Informatica Teorica

Appunti della lezione
su tesi di Church-Turing e
problemi indecidibili

Tesi di Church-Turing

- Nel 1936, Church propone di assimilare il concetto informale di computabilità con il concetto rigoroso di ricorsività generale:

  f è computabile ⇔ f è RG (tesi di Church)
- Contemporaneamente Turing dimostra che la ricorsività generale e la T-computabilità coincidono:

  f è RG ⇔ f è T-computabile (teorema di Turing)
- Unendo i due risultati: tesi di Church-Turing

  f è computabile ⇔ f è T-computabile

Quella di Church-Turing è una tesi…

- …e non un teorema, perché non ha una dimostrazione rigorosa (la parte di Church è basata sul concetto non rigoroso di algoritmo)
- Numerosi tentativi di smentirla (trovare una funzione computabile ma che non sia computabile da una macchina di Turing) sono falliti perché alla fine le funzioni risultavano non computabili oppure T-computabili:
  - λ-ricorsività (Church)
  - μ-ricorsività (Kleene)
  - URM-computabilità (Shepherdson & Sturgis)

Problema dell'arresto

- Dato il codice di una MT e un input I, la computazione di MT su I termina in tempo finito?
- Questo problema non è decidibile, ossia non è risolvibile tramite una MT
- Lo dimostriamo per assurdo, supponendo che esista una macchina H che riesca, in tempo finito, a darci sempre una risposta (positiva o negativa)

La macchina H

- Sia C_{MT} la codifica del codice di una MT
- Si suppone che esista la seguente macchina:

$$H(C_{MT}, I) = \begin{cases} 0, \text{ se } MT(I) \text{ termina} \\ 1, \text{ se } MT(I) \text{ non termina} \end{cases}$$

- Sulla base della macchina H, costruiamo la macchina H'

La macchina H'

- Si costruisce la seguente macchina:

$$H'(C_{MT}) = \begin{cases} 0, \text{ se } MT(C_{MT}) \text{ termina, ossia } H(C_{MT}, C_{MT}) = 0 \\ 1, \text{ se } MT(C_{MT}) \text{ non termina, } H(C_{MT}, C_{MT}) = 1 \end{cases}$$

- La macchina H' computa una funzione che è un caso particolare della funzione computata da H (C_{MT} è un valore particolare di I)

La macchina Z

- Sulla base di H', si costruisce la seguente macchina:

$$Z(C_{MT}) = \begin{cases} \text{non termina, se } H'(C_{MT}) = 0 \\ 0, \text{ se } H'(C_{MT}) = 1 \end{cases}$$

- Per la non-terminazione basta aggiungere istruzioni che facciano sì che, se H' restituisce 0 in output, la testina di Z vada, ad esempio, a destra all'infinito

Il paradosso

- Proviamo a calcolare $Z(C_Z)$
  a) $Z(C_Z)$ non termina $\Leftrightarrow H'(C_{MT}) = 0 \Leftrightarrow Z(C_Z)$ termina
  b) $Z(C_Z) = 0 \Leftrightarrow H'(C_{MT}) = 1 \Leftrightarrow Z(C_Z)$ non termina
- In ogni caso, si arriva a un assurdo che ci costringe a respingere l'assunzione che la macchina H esista
- La macchina H non può esistere, ossia il problema dell'arresto non è decidibile

Enumerazione delle MT

- Gödelizzazione delle MT:
  - creiamo una funzione d() che associa a ciascun simbolo un numero dispari (es.: d(C)=5)

    S D C s_0 q_0 s_1 q_1 s_2 q_2 …

    1 3 5 7 9 11 13 15 17 …
  - all'istruzione I: $q_1\ s_0\ s_2\ D\ q_3$ associamo il numero $g(I) = 2^{d(q1)}*3^{d(s0)}*5^{d(s2)}*7^{d(D)}*11^{d(q3)}$
  - alla macchina MT=$\{I_1,I_2,\ldots I_n\}$ associamo il numero $g(MT) = 2^{g(I1)}*3^{g(I2)}*\ldots*p_n^{g(In)}$
    dove p_n è l'n-esimo numero primo

Enumerazione delle MT

- Per l'unicità della scomposizione dei numeri in fattori primi, a ogni MT corrisponde uno e un solo gödeliano g(MT), e a un numero naturale può corrispondere al massimo una sola MT (attenzione: non tutti i numeri sono gödeliani di MT, ad esempio i numeri dispari non lo sono)
- Si induce in questo modo una enumerazione di MT, con le MT ordinate secondo l'ordine dei corrispondenti gödeliani in N:
  $MT_i < MT_j \Leftrightarrow g(MT_i) < g(MT_j)$

Enumerazione delle RG

- Ogni MT computa una funzione RG (per quanto dimostrato da Turing), quindi l'enumerazione delle MT è anche un'enumerazione delle funzioni RG
- Un altro problema non decidibile è il seguente:
  data l'enumerazione $\{\phi_i\}$ delle RG e dato un indice x, ϕ_x è totale?

Il problema della totalità delle funzioni

- Sia ψ la funzione caratteristica degli indici delle funzioni RG totali nell'enumerazione:

$$\psi(x) = \begin{cases} 0, \text{ se } \phi_x \text{ è totale} \\ 1, \text{ se } \phi_x \text{ non è totale} \end{cases}$$

- Supponiamo che ψ sia computabile e definiamo

$$\chi(x) = \begin{cases} \phi_x(x)+1, \text{ se } \psi(x) = 0 \ (\phi_x \text{ è totale}) \\ 0, \text{ se } \psi(x) = 1 \ (\phi_x \text{ non è totale}) \end{cases}$$

Il problema della totalità delle funzioni

- χ è una funzione totale, perché per qualunque x in input, $\chi(x)$ è un risultato definito (infatti si basa su ϕ_x solo quando essa è totale)
- χ è una funzione computabile, perché si suppone che ψ sia computabile, e tutte le ϕ_x sono computabili, quindi χ è nell'enumerazione a una certa posizione k:
  $\chi \equiv \phi_k$
- Calcoliamo $\chi(k)$:
  - secondo la definizione di χ, e dal momento che χ è totale,
    $\chi(k) = \phi_k(k)+1$
  - per il fatto che $\chi \equiv \phi_k$,
    $\chi(k) = \phi_k(k)$
  - mettendo insieme i due risultati, e ricordando che $\phi_k(k)$ esiste perché ϕ_k (cioè χ) è totale, si ottiene 1 = 0
- Si arriva a un assurdo: dobbiamo respingere l'ipotesi che ψ sia computabile: quindi il problema della totalità delle funzioni non è decidibile

Teorema di Rice

- La non-decidibilità di alcuni problemi è un caso particolare di un risultato generale che illustra come non siano decidibili tutte le proprietà non banali delle funzioni ricorsive
- Sia Σ un insieme di funzioni RG ($\Sigma \subseteq$ RG)
- Sia S l'insieme degli indici delle funzioni in Σ nell'enumerazione delle RG ($S=\{x \mid \phi_x \in \Sigma\}$)
- S è ricorsivo $\Leftrightarrow$ S = $\varnothing$ oppure S = N

Non-decidibilità

- Se si scopre che un problema non è decidibile, si può almeno sperare che esso sia semidecidibile
- Un insieme A è semidecidibile quando è enumerabile/ ricorsivamente enumerabile
- Infatti, se A è il rango di una funzione f computabile/ricorsiva generale totale, possiamo generare gli output di f e vedere che l'elemento x viene generato (cioè appartiene ad A) se effettivamente $x \in A$.
  In caso contrario, la procedura non termina mai.
- Semidecidibilità vuole quindi dire ottenere una risposta positiva in tempo finito, oppure attendere un tempo infinito
- Dei due problemi non decidibili, l'arresto di una MT è almeno semidecidibile (se la MT termina abbiamo una risposta positiva in tempi finiti), mentre la totalità delle funzioni non è nemmeno semidecidibile

Non-semidecidibilità della totalità

- Per assurdo, supponiamo che $T=\{x \mid \phi_x \text{ è totale}\}$ sia semidecidibile (ossia ricorsivamente enumerabile)
- T non è vuoto (esistono funzioni RG totali) quindi è il rango di una funzione RG totale ψ
- Ossia, ψ genera tutti gli indici delle totali, quindi
  $\phi_{\psi(0)}\ \phi_{\psi(1)}\ \phi_{\psi(2)}\ \phi_{\psi(3)} \dots$
  contiene tutte e sole le RG totali
- Definiamo $\chi: N \rightarrow N$ come $\chi(x) = \phi_{\psi(x)}(x)+1$
- χ è RG e totale, perché lo sono tutte le $\phi_{\psi(x)}$, e l'incremento di 1 non influisce negativamente su queste proprietà; quindi χ è anch'essa nella sequenza, ossia esiste un k tale che:
  $\chi \equiv \phi_{\psi(k)}$
- Per la definizione di χ, $\chi(k) = \phi_{\psi(k)}(k)+1$
- Per quanto scoperto dopo, $\chi(k) = \phi_{\psi(k)}(k)$
- Finiamo per avere 1 = 0 (perché essendo $\phi_{\psi(k)}$ totale, $\phi_{\psi(k)}(k)$ è una quantità definita)
- Dobbiamo quindi respingere l'ipotesi che T sia semidecidibile