Informatica teorica

Indice

1. Lezione 01

1.1. Introduzione

1.1.1. Definizione

L'**informatica teorica** è quella branca dell'informatica che si "contrappone" all'informatica applicata: in quest'ultima, l'informatica è usata solo come uno *strumento* per gestire l'oggetto del discorso, mentre nella prima l'informatica diventa l'*oggetto* del discorso, di cui ne vengono studiati i fondamenti.

1.1.2. Cosa e come

Analizziamo i due aspetti fondamentali che caratterizzano ogni materia:

1. il **cosa**: l'informatica è la scienza che studia l'informazione e la sua elaborazione automatica mediante un sistema di calcolo. Ogni volta che ho un *problema* cerco di risolverlo automaticamente scrivendo un programma. *Posso farlo per ogni problema? Esistono problemi che non sono risolubili?* Possiamo chiamare questo primo aspetto con il nome di **teoria della calcolabilità**, quella branca che studia cosa è calcolabile e cosa non lo è, a prescindere dal costo in termini di risorse che ne deriva. In questa parte utilizzeremo una caratterizzazione molto rigorosa e una definizione di problema il più generale possibile, così che l'analisi non dipenda da fattori tecnologici, storici...
2. il **come**: è relazionato alla **teoria della complessità**, quella branca che studia la quantità di risorse computazionali richieste nella soluzione automatica di un problema. Con *risorsa computazionale* si intende qualsiasi cosa venga consumato durante l'esecuzione di un programma, ad esempio:
   - elettricità;
   - numero di processori;
   - tempo;
   - spazio di memoria.

   In questa parte daremo una definizione rigorosa di tempo, spazio e di problema efficientemente risolubile in tempo e spazio, oltre che uno sguardo al famoso problema `P = NP`.

Possiamo dire che il *cosa* è uno studio **qualitativo**, mentre il *come* è uno studio **quantitativo**.

Grazie alla teoria della calcolabilità individueremo le funzioni calcolabili, di cui studieremo la complessità.

1.2. Richiami matematici

1.2.1. Funzioni

Una **funzione** da un insieme A ad un insieme B è una *legge*, spesso indicata con f, che spiega come associare agli elementi di A un elemento di B.

Abbiamo due tipi di funzioni:

- **generale**: la funzione è definita in modo generale come $f : A \longrightarrow B$, in cui A è detto **dominio** di f e B è detto **codominio** di f;
- **locale/puntuale**: la funzione riguarda i singoli valori a e b:

$$f(a) = b \quad | \quad a \overset{f}{\longmapsto} b$$

  in cui b è detta **immagine** di a rispetto ad f e a è detta **controimmagine** di b rispetto ad f.

Possiamo categorizzare le funzioni in base ad alcune proprietà:

- **iniettività**: una funzione $f : A \longrightarrow B$ si dice *iniettiva* se e solo se:

$$\forall a_1, a_2 \in A \quad a_1 \neq a_2 \Longrightarrow f(a_1) \neq f(a_2)$$

In poche parole, non ho *confluenze*, ovvero *elementi diversi finiscono in elementi diversi.*

- **suriettività**: una funzione $f : A \longrightarrow B$ si dice *suriettiva* se e solo se:

$$\forall b \in B \quad \exists a \in A \mid f(a) = b.$$

In poche parole, *ogni elemento del codominio ha almeno una controimmagine.*

Se definiamo l'**insieme immagine**:

$$\mathrm{Im}_f = \{b \in B \mid \exists a \in A \text{ tale che } f(a) = b\} = \{f(a) \mid a \in A\} \subseteq B$$

possiamo dare una definizione alternativa di funzione suriettiva, in particolare una funzione è *suriettiva* se e solo se $\mathrm{Im}_f = B$.

Infine, una funzione $f : A \longrightarrow B$ si dice **biiettiva** se e solo se è iniettiva e suriettiva, quindi vale: $\forall b \in B \quad \exists! a \in A \mid f(a) = b$.

Se $f : A \longrightarrow B$ è una funzione biiettiva, si definisce **inversa** di f la funzione $f^{-1} : B \longrightarrow A$ tale che:

$$f(a) = b \iff f^{-1}(b) = a.$$

Per definire la funzione inversa f^{-1}, la funzione f deve essere biiettiva: se così non fosse, la sua inversa avrebbe problemi di definizione.

Un'operazione definita su funzioni è la **composizione**: date $f : A \longrightarrow B$ e $g : B \longrightarrow C$, la funzione f *composto* g è la funzione $g \circ f : A \longrightarrow C$ definita come $(g \circ f)(a) = g(f(a))$.

La composizione *non è commutativa*, quindi $g \circ f \neq f \circ g$ in generale, ma è *associativa*, quindi $(f \circ g) \circ h = f \circ (g \circ h)$.

La composizione *f composto g* la possiamo leggere come *prima agisce f poi agisce g*.

Dato l'insieme A, la **funzione identità** su A è la funzione $i_A : A \longrightarrow A$ tale che:

$$i_A(a) = a \quad \forall a \in A,$$

ovvero è una funzione che mappa ogni elemento su se stesso.

Grazie alla funzione identità, possiamo dare una definizione alternativa di funzione inversa: data la funzione $f : A \longrightarrow B$ biiettiva, la sua inversa è l'unica funzione $f^{-1} : B \longrightarrow A$ che soddisfa:

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_A .$$

Possiamo vedere f^{-1} come l'unica funzione che ci permette di *tornare indietro.*

2. Lezione 02

2.1. Richiami matematici

2.1.1. Funzioni totali e parziali

Prima di fare un'ulteriore classificazione per le funzioni, introduciamo la notazione $f(a)\downarrow$ per indicare che la funzione f è definita per l'input a, mentre la notazione $f(a)\uparrow$ per indicare la situazione opposta.

Ora, data $f : A \longrightarrow B$ diciamo che f è:
- **totale** se è definita *per ogni elemento* $a \in A$, ovvero $f(a)\downarrow \ \forall a \in A$;
- **parziale** se è definita *per qualche elemento* $a \in A$, ovvero $\exists a \in A \mid f(a)\uparrow$.

Chiamiamo **dominio** (o *campo*) **di esistenza** di f l'insieme

$$\mathrm{Dom}_f = \{a \in A \mid f(a)\downarrow\} \subseteq A.$$

Notiamo che:
- $\mathrm{Dom}_f \subsetneq A \Longrightarrow f$ parziale;
- $\mathrm{Dom}_f = A \Longrightarrow f$ totale.

2.1.2. Totalizzare una funzione

È possibile *totalizzazione* una funzione parziale definendo una funzione a tratti $f : A \longrightarrow B \cup \{\perp\}$ tale che

$$\overline{f}(a) = \begin{cases} f(a) & a \in \mathrm{Dom}_f(a) \\ \perp & \text{altrimenti} \end{cases}.$$

Il nuovo simbolo introdotto è il *simbolo di indefinito*, e viene utilizzato per tutti i valori per cui la funzione di partenza f non è appunto definita.

Da qui in avanti utilizzeremo $B_\perp$ come abbreviazione di $B \cup \{\perp\}$.

2.1.3. Prodotto cartesiano

Chiamiamo **prodotto cartesiano** l'insieme

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\},$$

che rappresenta l'insieme di tutte le *coppie ordinate* di valori in A e in B.

In generale, il prodotto cartesiano **non è commutativo**, a meno che $A = B$.

Possiamo estendere il concetto di prodotto cartesiano a n-uple di valori, ovvero

$$A_1 \times ... \times A_n = \{(a_1, ..., a_n) \mid a_i \in A_i\}.$$

L'operazione "*opposta*" è effettuata dal **proiettore** i-esimo: esso è una funzione che estrae l'i-esimo elemento di un tupla, ovvero è una funzione $\pi_i : A_1 \times ... \times A_n \longrightarrow A_i$ tale che

$$\pi_i(a_1, ..., a_n) = a_i$$

Per comodità chiameremo $\underbrace{A \times ... \times A}_{n} = A^n$

2.1.4. Insieme di funzioni

L'insieme di tutte le funzioni da A in B si indica con

$$B^A = \{f : A \longrightarrow B\}.$$

Viene utilizzata questa notazione in quanto la cardinalità di B^A è esattamente $|B|^{|A|}$, se A e B sono insiemi finiti.

In questo insieme sono presenti anche tutte le funzioni parziali da A in B: mettiamo in evidenza questa proprietà, scrivendo

$$B_\perp^A = \{f : A \to B_\perp\}.$$

Sembrano due insiemi diversi ma sono la stessa cosa: nel secondo viene messo in evidenza il fatto che tutte le funzioni che sono presenti sono totali oppure parziali che sono state totalizzate.

2.1.5. Funzione di valutazione

Dati A, B e $B_\perp^A$ si definisce **funzione di valutazione** la funzione

$$\omega : B_\perp^A \times A \longrightarrow B$$

tale che

$$w(f, a) = f(a).$$

In poche parole, è una funzione che prende una funzione f e la valuta su un elemento a del dominio.

Abbiamo due possibili approcci:
- tengo fisso a e provo tutte le funzioni f: sto eseguendo un *benchmark*, quest'ultimo rappresentato da a;
- tengo fissa f e provo tutte le a del dominio: sto ottenendo il grafico di f.

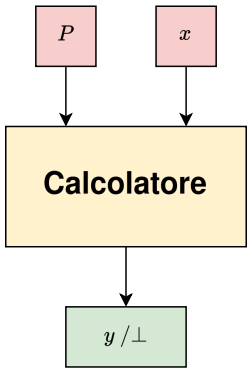
2.2. Teoria della calcolabilità

2.2.1. Sistema di calcolo

Quello che faremo ora è *modellare teoricamente un sistema di calcolo.*

Un **sistema di calcolo** lo possiamo vedere come una *black-box* che prende un programma P, una serie di dati x e calcola il risultato di P sull'input x.

La macchina ci restituisce:
- y se è riuscita a calcolare un risultato;
- $\perp$ se è entrata in un loop.



Un sistema di calcolo quindi è una funzione del tipo

$$\mathcal{C} : \text{PROG} \times \text{DATI} \longrightarrow \text{DATI}_\perp.$$

Come vediamo, è molto simile ad una funzione di valutazione: infatti, la parte dei dati x la riusciamo a "mappare" sull'input a del dominio, ma facciamo più fatica con l'insieme dei programmi, questo perché non abbiamo ancora definito cos'è un programma.

Un **programma** P è una **sequenza di regole** che trasformano un dato di input in uno di output (o in un loop): in poche parole, un programma è una funzione del tipo

$$P : \mathrm{DATI} \longrightarrow \mathrm{DATI}_\perp,$$

ovvero una funzione che appartiene all'insieme $\mathrm{DATI}_\perp^{\mathrm{DATI}}$.

Con questa definizione riusciamo a "mappare" l'insieme PROG sull'insieme delle funzioni che ci serviva per definire la funzione di valutazione.

Formalmente, un sistema di calcolo è quindi la funzione

$$\mathcal{C} : \mathrm{DATI}_\perp^{\mathrm{DATI}} \times \mathrm{DATI} \longrightarrow \mathrm{DATI}.$$

Con $\mathcal{C}(P, x)$ indichiamo la funzione calcolata da P su x, ovvero la sua **semantica**, il suo *significato*.

Il modello classico che viene considerato quando si parla di calcolatori è quello di **Von Neumann**.

2.2.2. Potenza computazionale

Prima di definire la potenza computazionale facciamo una breve premessa: indichiamo con

$$\mathcal{C}(P, \_) : \mathrm{DATI} \longrightarrow \mathrm{DATI}_\perp$$

la funzione che viene calcolata dal programma P, ovvero la semantica di P.

Fatta questa premessa, definiamo la **potenza computazionale** di un calcolatore come l'insieme di tutte le funzioni che quel sistema di calcolo può calcolare grazie ai programmi, ovvero

$$F(\mathcal{C}) = \{\mathcal{C}(P, \_) \mid P \in \mathrm{PROG}\} \subseteq \mathrm{DATI}_\perp^{\mathrm{DATI}}.$$

In poche parole, $F(\mathcal{C})$ rappresenta l'insieme di tutte le possibili semantiche di funzioni che sono calcolabili con il sistema $\mathcal{C}$.

Stabilire *cosa può fare l'informatica* equivale a studiare quest'ultima inclusione: in particolare, se
- $F(\mathcal{C}) \subsetneq \mathrm{DATI}_\perp^{\mathrm{DATI}}$ allora esistono compiti **non automatizzabili**;
- $F(\mathcal{C}) = \mathrm{DATI}_\perp^{\mathrm{DATI}}$ allora l'informatica può fare tutto.

Se ci trovassimo nella prima situazione dovremmo individuare una sorta di "recinto" per dividere le funzioni calcolabili da quelle che non lo sono.

Calcolare una funzione vuole dire *risolvere un problema*: ad ognuno di questi associo una **funzione soluzione**, che mi permette di risolvere in modo automatico il problema.

Grazie a questa definizione, calcolare le funzioni equivale a risolvere problemi.

In che modo possiamo risolvere l'inclusione?

Un primo approccio è quello della **cardinalità**: viene definita come una funzione che associa ad ogni insieme il numero di elementi che contiene.

Sembra un ottimo approccio, ma presenta alcuni problemi: infatti, funziona solo quando l'insieme è finito, mentre è molto fragile quando si parla di insiemi infiniti.

Ad esempio, gli insiemi
- $\mathbb{N}$ dei numeri naturali e
- $\mathbb{P}$ dei numeri naturali pari

sono tali che $\mathbb{P} \subsetneq \mathbb{N}$ ma hanno cardinalità $|\mathbb{N}| = |\mathbb{P}| = \infty$.

Dobbiamo dare una definizione diversa di cardinalità, visto che possono esistere "*infiniti più fitti/densi di altri*", come abbiamo visto nell'esempio precedente.

3. Lezione 03

3.1. Relazioni di equivalenza

3.1.1. Definizione

Una **relazione binaria** R su due insiemi A, B è un sottoinsieme $R \subseteq A \times B$ di coppie ordinate. Una relazione particolare che ci interessa è $R \subseteq A^2$. Due elementi $a, b \in A$ sono in relazione R se e solo se $(a, b) \in R$. Indichiamo la relazione tra due elementi tramite notazione infissa aRb.

Una classe molto importante di relazioni è quella delle **relazioni di equivalenza**: una relazione $R \subseteq A^2$ è una relazione di equivalenza se e solo se R è RST, ovvero:

- **riflessiva**: $\forall a \in A \quad aRa$;
- **simmetrica**: $\forall a, b \in A \quad aRb \implies bRa$;
- **transitiva**: $\forall a, b, c \in A \quad aRb \land bRc \implies aRc$.

3.1.2. Partizione

Ad ogni relazione di equivalenza si può associare una **partizione**, ovvero un insieme di sottoinsiemi tali che:

- $\forall i \in \mathbb{N}^+ \quad A_i \neq \varnothing$;
- $\forall i, j \in \mathbb{N}^+ \quad i \neq j \implies A_i \cap A_j = \varnothing$;
- $\bigcup_{i \in \mathbb{N}^+} A_i = A$.

Diremo che R definita su A^2 *induce* una partizione $A_1, A_2, \ldots$ su A.

3.1.3. Classi di equivalenza e insieme quoziente

Dato un elemento $a \in A$, la sua **classe di equivalenza** è l'insieme

$$[a]_R = \{b \in A \mid aRb\},$$

ovvero tutti gli elementi che sono in relazione con a, chiamato anche *rappresentante della classe*.

Si può dimostrare che:

- non esistono classi di equivalenza vuote $\rightarrow$ garantito dalla riflessività;
- dati $a, b \in A$ allora $[a]_R \cap [b]_R = \varnothing$ oppure $[a]_R = [b]_R \rightarrow$ in altre parole, due elementi o sono in relazione o non lo sono;
- $\bigcup_{a \in A} [a]_R = A$.

Notiamo che, per definizione, l'insieme delle classi di equivalenza è una partizione indotta dalla relazione R sull'insieme A. Questa partizione è detta **insieme quoziente** di A rispetto a R ed è denotato con A/R.

3.2. Cardinalità

3.2.1. Isomorfismi

Due insiemi A e B sono **isomorfi** (*equinumerosi* o *insiemi che hanno la stessa cardinalità*) se esiste una biiezione tra essi. Formalmente scriviamo:

$$A \sim B.$$

Detto $\mathcal{U}$ l'insieme di tutti gli insiemi, la relazione $\sim$ è sottoinsieme di $\mathcal{U}^2$.

Dimostriamo che $\sim$ è una relazione di equivalenza:

- *riflessività*: $A \sim A$ se la biiezione è i_A;
- *simmetria*: $A \sim B \implies B \sim A$ se la biiezione è la funzione inversa;

- *transitività*: $A \sim B \land B \sim C \implies A \sim C$ se la biiezione è la composizione della funzione usata per $A \sim B$ con la funzione usata per $B \sim C$.

Dato che $\sim$ è una relazione di equivalenza, è possibile partizionare l'insieme $\mathcal{U}$. La partizione creata è formata da classi di equivalenza che contengono insiemi isomorfi, ossia con la stessa cardinalità.

Possiamo quindi definire la **cardinalità** come l'insieme quoziente di $\mathcal{U}$ rispetto alla relazione $\sim$.

Questo approccio permette di utilizzare la nozione di *cardinalità* anche con gli insiemi infiniti, dato che l'unica incognita da trovare è una funzione biettiva tra i due insiemi.

3.2.2. Cardinalità finita

La prima classe di cardinalità che vediamo è quella delle **cardinalità finite**. Prima di tutto definiamo la famiglia di insiemi:

$$J_n = \begin{cases} \varnothing & \text{se } n = 0 \\ \{1, ..., n\} & \text{se } n > 0 \end{cases}.$$

Un insieme A ha cardinalità finita se $A \sim J_n$ per qualche $n \in \mathbb{N}$. In tal caso possiamo scrivere $|A| = n$.

La classe di equivalenza $[J_n]_\sim$ riunisce tutti gli insiemi di $\mathcal{U}$ contenenti n elementi.

3.2.3. Cardinalità infinita

L'altra classe di cardinalità da studiare è quella delle **cardinalità infinite**, ovvero gli insiemi non in relazione con J_n.

3.2.3.1. Insiemi numerabili

I primi insiemi a cardinalità infinita sono gli **insiemi numerabili**. Un insieme A è numerabile se e solo se $A \sim \mathbb{N}$, ovvero $A \in [\mathbb{N}]_\sim$.

Gli insiemi numerabili sono "**listabili**", ovvero è possibile elencare *tutti* gli elementi dell'insieme A tramite una regola, in questo caso la funzione f biiezione tra $\mathbb{N}$ e A. Infatti, grazie alla funzione f, è possibile elencare gli elementi di A formando l'insieme:

$$A = \{f(0),\ f(1),\ ...\}.$$

Questo insieme è esaustivo, quindi elenca ogni elemento dell'insieme A senza perderne nessuno.

Gli insiemi numerabili più famosi sono:
- numeri pari $\mathbb{P}$ e numeri dispari $\mathbb{D}$;
- numeri interi $\mathbb{Z}$ generati con la biiezione $f(n) = (-1)^n \left(\frac{n + (n \bmod 2)}{2} \right)$;
- numeri razionali $\mathbb{Q}$.

Gli insiemi numerabili hanno cardinalità $\aleph_0$ (si legge *"aleph"*).

3.2.3.2. Insiemi non numerabili

Gli **insiemi non numerabili** sono insiemi a cardinalità infinita che non sono listabili come gli insiemi numerabili, ovvero sono "più fitti" di $\mathbb{N}$.

Il *non poter listare gli elementi* si traduce in *qualunque lista generata mancherebbe di qualche elemento*, di conseguenza non sarebbe una lista esaustiva di tutti gli elementi.

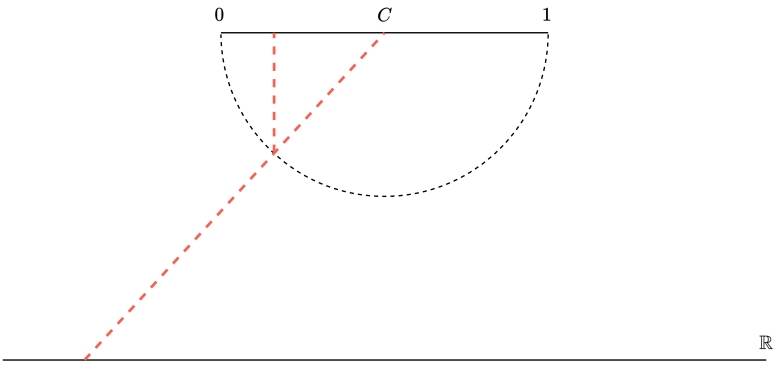
Il più famoso insieme non numerabile è l'insieme dei numeri reali $\mathbb{R}$.

Teorema L'insieme $\mathbb{R}$ non è numerabile

Dimostrazione
Suddividiamo la dimostrazione in tre punti:
1. dimostriamo che $\mathbb{R} \sim (0,1)$;
2. dimostriamo che $\mathbb{N} \nsim (0,1)$;
3. dimostriamo che $\mathbb{R} \nsim \mathbb{N}$.

[1] Partiamo con il dimostrare che $\mathbb{R} \sim (0,1)$: mostro che esiste una biiezione tra $\mathbb{R}$ e $(0,1)$. Usiamo una biiezione "grafica" costruita in questo modo:
- disegna la circonferenza di raggio $\frac{1}{2}$ centrata in $\frac{1}{2}$;
- disegna la perpendicolare al punto da mappare che interseca la circonferenza;
- disegna la retta passante per il centro C e l'intersezione precedente.

L'intersezione tra l'asse reale e la retta finale è il punto mappato.



In realtà, $\mathbb{R}$ è isomorfo a qualsiasi segmento di lunghezza maggiore di 0.

La stessa biiezione vale anche sull'intervallo chiuso $[0,1]$ utilizzando la "compattificazione" $\mathring{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$ di $\mathbb{R}$, mappando 0 su $-\infty$ e 1 su $+\infty$.

[2] Continuiamo dimostrando che $\mathbb{N} \nsim (0,1)$: devo dimostrare che l'intervallo $(0,1)$ non è listabile, ovvero ogni lista che scrivo è un "colabrodo", termine tecnico che indica la possibilità di costruire un elemento che dovrebbe appartenere alla lista ma che invece non è presente.
Per assurdo sia $\mathbb{N} \sim (0,1)$, allora posso listare gli elementi di $(0,1)$ esaustivamente come:

$$\begin{aligned} &0.\ a_{00}\ a_{01}\ a_{02}\ \dots \\ &0.\ a_{10}\ a_{11}\ a_{12}\ \dots \\ &0.\ a_{20}\ a_{21}\ a_{22}\ \dots \\ &0.\ \dots \quad , \end{aligned}$$

dove con a_{ij} indichiamo la cifra di posto j dell'i-esimo elemento della lista.

Costruisco il *"numero colpevole"* $c = 0.c_0c_1c_2\dots$ tale che

$$c_i = \begin{cases} 2 \text{ se } a_{ii} \neq 2 \\ 3 \text{ se } a_{ii} = 3 \end{cases} .$$

In poche parole, questo numero è costruito "guardando" tutte le cifre sulla diagonale.

Questo numero sicuramente appartiene a $(0,1)$ ma non appare nella lista: infatti ogni cifra c_i del colpevole differisce da qualunque numero nella lista in almeno una posizione, che è quella della diagonale. Ma questo è assurdo: avevamo assunto $(0,1)$ numerabile.

Quindi $N \nsim (0,1)$.

Questo tipo di dimostrazione è detta **dimostrazione per diagonalizzazione**.

[3] Terminiamo dimostrando che $\mathbb{R} \nsim \mathbb{N}$: per transitività. Vale il generico, ovvero non si riesce a listare nessun segmento di lunghezza maggiore di 0. □

L'insieme $\mathbb{R}$ viene detto **insieme continuo** e tutti gli insiemi isomorfi a $\mathbb{R}$ si dicono a loro volta *continui*. I più famosi insiemi continui sono:

- $\mathbb{R}$ insieme dei numeri reali;
- $\mathbb{C}$ insieme dei numeri complessi;
- $\mathbb{T} \subset \mathbb{I}$ insieme dei numeri trascendenti.

4. Lezione 04

4.1. Cardinalità

Vediamo due insiemi continui che saranno importanti successivamente.

4.1.1. Insieme delle parti

Il primo insieme che vediamo è l'**insieme delle parti**, o *power set*, di $\mathbb{N}$.

Quest'ultimo è l'insieme

$$P(\mathbb{N}) = 2^{\mathbb{N}} = \{S \mid S \text{ è sottoinsieme di } \mathbb{N}\}.$$

Teorema $P(\mathbb{N}) \nsim \mathbb{N}$.

Dimostrazione
Dimostriamo questo teorema con la diagonalizzazione.

Rappresentiamo il sottoinsieme $A \subseteq \mathbb{N}$ tramite il suo **vettore caratteristico**:

$$\begin{aligned} &\mathbb{N} : 0\ 1\ 2\ 3\ 4\ 5\ 6\ \ldots \\ &A : 0\ 1\ 1\ 0\ 1\ 1\ 0\ \ldots \quad . \end{aligned}$$

Il vettore caratteristico di un sottoinsieme è un vettore che nella posizione p_i ha 1 se $i \in A$, altrimenti ha 0.

Per assurdo sia $P(\mathbb{N})$ numerabile. Vista questa proprietà posso listare tutti i vettori caratteristici che appartengono a $P(\mathbb{N})$ come

$$\begin{aligned} b_0 &= b_{00}\ b_{01}\ b_{02}\ \ldots \\ b_1 &= b_{10}\ b_{11}\ b_{12}\ \ldots \\ b_2 &= b_{20}\ b_{21}\ b_{22}\ \ldots \quad . \end{aligned}$$

Costruiamo un *colpevole among us* che appartiene a $P(\mathbb{N})$ ma non è presente nella lista precedente. Definiamo il vettore

$$c = \overline{b_{00}}\ \overline{b_{11}}\ \overline{b_{22}}\ldots$$

che contiene nella posizione c_i il complemento di b_{ii}.

Questo vettore appartiene a $P(\mathbb{N})$ ma non è presente nella lista precedente perché è diverso da ogni elemento della lista in almeno una cifra.

Ma questo è assurdo perché $P(\mathbb{N})$ era numerabile, quindi $P(\mathbb{N}) \nsim \mathbb{N}$. □

Visto questo teorema possiamo affermare che:

$$P(\mathbb{N}) \sim [0,1] \sim \mathring{\mathbb{R}}.$$

4.1.2. Insieme delle funzioni

Il secondo insieme che vediamo è l'insieme delle funzioni da $\mathbb{N}$ in $\mathbb{N}$.

Quest'ultimo è l'insieme

$$\mathbb{N}_{\perp}^{\mathbb{N}} = \{f : \mathbb{N} \longrightarrow \mathbb{N}\}.$$

Teorema $\mathbb{N}_{\perp}^{\mathbb{N}} \nsim \mathbb{N}$.

Dimostrazione
Anche in questo caso useremo la dimostrazione per diagonalizzazione.

Per assurdo sia $\mathbb{N}_\perp^{\mathbb{N}}$ numerabile, quindi possiamo listare $\mathbb{N}_\perp^{\mathbb{N}}$ come $\{f_0, f_1, f_2, ...\}$.

	0	1	2	3	...	$\mathbb{N}$
f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$f_0(3)$	...	...
f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$f_1(3)$	...	...
f_2	$f_2(0)$	$f_2(1)$	$f_2(2)$	$f_2(3)$	...	...
f_3	$f_3(0)$	$f_3(1)$	$f_3(2)$	$f_3(3)$	...	...

Scriviamo un colpevole $\varphi : \mathbb{N} \longrightarrow \mathbb{N}_\perp$ per dimostrare l'assurdo. Una prima versione potrebbe essere la funzione $\varphi(n) = f_n(n) + 1$ per *disallineare* la diagonale, ma questo non va bene: infatti, se $f_n(n) = \perp$ non sappiamo dare un valore a $\varphi(n) = \perp + 1$.

Definiamo quindi la funzione

$$\varphi(n) = \begin{cases} 1 & \text{se } f_n(n) = \perp \\ f_n(n) + 1 & \text{se } f_n(n) \downarrow \end{cases}.$$

Questa funzione è una funzione che appartiene a $\mathbb{N}_\perp^{\mathbb{N}}$ ma non è presente nella lista precedente: infatti, $\forall k \in \mathbb{N}$ otteniamo

$$\varphi(k) = \begin{cases} 1 \neq f_k(k) = \perp & \text{se } f_k(k) = \perp \\ f_k(k) + 1 \neq f_k(k) & \text{se } f_k(k) \downarrow \end{cases}.$$

Ma questo è assurdo perché $P(\mathbb{N})$ era numerabile, quindi $P(\mathbb{N}) \nsim \mathbb{N}$. □

4.2. Potenza computazionale

4.2.1. Validità dell'inclusione $F(\mathcal{C}) \subseteq \text{DATI}_\perp^{\text{DATI}}$

Ora che abbiamo una definizione "potente" di cardinalità, essendo basata su strutture matematiche, possiamo verificare la validità dell'inclusione

$$F(\mathcal{C}) \subseteq \text{DATI}_\perp^{\text{DATI}}.$$

Diamo prima qualche considerazione:
- $\text{PROG} \sim \mathbb{N}$: identifico ogni programma con un numero, ad esempio la sua codifica in binario;
- $\text{DATI} \sim \mathbb{N}$: come prima, identifico ogni dato con la sua codifica in binario.

In poche parole, stiamo dicendo che programmi e dati non sono più dei numeri naturali $\mathbb{N}$.

Ma questo ci permette di dire che:

$$F(\mathcal{C}) \sim \text{PROG} \sim \mathbb{N} \nsim \mathbb{N}_\perp^{\mathbb{N}} \sim \text{DATI}_\perp^{\text{DATI}}.$$

Questo è un risultato importantissimo: abbiamo appena dimostrato con la relazione precedente che **esistono funzioni non calcolabili**. Le funzioni non calcolabili sono problemi pratici e molto sentiti

al giorno d'oggi: un esempio di funzione non calcolabile è la funzione che, dato un software, dice se è corretto o no. Il problema è che *ho pochi programmi e troppe/i funzioni/problemi*.

Questo risultato però è arrivato considerando vere le due considerazioni precedenti: andiamo quindi a dimostrarle utilizzando le **tecniche di aritmetizzazione** (o *godelizzazione*) **di strutture**, ovvero delle tecniche che rappresentano delle strutture con un numero, così da avere la matematica e l'insiemi degli strumenti che ha a disposizione.

5. Lezione 05

5.1. DATI $\sim \mathbb{N}$

Vogliamo formare una legge che:

1. associ biunivocamente dati a numeri e viceversa;
2. consenta di operare direttamente sui numeri per operare sui corrispondenti dati, ovvero abbia delle primitive per lavorare il numero che "riflettano" il risultato sul dato senza ripassare per il dato stesso;
3. ci consenta di dire, senza perdita di generalità, che i nostri programmi lavorano sui numeri.

5.1.1. Funzione coppia di Cantor

5.1.1.1. Definizione

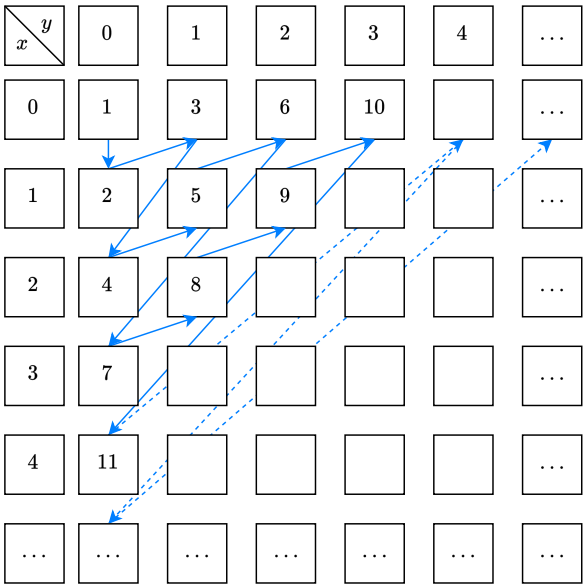
La **funzione coppia di Cantor** è la funzione

$$<,>: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}^+.$$

Questa funzione sfrutta due *"sotto-funzioni"*, *sin* e *des*, tali che

$$< x, y >= n,$$
$$\text{sin} : \mathbb{N}^+ \longrightarrow \mathbb{N}, \quad \text{sin } (n) = x$$
$$\text{des} : \mathbb{N}^+ \longrightarrow \mathbb{N}, \quad \text{des } (n) = y.$$

Vediamo una rappresentazione grafica della funzione di Cantor.



$< x, y >$ rappresenta il valore all'incrocio tra la x-esima riga e la y-esima colonna.

La tabella viene riempita *diagonale per diagonale*, ovvero:

1. sia $x = 0$;
2. partendo dalla cella $(x, 0)$ si enumerano le celle della diagonale identificata da $(x, 0)$ e da $(0, x)$;
3. si ripete il punto 2 aumentando x di 1.

Vorremmo che questa funzione sia iniettiva e suriettiva, quindi:

- non posso avere celle con lo stesso numero (*iniettiva*);
- ogni numero in $\mathbb{N}^+$ deve comparire.

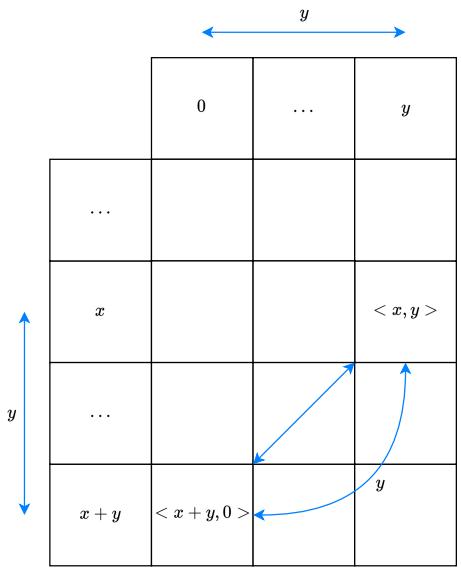
Questa richiesta è soddisfatta in quanto:

- numeriamo in maniera incrementale (*iniettiva*);
- ogni numero prima o poi compare in una cella, quindi ho una coppia che lo genera (*suriettiva*).

5.1.1.2. Forma analitica della funzione coppia

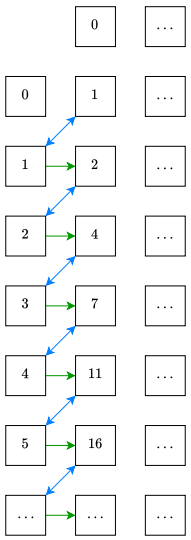
Quello che vogliamo fare ora è cercare una forma analitica della funzione coppia, questo perché non è molto comodo costruire ogni volta la tabella sopra. Nella successiva immagine notiamo come valga la relazione

$$< x, y >=< x + y, 0 > +y.$$



Questo è molto comodo perché il calcolo della funzione coppia si riduce al calcolo di $< x + y, 0 >$.

Chiamiamo $x + y = z$, osserviamo con la successiva immagine un'altra proprietà.



Ogni cella $< z, 0 >$ la si può calcolare come la somma di z e $< z - 1, 0 >$, ma allora

$$
\begin{aligned}
< z, 0 >= z + < z-1, 0 >= \\
&= z + (z-1) + < z-2, 0 >= \\
&= z + (z-1) + ... + 1 + < 0, 0 >= \\
&= z + (z-1) + ... + 1 + 1 = \\
&= \sum_{i=1}^{z} i + 1 = \frac{z(z+1)}{2} + 1.
\end{aligned}
$$

Questa forma è molto più compatta ed evita il calcolo di tutti i singoli $< z, 0 >$.

Mettiamo insieme le due proprietà per ottenere la formula analitica della funzione coppia:

$$
< x, y >=< x + y, 0 > + y = \frac{(x+y)(x+y+1)}{2} + y + 1.
$$

5.1.1.3. Forma analitica di sin e des

Vogliamo adesso dare la forma analitica di *sin* e *des* per poter computare l'inversa della funzione di Cantor, dato n.

Grazie alle osservazioni precedenti sappiamo che

$$
\begin{aligned}
n = y + < \gamma, 0 > \implies y = n - < \gamma, 0 >, \\
\gamma = x + y \implies x = \gamma - y.
\end{aligned}
$$

Se troviamo il valore di gamma abbiamo trovato anche i valori di x e y.

Notiamo come γ sia il *"punto di attacco"* della diagonale che contiene n, ma allora

$$
\gamma = \max\{z \in \mathbb{N} \mid < z, 0 >\leq n\}
$$

perché tra tutti i punti di attacco $< z, 0 >$ voglio quello che potrebbe contenere n e che sia massimo, ovvero sia esattamente la diagonale che contiene n.

Risolviamo quindi la disequazione

$$
\begin{aligned}
< z, 0 >\leq n &\implies \frac{z(z+1)}{2} + 1 \leq n \\
&\implies z^2 + z - 2n + 2 \leq 0 \\
&\implies z_{1,2} = \frac{-1 \pm \sqrt{1 + 8n - 8}}{2} \\
&\implies \frac{-1 - \sqrt{8n-7}}{2} \leq z \leq \frac{-1 + \sqrt{8n-7}}{2}.
\end{aligned}
$$

Come valore di γ scelgo

$$
\gamma = \left\lfloor \frac{-1 + \sqrt{8n-7}}{2} \right\rfloor.
$$

Ora che abbiamo γ possiamo definire le funzioni *sin* e *des* come

$$
\begin{aligned}
\text{des}\ (n) = y = n - < \gamma, 0 >= n - \frac{\gamma(\gamma+1)}{2} - 1, \\
\text{sin}\ (n) = x = \gamma - y.
\end{aligned}
$$

5.1.1.4. $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$

Con la funzione coppia di Cantor possiamo dimostrare un importante risultato.

Teorema $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}^+$.

Dimostrazione
La funzione di Cantor è una funzione biiettiva tra l'insieme $\mathbb{N} \times \mathbb{N}$ e l'insieme $\mathbb{N}^+$, quindi i due insiemi sono isomorfi. □

Estendiamo adesso il risultato all'interno insieme $\mathbb{N}$, ovvero

$$\mathbb{N} \times \mathbb{N} \sim \mathbb{N}^+ \rightsquigarrow \mathbb{N} \times \mathbb{N} \sim \mathbb{N}.$$

Teorema $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

Dimostrazione
Definiamo la funzione

$$[,] : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

tale che

$$[x, y] =< x, y > -1.$$

Questa funzione è anch'essa biiettiva, quindi i due insiemi sono isomorfi. □

Grazie a questi risultati si può dimostrare che $\mathbb{Q} \sim \mathbb{N}$: infatti, i numeri razionali li possiamo rappresentare come coppie (num, den). In generale, tutte le tuple sono isomorfe a $\mathbb{N}$, iterando in qualche modo la funzione coppia di Cantor.

5.1.2. Dimostrazione

I risultati ottenuti fino a questo punto ci permettono di dire che ogni dato è trasformabile in un numero, che può essere soggetto a trasformazioni e manipolazioni matematiche.

La dimostrazione *formale* non verrà fatta, ma verranno fatti esempi di alcune strutture dati che possono essere trasformate in un numero tramite la funzione coppia di Cantor. Vedremo come ogni struttura dati verrà manipolata e trasformata in una coppia (x, y) per poterla applicare alla funzione coppia.

5.1.2.1. Strutture dati

5.1.2.1.1. Liste

Le **liste** sono le strutture dati più utilizzate nei programmi. In generale non ne è nota la grandezza, di conseguenza dobbiamo trovare un modo, soprattutto durante la applicazione di *sin* e *des*, per capire quando abbiamo esaurito gli elementi della lista.

Codifichiamo la lista $[x_1, ..., x_n]$ con

$$< x_1, ..., x_n >=< x_1, < x_2, < ... < x_n, 0 > ... \ggg .$$

Abbiamo quindi applicato la funzione coppia di Cantor alla coppia formata da un elemento della lista e il risultato della funzione coppia stessa applicata ai successivi elementi.

Ad esempio, la codifica della lista $M = [1, 2, 5]$ risulta essere:

$$
\begin{aligned}
< 1, 2, 5 > &= < 1, < 2, < 5, 0 \gg \gg \\
&= < 1, < 2, 16 \gg \\
&= < 1, 188 > \\
&= 18144.
\end{aligned}
$$

Per decodificare la lista M applichiamo le funzioni *sin* e *des* al risultato precedente. Alla prima iterazione otterremo il primo elemento della lista e la restante parte ancora da decodificare.

Quando ci fermiamo? Durante la creazione della codifica di M abbiamo inserito un *"tappo"*, ovvero la prima iterazione della funzione coppia $< x_n, 0 >$. Questo ci indica che quando des (M) sarà uguale a 0 ci dovremo fermare.

Cosa succede se abbiamo uno 0 nella lista? Non ci sono problemi: il controllo avviene sulla funzione *des*, che restituisce la *"somma parziale"* e non sulla funzione *sin*, che restituisce i valori della lista.

Possiamo anche anche delle implementazioni di queste funzioni. Assumiamo che:
- 0 codifichi la lista nulla;
- esistano delle routine per $<, >$, sin e des.

Codifica

```
def encode(numbers: list[int]) -> int:
  k = 0
  for i in range(n,0,-1):
    xi = numbers[i]
    k = <xi,k>
  return k
```

Decodifica

```
def decode(n: int) -> list[int]:
  numbers = []
  while True:
    left, n = sin(n), des(n)
    numbers.append(left)
    if n == 0:
      break
  return numbers
```

Un metodo molto utile delle liste è quello che ritorna la sua **lunghezza**.

Lunghezza

```
def length(n: int) -> int:
  return 0 if n == 0 else 1 + length(des(n))
```

Infine, definiamo la funzione **proiezione** come:

$$
\text{proj}(t, n) = \begin{cases} -1 & \text{se } t > \text{length}(n) \vee t \leq 0 \\ x_t & \text{altrimenti} \end{cases}
$$

e la sua implementazione:

Proiezione

```
def proj(t: int, n: int) -> int:
  if t <= 0 or t > length(n):
    return -1
  else:
    if t == 1:
      return sin(n)
    else:
      return proj(t - 1, des(n))
```

5.1.2.1.2. Array

Per gli **array** il discorso è più semplice, in quanto la dimensione è nota a priori. Di conseguenza, non necessitiamo di un carattere di fine sequenza. Dunque avremo che l'array $\{x_1, ..., x_n\}$ viene codificato con:

$$[x_1, ..., x_n] = [x_1, ...[x_{n-1}, x_n]...].$$

5.1.2.1.3. Matrici

Per quanto riguarda **matrici** l'approccio utilizzato codifica singolarmente le righe e successivamente codifica i risultati ottenuti come se fossero un array di dimensione uguale al numero di righe.

Ad esempio, la matrice

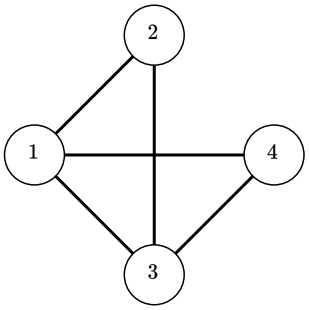
$$\begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix}$$

viene codificata in:

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix} = [[x_{11}, x_{12}, x_{13}], [x_{21}, x_{22}, x_{23}], [x_{31}, x_{32}, x_{33}]].$$

5.1.2.1.4. Grafi

Consideriamo il seguente grafo.



I **grafi** sono rappresentati principalmente in due modi:

- **liste di adiacenza dei vertici**: per ogni vertice si ha una lista che contiene gli identificatori dei vertici che collegati direttamente con esso. Il grafo precedente ha

  $$\{1 : [2, 3, 4], 2 : [1, 3], 3 : [1, 2, 4], 4 : [1, 3]\}$$

  come lista di adiacenza, e la sua codifica si calcola come:

  $$[< 2, 3, 4 >, < 1, 2 >, < 1, 2, 4 >, < 1, 3 >].$$

  Questa soluzione esegue prima la codifica di ogni lista di adiacenza e poi la codifica dei risultati del passo precedente.
- **matrice di adiacenza**: per ogni cella m_{ij} della matrice $|V| \times |V|$, dove V è l'insieme dei vertici, si ha:
  - 1 se esiste un arco dal vertice i al vertice j;
  - 0 altrimenti;

  Essendo questa una matrice la andiamo a codificare come abbiamo già descritto.

5.1.2.2. Applicazioni

Una volta visto come rappresentare le principali strutture dati, è facile trovare delle vie per codificare qualsiasi tipo di dato in un numero. Vediamo alcuni esempi.

5.1.2.2.1. Testi

Dato un **testo**, possiamo ottenere la sua codifica nel seguente modo:

1. trasformiamo il testo in una lista di numeri tramite la codifica ASCII dei singoli caratteri;
2. sfruttiamo l'idea dietro la codifica delle liste per codificare quanto ottenuto.

Per esempio,

$$\text{ciao} = [99, 105, 97, 111] =< 99, < 105, < 97, < 111, 0 \ggg .$$

Possiamo chiederci:

- *Il codificatore proposto è un buon compressore?*
  No, si vede facilmente che il numero ottenuto tramite la funzione coppia (o la sua concatenazione) sia generalmente molto grande, e che i bit necessari a rappresentarlo crescano esponenzialmente sulla lunghezza dell'input. Ne segue che questo è un *pessimo* modo per comprimere messaggi.
- *Il codificatore proposto è un buon sistema crittografico?*
  La natura stessa del processo garantisce la possibilità di trovare un modo per decifrare in modo analitico, di conseguenza chiunque potrebbe, in poco tempo, decifrare il mio messaggio. Inoltre, questo metodo è molto sensibile agli errori.

5.1.2.2.2. Suoni

Dato un **suono**, possiamo *campionare* il suo segnale elettrico a intervalli di tempo regolari e codificare la sequenza dei valori campionati tramite liste o array.

5.1.2.2.3. Immagini

Per codificare le **immagini** esistono diverse tecniche, ma la più usata è la **bitmap**: ogni pixel contiene la codifica numerica di un colore, quindi posso codificare separatamente ogni pixel e poi codificare i singoli risultati insieme tramite liste o array.

5.1.3. Conclusioni

Abbiamo mostrato come i dati possano essere *"buttati via"* in favore delle codifiche numeriche associate ad essi.

Di conseguenza, possiamo sostituire tutte le funzioni $f : \text{DATI} \longrightarrow \text{DATI}_\perp$ con delle funzioni $f' : \mathbb{N} \to \mathbb{N}_\perp$. In altre parole, l'universo dei problemi per i quali cerchiamo una soluzione automatica è rappresentabile dall'insieme $\mathbb{N}_\perp^\mathbb{N}$.

6. Lezione 06

6.1. $\text{PROG} \sim \mathbb{N}$

La relazione interviene nella parte che afferma che

$$F(\mathcal{C}) \sim \text{PROG} \sim \mathbb{N}.$$

In poche parole, la potenza computazionale, cioè l'insieme dei programmi che $\mathcal{C}$ riesce a calcolare, è isomorfa all'insieme di tutti i programmi, a loro volta isomorfi a $\mathbb{N}$.

Per dimostrare l'ultima parte di questa catena di relazione dobbiamo esibire una legge che mi permetta di ricavare un numero dato un programma e viceversa.

Per fare questo vediamo l'insieme PROG come l'insieme dei programmi scritti in un certo linguaggio di programmazione. Analizzeremo due sistemi diversi:
- Sistemi di calcolo RAM;
- Sistemi di calcolo while.

In generale, ogni sistema di calcolo ha la propria macchina e il proprio linguaggio.

6.1.1. Sistema di calcolo RAM

6.1.1.1. Introduzione

Questo sistema è molto semplice e ci permette di definire rigorosamente:
- $\text{PROG} \sim \mathbb{N}$;
- la **semantica dei programmi eseguibili**, ovvero calcolo $\mathcal{C}(P, \_)$ con $\mathcal{C} = \text{RAM}$ ottenendo $\text{RAM}(P, \_)$;
- la **potenza computazionale**, ovvero calcolo $F(\mathcal{C})$ con $\mathcal{C} = \text{RAM}$ ottenendo $F(\text{RAM})$.

Il linguaggio utilizzato è un assembly molto semplificato, immediato e semplice.

Dopo aver definito $F(\text{RAM})$ potremmo chiederci se questa definizione sia troppo stringente e riduttiva per definire tutti i sistemi di calcolo. In futuro introdurremo delle macchine più sofisticate, dette **macchine while**, che, a differenza delle macchine RAM, sono *strutturate*. Infine, confronteremo $F(\text{RAM})$ e $F(\text{WHILE})$. I due risultati possibili sono:
- le potenze computazionali sono *diverse*: ciò che è computazionale dipende dallo strumento, cioè dal linguaggio utilizzato;
- le potenze computazionali sono *uguali*: la computabilità è intrinseca dei problemi, non dello strumento.

Il secondo è il caso più promettente e, in quel caso, cercheremo di trovare una caratterizzazione teorica, ovvero di *"recintare"* tutti i problemi calcolabili.

6.1.1.2. Macchina RAM

Una macchina RAM è una macchina formata da un processore e da una memoria *potenzialmente infinita* divisa in **celle/registri**, contenenti dei numeri naturali (i nostri dati aritmetizzati).

Indichiamo i registri con R_k, con $k \geq 0$. Tra questi ci sono due registri particolari:
- R_0 contiene l'*output*;
- R_1 contiene l'*input*.

Un altro registro molto importante, che non rientra nei registri R_k, è il registro L, detto anche **program counter** (*PC*). Questo registro è essenziale in questa architettura, in quanto indica l'indirizzo della prossima istruzione da eseguire.

Dato un programma P, indichiamo con $|P|$ il numero di istruzioni che il programma contiene.

Le istruzioni nel linguaggio RAM sono:
- **incremento**: $R_k \longleftarrow R_k + 1$;
- **decremento**: $R_k \longleftarrow R_k \dot{-} 1$;
- **salto condizionato**: IF $R_k = 0$ THEN GOTO m, con $m \in \{1, ..., |P|\}$.

L'istruzione di decremento é tale che

$$x \dot{-} y = \begin{cases} x - y & \text{se } x \geq y \\ 0 & \text{altrimenti} \end{cases} .$$

6.1.1.3. Fasi dell'esecuzione

L'esecuzione di un programma su una macchina RAM segue i seguenti passi:
1. **Inizializzazione**:
   1. viene caricato il programma $P \equiv \text{Istr}_1, ..., \text{Istr}_n$ in memoria;
   2. il PC viene posto a 1 per indicare di eseguire la prima istruzione del programma;
   3. nel registro R_1 viene caricato l'input;
   4. ogni altro registro è azzerato.
2. **Esecuzione**: si eseguono tutte le istruzioni *una dopo l'altra*, ovvero ad ogni iterazione passo da L a $L + 1$, a meno di istruzioni di salto. Essendo il linguaggio RAM *non strutturato* il PC è necessario per indicare ogni volta l'istruzione da eseguire al passo successivo. Un linguaggio strutturato, invece, sa sempre quale istruzione eseguire dopo quella corrente, infatti non è dotato di PC;
3. **Terminazione**: per convenzione si mette $L = 0$ per indicare che l'esecuzione del programma è finita oppure è andata in loop. Questo segnale, nel caso il programma termini, è detto **segnale di halt** e arresta la macchina;
4. **Output**: il contenuto di R_0, se vado in halt, contiene il risultato dell'esecuzione del programma P. Indichiamo con $\varphi_P(n)$ il contenuto del registro R_0 (in caso di halt) oppure $\perp$ (in caso di loop).

$$\varphi_P(n) = \begin{cases} \text{contenuto}(R_0) & \text{se halt} \\ \perp & \text{se loop} \end{cases} .$$

Con $\varphi_P : \mathbb{N} \longrightarrow \mathbb{N}_\perp$ indichiamo la **semantica** del programma P.

Come indicavamo con $\mathcal{C}(P, \_)$ la semantica del programma P nel sistema di calcolo $\mathcal{C}$, indichiamo con $\text{RAM}(P, \_) = \varphi_P$ la semantica del programma P nel sistema di calcolo RAM.

6.1.1.4. Definizione formale semantica

Vogliamo dare una definizione formale della semantica di un programma RAM. Quello che faremo sarà dare una **semantica operazionale** alle istruzioni RAM, ovvero specificare il significato di ogni istruzione esplicitando l'**effetto** che quell'istruzione ha sui registri della macchina.

Per descrivere l'effetto di un'istruzione ci serviamo di una *foto*. L'idea che ci sta dietro è:
1. faccio una foto della macchina *prima* dell'esecuzione dell'istruzione;
2. eseguo l'istruzione;
3. faccio una foto della macchina *dopo* l'esecuzione dell'istruzione.

La foto della macchina si chiama **stato** e deve descrivere completamente la situazione della macchina in un certo istante. La coppia $(\text{StatoPrima}, \text{StatoDopo})$ rappresenta la semantica operazionale di una data istruzione del linguaggio RAM.

L'unica informazione da salvare dentro una foto è la situazione globale dei registri R_k e il registro L. Il programma non serve, visto che rimane sempre uguale.

La **computazione** del programma P è una sequenza di stati S_i, ognuno generato dall'esecuzione di un'istruzione del programma. Diciamo che P induce una sequenza di stati S_i. Se quest'ultima è formata da un numero infinito di stati, allora il programma è andato in loop. In caso contrario, nel registro R_0 si trova il risultato y della computazione di P. In poche parole:

$$\varphi_P : \mathbb{N} \longrightarrow \mathbb{N}_\perp \text{ tale che } \varphi_P(n) = \begin{cases} y & \text{se } \exists S_{\text{finale}} \\ \perp & \text{altrimenti} \end{cases} .$$

Definiamo ora come passiamo da uno stato all'altro. Per far ciò, definiamo:

- **stato**: istantanea di tutte le componenti della macchina, è una funzione

  $$S : \{L, R_i\} \longrightarrow \mathbb{N}$$

  tale che $S(R_k)$ restituisce il contenuto del registro R_k quando la macchina si trova nello stato S. Gli stati possibili di una macchina appartengono all'insieme

  $$\text{STATI} = \{f : \{L, R_i\} \longrightarrow \mathbb{N}\} = \mathbb{N}^{\{L, R_i\}}.$$

  Questa rappresentazione è molto comoda perché ho potenzialmente un numero di registri infinito. Se così non fosse avrei delle tuple per indicare tutti i possibili registri al posto dell'insieme $\{L, R_i\}$;
- **stato finale**: uno stato finale è un qualsiasi stato S tale che $S(L) = 0$;
- **dati**: abbiamo già dimostrato come $\text{DATI} \sim \mathbb{N}$;
- **inizializzazione**: serve una funzione che, preso l'input, ci dia lo stato iniziale della macchina. La funzione è

  $$\text{in} : \mathbb{N} \longrightarrow \text{STATI} \text{ tale che } \text{in}(n) = S_{\text{iniziale}}.$$

  Lo stato S_{iniziale} è tale che

  $$S_{\text{iniziale}}(R) = \begin{cases} 1 & \text{se } R = L \\ n & \text{se } R = R_1 \\ 0 & \text{altrimenti} \end{cases} ;$$
- **programmi**: definisco PROG come l'insieme dei programmi RAM.

Ci manca da definire la *parte dinamica* del programma, ovvero l'**esecuzione**. Definiamo la **funzione di stato prossimo**

$$\delta : \text{STATI} \times \text{PROG} \longrightarrow \text{STATI}_\perp$$

tale che

$$\delta(S, P) = S',$$

dove S rappresenta lo stato attuale e S' rappresenta lo stato prossimo dopo l'esecuzione di un'istruzione di P.

La funzione $\delta(S, P) = S'$ è tale che:

- se $S(L) = 0$ ho halt, ovvero deve terminare la computazione. Poniamo lo stato come indefinito, quindi $S' = \perp$;
- se $S(L) > |P|$ vuol dire che P non contiene istruzioni che bloccano esplicitamente l'esecuzione del programma. Lo stato S' è tale che:

  $$S'(R) = \begin{cases} 0 & \text{se } R = L \\ S(R_i) & \text{se } R = R_i \ \forall i \end{cases} ;$$
- se $1 \leq S(L) \leq |P|$ considero l'istruzione $S(L)$-esima:

- se ho incremento/decremento sul registro R_k definisco S' tale che

$$\begin{cases} S'(L) = S(L) + 1 \\ S'(R_k) = S(R_k) \pm 1 \\ S'(R_i) = S(R_i) \text{ per } i \neq k \end{cases};$$

- se ho il GOTO sul registro R_k che salta all'indirizzo m definisco S' tale che

$$S'(L) = \begin{cases} m & \text{se } S(R_k) = 0 \\ S(L) + 1 & \text{altrimenti} \end{cases},$$
$$S'(R_i) = S(R_i) \quad \forall i.$$

L'esecuzione di un programma $P \in \text{PROG}$ su input $n \in \mathbb{N}$ genera una sequenza di stati

$$S_0, S_1, ..., S_i, S_{i+1}, ...$$

tali che

$$S_0 = \text{in}(n)$$
$$\forall i \quad S_{i+1} = \delta(S_i, P).$$

La sequenza è infinita quando P va in loop, mentre se termina raggiunge uno stato S_m tale che $S_m(L) = 0$, ovvero ha ricevuto il segnale di halt.

La semantica di P è

$$\varphi_P(n) = \begin{cases} y & \text{se } P \text{ termina in } S_m, \text{ con } S_m(L) = 0 \text{ e } S_m(R_0) = y \\ \perp & \text{se } P \text{ va in loop} \end{cases}.$$

La potenza computazionale del sistema RAM è:

$$F(\text{RAM}) = \left\{ f \in \mathbb{N}_\perp^\mathbb{N} \mid \exists P \in \text{PROG} \mid \varphi_P = f \right\} = \{ \varphi_P \mid P \in \text{PROG} \} \subsetneq \mathbb{N}_\perp^\mathbb{N}.$$

L'insieme è formato da tutte le funzioni $f : \mathbb{N} \longrightarrow \mathbb{N}_\perp$ che hanno un programma che le calcola in un sistema RAM.

7. Lezione 07

8. Lezione 08

8.1. Semantica di un programma while

L'esecuzione di un programma while W passa per i seguenti step:

1. **inizializzazione**: ogni registro x_i viene posto a 0 tranne x_1, che contiene l'input n;
2. **esecuzione**: essendo WHILE un linguaggio con strutture di controllo, non serve un program counter perché le istruzioni di W vengono eseguite una dopo l'altra ;
3. **terminazione**: l'esecuzione di W può:
   - arrestarsi se sono arrivato al termine delle istruzioni;
   - entrare in loop;
4. **output**: se il programma va in halt l'output è contenuto nel registro x_0, ovvero

$$\Psi_W(n) = \begin{cases} \text{contenuto}(x_0) & \text{se halt} \\ \bot & \text{se loop} \end{cases}.$$

La funzione $\Psi_W : \mathbb{N} \longrightarrow \mathbb{N}_\bot$ è la semantica del programma W.

Diamo ora la *definizione formale* della semantica di un programma while. Come per i programmi RAM abbiamo bisogno di una serie di ingredienti:

1. **stato**: avendo un numero finito di variabili usiamo una tupla grande quanto il numero di quest'ultime, quindi $\underline{x} = (c_0, ..., c_{20})$ rappresenta il nostro stato, con c_i contenuto della variabile i;
2. $\boldsymbol{W}$**-STATI**: insieme di tutti gli stati possibili, lo indichiamo con $\mathbb{N}^{21}$;
3. **dati**: già dimostrato che $\text{DATI} \sim \mathbb{N}$;
4. **inizializzazione**: usiamo la funzione

$$\text{w-in}(n) = (0, n, 0, ..., 0);$$

5. **semantica operazionale**: dobbiamo trovare una funzione che, presi il comando da eseguire e lo stato corrente, restituisce lo stato prossimo.

Soffermiamoci sull'ultimo punto: definiamo la funzione

$$[\![]\!]() : \text{W-COM} \times W\text{-STATI} \longrightarrow W\text{-STATI}_\bot$$

che, dati un comando del linguaggio while C e lo stato corrente $\underline{x}$, calcola

$$[\![C]\!](\underline{x}) = \underline{y},$$

con $\underline{y}$ stato prossimo. Quest'ultimo dipende dal comando C, ma essendo C induttivo, proviamo a dare una definizione induttiva della funzione $[\![]\!]()$.

Partiamo dal passo base, quindi dagli **assegnamenti**:

$$[\![x_k := 0]\!](\underline{x}) = \underline{y} = \begin{cases} x_i & \text{se } i \neq k \\ 0 & \text{se } i = k \end{cases},$$

$$[\![x_k := x_j \pm 1]\!](\underline{x}) = \underline{y} = \begin{cases} x_i & \text{se } i \neq k \\ x_j \pm 1 & \text{se } i = k \end{cases}.$$

Vediamo invece i passi induttivi, quindi:

- *comando composto*: vogliamo calcolare

$$[\![\text{begin } C_1; ...; C_m \text{ end}]\!](\underline{x})$$

  conoscendo ogni $[\![C_i]\!]$ per ipotesi induttiva. Calcoliamo allora la funzione:

$$[\![C_m]\!](...([\![C_2]\!]([\![C_1]\!](\underline{x})))...) = ([\![C_m]\!] \circ ... \circ [\![C_1]\!])(\underline{x}),$$

ovvero applichiamo in ordine i comandi C_i presenti nel comando composto C.

- *comando while*: vogliamo calcolare

$$[\![\text{while } x_k \neq 0 \text{ do } C]\!](\underline{x})$$

conoscendo ogni $[\![C_i]\!]$ per ipotesi induttiva. Calcoliamo allora la funzione:

$$[\![C]\!](...([\![C]\!](\underline{x}))...).$$

Dobbiamo capire quante volte eseguiamo il loop, ovvero data $[\![C]\!]^e$ esecuzione del loop vorremmo sapere il valore di e. Questo numero deve essere uguale al minimo numero di iterazioni che mi portano in $x_k = 0$, ovvero il mio comando while diventa:

$$\text{while } x_k \neq 0 \text{ do } C = \begin{cases} [\![C]\!]^e(\underline{x}) & \text{se } e = \mu_t \\ \perp & \text{altrimenti} \end{cases}.$$

Il valore $e = \mu_t$ è quel numero tale che $[\![C]\!]^e(\underline{x})$ ha la k-esima componente dello stato uguale a 0.

Abbiamo quasi finito: manca solo da definire cos'è la **semantica** del programma W su input n. Quest'ultima è la funzione

$$\Psi_W : \mathbb{N} \longrightarrow \mathbb{N}_\perp \quad | \quad \text{Pro}(0, [\![W]\!](\text{w-in}(n))).$$

Possiamo affermare questo perché W, essendo un programma while, è un programma composto, e noi abbiamo definito come deve comportarsi la funzione $[\![]\!]()$ sui comandi composti.

La **potenza computazionale** del sistema di calcolo while è l'insieme

$$F(\text{WHILE}) = \left\{ f \in \mathbb{N}_\perp^{\mathbb{N}} \mid \exists W \in W\text{-PROG} \mid f = \Psi_W \right\} = \{\Phi_W : W \in W\text{-PROG}\},$$

ovvero l'insieme formato da tutte le funzioni che possono essere calcolate con un programma in W-PROG.

8.2. $F(\text{WHILE})$ VS $F(\text{RAM})$

Che relazione esiste tra $F(\text{WHILE})$ e $F(\text{RAM})$?

Abbiamo quattro possibili situazioni:

- $F(\text{RAM}) \subsetneq F(\text{WHILE})$ sarebbe comprensibile vista l'estrema semplicità del sistema RAM;
- $F(\text{RAM}) \cap F(\text{WHILE})$, che sia vuota (*insiemi disgiunti*) o abbia elementi (*insiemi sghembi*), sarebbe preoccupante perché il concetto di calcolabile dipenderebbe dalla macchina che si sta utilizzando;
- $F(\text{WHILE}) \subseteq F(\text{RAM})$ sarebbe sorprendente perché il sistema while sembra più sofisticato del sistema RAM ma la relazione decreterebbe che il sistema while non è più potente del sistema ram;
- $F(\text{WHILE}) = F(\text{RAM})$ sarebbe un risultato ottimo perché così facendo il concetto di *calcolabile* non dipende dalla tecnologia utilizzata, ma è intrinseco nei problemi.

Poniamo di avere C_1 e C_2 sistemi di calcolo con insiemi di programmi C_1-PROG e C_2-PROG e potenze computazionali

$$F(C_1) = \left\{ f : \mathbb{N} \longrightarrow \mathbb{N}_\perp \mid f = \Psi_{P_1} \text{ per qualche } P_1 \in C_1\text{-PROG} \right\} = \left\{ \Psi_{P_1} : P_1 \in C_1\text{-PROG} \right\}$$

e

$$F(C_2) = \left\{ f : \mathbb{N} \longrightarrow \mathbb{N}_\perp \mid f = \Psi_{P_2} \text{ per qualche } P_2 \in C_2\text{-PROG} \right\} = \left\{ \Psi_{P_2} : P_2 \in C_2\text{-PROG} \right\}.$$

Come mostro che $F(C_1) \subseteq F(C_2)$, ovvero che il primo sistema di calcolo non è più potente del secondo? Devo dimostrare che ogni elemento nel primo insieme deve stare nel secondo, ovvero

$$\forall f \in F(C_1) \Longrightarrow f \in F(C_2).$$

Se *espandiamo* la definizione di $f \in F(C)$ allora la relazione diventa:

$$\exists P_1 \in C_1\text{-PROG} \mid f = \Psi_{P_1} \Longrightarrow \exists P_2 \in C_2\text{-PROG} \mid f = \Psi_{P_2}.$$

In poche parole, per ogni programma calcolabile nel primo sistema di calcolo ne esiste uno con la stessa semantica nel secondo sistema di calcolo. Quello che vogliamo trovare è **compilatore**, ovvero una funzione che trasformi un programma del primo sistema in un programma del secondo sistema. Useremo il termine **traduttore** al posto di *compilatore*.

8.3. Traduzioni

Dati C_1 e C_2 due sistemi di calcolo, una **traduzione** da C_1 a C_2 è una funzione

$$T : C_1\text{-PROG} \longrightarrow C_2\text{-PROG}$$

con le seguenti proprietà:

- **programmabile**, ovvero esiste un modo per programmarla effettivamente;
- **completo**, ovvero sappia tradurre ogni programma in C_1-PROG in un programma in C_2-PROG;
- **corretto**, ovvero mantiene la semantica del programma di partenza, cioè

$$\forall P \in C_1\text{-PROG} \quad : \quad \Psi_P = \varphi_{T(P)},$$

  dove Ψ rappresenta la semantica dei programmi in C_1-PROG e φ rappresenta la semantica dei programmi in C_2-PROG.

Teorema Se esiste $T : C_1\text{-PROG} \longrightarrow C_2\text{-PROG}$ allora $F(C_1) \subseteq F(C_2)$.

Dimostrazione
Se $f \in F(C_1)$ allora esiste un programma $P_1 \in C_1$-PROG tale che $\Psi_{P_1} = f$.

A questo programma P_1 applico T, ottenendo $T(P_1) = P_2 \in C_2$-PROG (per *completezza*) tale che $\varphi_{P_2} = \Psi_{P_1} = f$ (per *correttezza*).

Ho trovato un programma $P_2 \in C_2$-PROG la cui semantica è f, allora $F(C_1) \subseteq F(C_2)$. □

Mostreremo che $F(\text{WHILE}) \subseteq F(\text{RAM})$, ovvero il sistema while non è più potente del sistema RAM. Quello che faremo sarà costruire un compilatore

$$\text{Comp} : W\text{-PROG} \longrightarrow \text{PROG}.$$