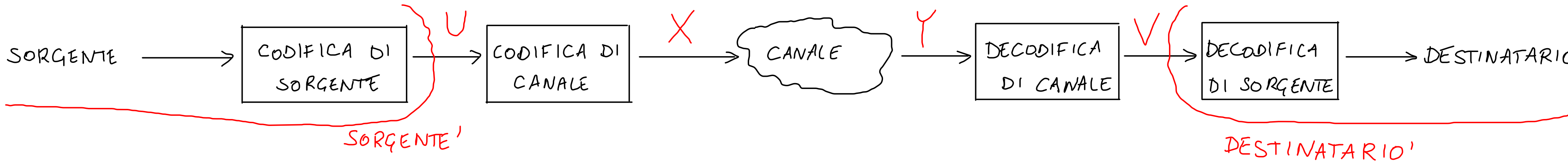
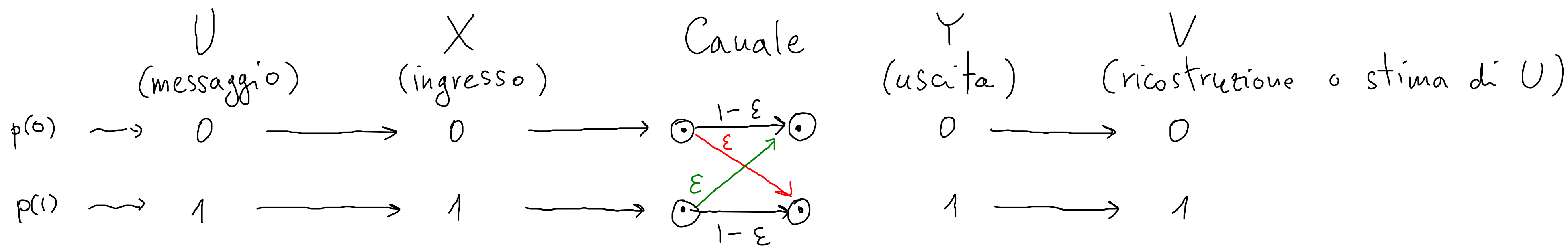


CODIFICA/DECODIFICA DI CANALE (FABRIS CAP. 4 E 6)



$\varepsilon \in [0, 1/2]$ parametro

Canale binario simmetrico

↓

ε è anche detto parametro di errore

Probabilità di errore nella ricostruzione: $Pr[V \neq U]$

$$P_{err} = Pr[V \neq U] = Pr[(U=0 \wedge V=1) \vee (U=1 \wedge V=0)] =$$

$$= Pr[U=0 \wedge V=1] + Pr[U=1 \wedge V=0] =$$

$$= Pr[V=1 \mid U=0] \cdot Pr[U=0] + Pr[V=0 \mid U=1] \cdot Pr[U=1]$$

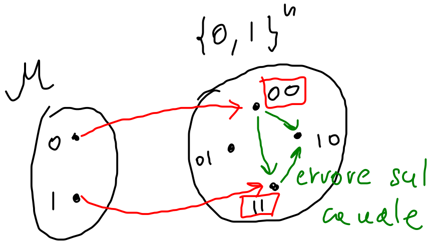
$U=X,\ V=Y$

$$= Pr[Y=1 \mid X=0] \cdot Pr[U=0] + Pr[Y=0 \mid X=1] \cdot Pr[U=1]$$

$$= \varepsilon \cdot Pr[U=0] + \varepsilon \cdot Pr[U=1] = \varepsilon(Pr[U=0] + Pr[U=1]) = \varepsilon \cdot 1 = \varepsilon.$$

Idea: codificare i messaggi con sequenze più lunghe per rilevare e/o correggere gli errori sul canale

Es. $n=2$ Se $u=0$, codifico con $x=00$; se ricevo 00, decodifico in 0
Se $u=1$, codifico con $x=11$; se ricevo 11, decodifico in 1
se ricevo 01 o 10, rilevo errore.



Es. $\underline{n=3}$. Se $u=0$, codifico con $x=\boxed{000}$;
$u=1$, " " $x=\boxed{111}$;

V

In decodifica, se ricevo $y\in\{000,001,010,100\}$, decodifico in 0
se ricevo $y\in\{111,110,101,011\}$, decodifico in 1

Quanto vale p_{err}?

$$U=0 \rightarrow X=000 \xrightarrow{?} 111$$

$$p_{err}=Pr[U\neq V]=\boxed{Pr[V=1|U=0]}Pr[U=0]+\boxed{Pr[V=0|U=1]}Pr[U=1]$$

$$Pr[V=1|U=0]=Pr[Y\in\{111,110,101,011\}|U=0]=Pr[Y=111|U=0]+Pr[Y=110|U=0]+Pr[Y=101|U=0]+Pr[Y=011|U=0]$$

$$=\varepsilon\cdot\varepsilon\cdot\varepsilon+\varepsilon\cdot\varepsilon\cdot(1-\varepsilon)+\varepsilon(1-\varepsilon)\varepsilon+(1-\varepsilon)\varepsilon\cdot\varepsilon=\varepsilon^3+3(1-\varepsilon)\varepsilon^2<\varepsilon^3+3\varepsilon^2<4\varepsilon^2$$

$$Pr[V=0|U=1]=Pr[Y\in\{000,001,010,100\}|U=1]=\varepsilon^3+3(1-\varepsilon)\varepsilon^2<4\varepsilon^2$$

$$p_{err}=(\varepsilon^3+3(1-\varepsilon)\varepsilon^2)Pr[U=0]+(\varepsilon^3+3(1-\varepsilon)\varepsilon^2)Pr[U=1]=\varepsilon^3+3(1-\varepsilon)\varepsilon^2<4\varepsilon^2$$

Codici di canale

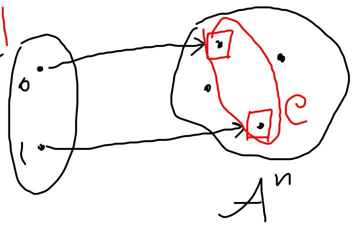
$q = |\mathcal{A}|$, $\mathcal{A}$ = alfabeto del canale ; n = lunghezza delle parole di codice

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

Ogni $x \in \mathcal{C}$ è detta parola di codice

Nell'ultimo esempio, $\mathcal{A} = \{0,1\}$, $q = 2$, $n = 3$, $\mathcal{C} = \{000, 111\} \subseteq \mathcal{A}^3$ (001 non è una parole di codice)

$M = |\mathcal{M}|$



La cardinalità del codice è $|\mathcal{C}| = |\mathcal{M}| =: M$

Si ha sempre $\mathcal{C} \subseteq \mathcal{A}^n \rightarrow M = |\mathcal{C}| \leq |\mathcal{A}^n| = q^n \rightarrow M \leq q^n$

$\log_q M \leq n$

Per rilevare errori occorre che $M < q^n$

Tasso di trasmissione del codice $\rightarrow R := \dfrac{\log_q M}{n} \leq \dfrac{n}{n} = 1$

Se $\log_q M$ è un intero k, allora $R = \dfrac{k}{n}$ e posso dire che degli n simboli delle sequenze di $\mathcal{A}^n$

k simboli sono simboli di informazione

$n-k$ simboli sono simboli di controllo

Es. Codice a ripetizione di lunghezza 3

$M = 2 \quad q = 2 \rightarrow \log_q M = \underset{k}{\underset{\shortparallel}{1}}$, $n = 3$

Osservazione : $M = |\mathcal{C}| = q^{Rn}$ (perché $Rn = \log_q M$)

Descrizione del canale

$\mathcal{X} = \{x_1, x_2, \dots, x_i, \dots\}$ alfabeto di ingresso

$\mathcal{Y} = \{y_1, y_2, \dots, y_j, \dots\}$ " " uscita

Canale stazionario e senza memoria:

x parola di ingresso

y parola di uscita

$$\Pr[y \mid x] = \prod_{r=1}^{n} \Pr[y_{j_r} \mid x_{i_r}]$$

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

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

Il canale è descritto dalle probabilità condizionate $\Pr[y_j \mid x_i]$ $\forall i \; \forall j$

Matrice di transizione del canale

Γ dove

$$\Gamma_{ij} := \Pr[y_j \mid x_i]$$

$$\Gamma = \begin{bmatrix} p(y_1|x_1) & p(y_2|x_1) & \cdots & p(y_m|x_1) \\ p(y_1|x_2) & \cdots & & \\ & & & \\ p(y_1|x_K) & \cdots & & \end{bmatrix}$$

Righe: simboli in ingresso

Colonne: simboli in uscita

v.a. simbolo in ingresso

v.a. simbolo in uscita

$I(X;Y)$

$$= \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}$$

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

$\rightarrow$ Posso esprimere $I(X;Y)$ in termini di $p_X(\cdot)$ e di $p_{Y|X}(\cdot)$

$p_X(\cdot)$ $\downarrow$ descrive la sorgente

$p_{Y|X}(\cdot)$ $\downarrow$ descrive il canale

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

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

$H(X|Y)$ è detta equivocazione

$H(Y|X)$ è detta ambiguità

4.2.1 Canale senza rumore

Ho $|\mathcal{X}| = |\mathcal{Y}| = m$ e una corrispondenza biunivoca tra x_i e y_i

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

$$\begin{array}{l} x_1 \xrightarrow{1} y_1 \\ x_2 \xrightarrow{1} y_2 \\ x_3 \xrightarrow{1} y_3 \\ \quad\vdots \\ x_m \xrightarrow{1} y_m \end{array}$$

$$\Gamma = \begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & 0 & & 1 \end{bmatrix}$$

m^2

$$\Gamma \in \mathbb{R}^{|\mathcal{X}|\times|\mathcal{Y}|}$$

Equivocazione $H(X|Y) = -\sum_{i=1}^{m}\sum_{j=1}^{m} p(x_i, y_j) \log p(x_i|y_j) = 0$

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

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

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

$m = |\mathcal{X}|$