_1) & \cdots & p(y_{|\mathcal{Y}|}|x_1) \\ & & \boxed{p(y_j|x_i)} & \\ p(y_1|x_{|\mathcal{X}|}) & p(y_2|x_{|\mathcal{X}|}) & \cdots & p(y_{|\mathcal{Y}|}|x_{|\mathcal{X}|}) \end{bmatrix}}_{\text{Colonne: simboli di uscita}} \begin{matrix} \\ \leftarrow i \\ \\ \end{matrix}$$

j

Righe: simboli di ingresso

$$I(X;Y) = \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} \overset{\text{Regole di Bayes}}{=} \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} p(x)p(y|x) \log \frac{\cancel{p(x)}\,p(y|x)}{\cancel{p(x)}\,p(y)}$$

Inoltre: $p(y) = \sum_{x\in\mathcal{X}} p(x,y) = \sum_{x\in\mathcal{X}} p(x)\cdot p(y|x)$

→ Posso esprimere $I(X;Y)$ in termini di $\underbrace{p_X}_{\text{caratteristica della sorgente}}$ e $\underbrace{p_{Y|X}}_{\text{caratteristica del canale}}$

(e della codifica di canale)

Capacità di un canale $C = \max_{p_X} I(X;Y) = \max_{p_X} [H(X) - H(X|Y)]$

$$= \max_{p_X} [H(Y) - H(Y|X)]$$

$H(X|Y)$: incertezza che rimane su X nota Y (informazione "persa"; equivocazione)

$H(Y|X)$: quantità di informazione che perviene a Y ma non dipende da X (ambiguità)

4.2.1 Canale senza rumore

$|X| = |Y| = m$ e una corrispondenza biunivoca tra x_i e y_i

$$m \left\{ \begin{tikzcd}[row sep=tiny] x_1 \arrow[r, "1"] & y_1 \\ x_2 \arrow[r, "1"] & y_2 \\ x_3 \arrow[r, "1"] & y_3 \end{tikzcd} \right.$$

$$p(y_j|x_i) = \begin{cases} 1 & \text{se } j = i \\ 0 & \text{se } j \neq i \end{cases}$$

Γ è la matrice identità $m \times m$

$i \neq j \to \cancel{0 \log 0}$ $\quad i = j \Rightarrow \cancel{1 \log 1}$

$$\Gamma = \begin{array}{c} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{matrix} \leftarrow x_1 \\ \leftarrow x_2 \\ \leftarrow x_3 \end{matrix} \\ \begin{matrix} \downarrow & \downarrow & \downarrow \\ y_1 & y_2 & y_3 \end{matrix} \end{array}$$

Equivocazione $H(X|Y) = -\sum_{i,j} p(x_i, y_j) \log p(x_i|y_j) = 0$

$$p(x_i|y_j) \overset{\text{Bayes}}{=} \frac{p(x_i)\, p(y_j|x_i)}{p(y_j)} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

Ambiguità $H(Y|X) = E[\log p(Y_j|X_i)] = 0$

Mutua informazione : $I(X;Y) = H(Y) - \overbrace{H(Y|X)}^{0} = H(X) - \overbrace{H(X|Y)}^{0} = H(X)$

Capacità del canale : $C = \max_{P_X} I(X;Y) = \max_{P_X} H(X) = \log m$.