Teoria dell'informazione
Lezione II

Andrea Cosentino

5 January 2024

1 Limitazioni

La limitazione imposta la scorsa lezione, ovvero che il codice sia non singolare, non è sufficiente. Infatti, senza nessun'altra limitazione non possiamo decodificare un in modo univoco.

Esempio: La sorgente produde due simboli: A e B.
Se A viene codificato in 0, e B in 00, il codice è non singolare, ma se ricevo 00, non so se la stringa inviata era B o AA.

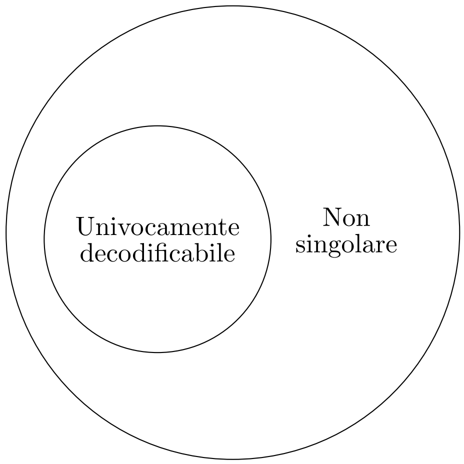
Introduciamo un'altra limitazione, questa volta sulla **estensione di un codice**. L'estensione del codice $c : \mathbb{X} \to \mathbb{D}^+$ è definita come

$$\mathbb{C} : \mathbb{X}^+ \to \mathbb{D}^+$$

Imponiamo che il codice sia **univocamente decodificabile**. Si dice che il codice è univocamente decodifcabile se e solo se la sua estensione è non singolare. Questa proprietà implica che

$$\forall\, y \,\epsilon\, \mathbb{D}^+ \text{ c'è al più un unico messaggio} x \,\epsilon\, \mathbb{X}^+ : \mathbb{C}(x) = y$$

Per determinare se un codice è univocamente decodificabile si usa l'algoritmo di **Sardinas-Patterson**. L'algoritmo ha complessita O(mL), dove m è il numero delle parole di codice ($|\mathbb{X}|$) e L è la somma delle loro lunghezze ($\sum_{x \epsilon \mathbb{X}} l(x)$).



In questo modo riusciamo a distinguere i simboli all'interno di una stringa in fase di decodifica. Il problema è che riusciamo solamente se abbiamo tutta la stringa. Questo non è sempre possibile (si pensi a situazioni in cui le informazioni arrivino in streaming senza terminare).
Dobbiamo aggiungere una limitazione che impedisca a una parola di codice di essere prefissa di un'altra.
Introduciamo il concetto i **codice istantaneo**. Un codice si dice istantaneo se nessuna parola è prefissa di un'altra.

2 Codici istantanei

> **FATTO**
>
> Se c è istantaneo allora è anche univocamente decodificabile

DIMOSTRAZIONE

Sia $c : \mathbb{X} \to \mathbb{D}^+$ e $\mathbb{C}$ la sua estensione.

Possiamo escludere il caso in cui c sia non singolare. Infatti, in questo caso, avrei 2 simboli che codificano nella stessa parola di codice. Due parole uguali sono l'una il prefisso dell'altra.

A questo punto resta da dimostrare che se c non è univocamente decodificabile allora non è istantaneo.
Assumiamo che c sia non univocamente decodificabile, quindi

$$\exists\, x \,,\, x^{'} \,\epsilon\, \mathbb{X} \,\text{con}\, x \neq x^{'} \,|\, \mathbb{C}(x) = \mathbb{C}(x^{'}) \tag{1}$$

x e $x^{'}$ possono differire in 2 modi soltanto:

- Un messaggio è prefisso dell'altro
- C'è almeno uuna posizione in cui i 2 messaggi differiscono

Se $\mathbb{C}(x) = \mathbb{C}(x^{'})$ e x è prefisso di $x^{'}$ (o viceversa) allora i restanti simboli di x dovrebbero per forza essere mappati in parola vuota.
Ma questo non è possibile, per costruzione infatti sappiamo che un simbolo non può essere mappato in una parola vuota. Ma anche se cambiassimo la nostra definizione, e ammettessimo la parola vuota, questo ci porterebbe a dire che il codice è non istantaneo, perché la parola vuota è prefisso di tutte le parole.

L'unico caso possibile è quindi il secondo.
Siccome $x \neq x^{'}$, c'è una posizione i tale che $x_i \neq x_i^{'}$.

Allora fino alla posizione i, ovvreo per $j = 1, .., i-1$ si ha che

$$\mathbb{C}(x_j) = \mathbb{C}(x_j^i)$$

Se però, $\mathbb{C}(x) = \mathbb{C}(x^i)$, allora $c(x_i)$ è prefisso di $c(x_i^{'})$ (o viceversa).

Questo perché, se fino alla posizione j sono uguale, e invece a i sono diverso, condizione necessaria affinché valga $\mathbb{C}(x) = \mathbb{C}(x^i)$ è che da j in poi, qualunque cosa ci sia dopo, io la codifico uguale. Questo non può succedere se $c(x_i)$ non è prefisso di $c(x_i^i)$ o viceversa.

Questo implica che il codice non è istantaneo.
Abbiamo dimostrato che

$$\text{codici istantanei} \subset \text{codici univocamente decodificabili}$$

LEMMA Disuguaglianza di Kraft

Dati $\mathbb{X} = \{x_1, .., x_n\}, D > 1$ e m interi $l_1, .., l_m > 0$, esiste n codice istantaneo $c : \mathbb{X} \to \mathbb{D}^+$ tale che $l_c(x_i) = l_i$ per $i = 1, .., m \leftrightarrow$

$$\sum_{i=1}^{m} D^{-l_i} \leq 1$$

Dimostro il lato $\to$.

Sia $l_{max} = \max_{i=1,...,m} l_c(x_i)$
Posso costruire un albero D-ario completo e di profondità l_max. Ogni nodo rappresnta una parola **possibile** di codice. Non è detto che sia utilizzata.