9 Calcolabilita'

Questa sezione integra il capitolo 3 del Papadimitriou con ulteriori risultati attinenti al modello di calcolo basato sulle Turing Machines (TM).

Il modello di calcolo delle Macchine di Turing (TM) puo' essere utilizzato sia per risolvere problemi di decisione (o accettazione), sia per calcolare funzioni (parziali) su Σ^*. Per far questo e' sufficiente aggiungere un nastro di output (per semplicita' si puo supporre che il nastro di input e' read-only, quello di output write-only, e che su tali nastri si possano trovare solo caratteri in un alfabeto Σ prefissato, mentre sui nastri di lavoro si possono usare caratteri in un alfabeto $\Gamma \supseteq \Sigma$ che varia da TM a TM). Un modo conciso di esprimere una serie di risultati fondamentali sul modello di calcolo delle TM e' di considerare la struttura applicativa parziale $\mathsf{X} = (\Sigma^*, \cdot)$, dove la **operazione binaria e parziale $\cdot$ e' data in termini di una codifica delle TM (canoniche) in Σ^*: $y \cdot x = z$ sse y codifica una TM M e M con input x termina e produce z in output**. Indicheremo con $\langle M \rangle$ la stringa che codifica la TM M.

Indichiamo con X l'insieme Σ^* delle stringhe. La nozione di funzione m-aria Turing-calcolabile puo' essere data in modo diretto, mettendo sul nastro di input di una TM m stringhe (separate da un opportuno carattere), oppure in termini di $\cdot$

Definition 9.1 *Una funzione parziale $f: \mathsf{X}^m \rightharpoonup \mathsf{X}$ e'* **calcolabile** $\stackrel{\Delta}{\Longleftrightarrow}$ *esiste $e \in \mathsf{X}$ t.c. $f(x_1, \ldots, x_m) \simeq e \cdot x_1 \cdot \ldots \cdot x_m$, dove $x_i \in \mathsf{X}$. La funzione* **universale** *e' quella funzione $U_m: \mathsf{X}^{m+1} \rightharpoonup \mathsf{X}$ tale che $U_m(\langle M \rangle, x_1, \ldots, x_m) = y$ sse M con input $x_1; \ldots; x_m$ termina e produce y in output. (Si suppone di estendere Σ con un simbolo separatore ";", p.e. il carattere blank).*

Valgono i seguenti risultati fondamentali.

Theorem 9.2 (TM universale) *La funzione U_m e' calcolabile, e la TM che la calcola e' detta TM universale.*

Theorem 9.3 (S-m-n) *Data $f: \mathsf{X}^{m+n} \rightharpoonup \mathsf{X}$ parziale calcolabile, esiste $g: \mathsf{X}^m \to \mathsf{X}$ totale calcolabile t.c. $U_n(g(\overline{x}), \overline{y}) \simeq f(\overline{x}, \overline{y})$ per ogni $\overline{x} \in \mathsf{X}^m$ e $\overline{y} \in \mathsf{X}^n$.*

Le nozioni di insieme decidibile o semi-decidibile e la relazione di riducibilita' possono essere formulate in termini di funzioni calcolabili:

- $L \subseteq \mathsf{X}$ e' **decidibile** sse $\exists e{:}\mathsf{X}.\forall x{:}\mathsf{X}.(x \in L \supset e \cdot x = T) \wedge (x \notin L \supset e \cdot x = F)$
  (dove T e F sono due elementi distinti di X che rappresentano rispettivamente vero e falso)
- $L \subseteq \mathsf{X}$ e' **semi-decidibile** sse $\exists e{:}\mathsf{X}.\forall x{:}\mathsf{X}.(x \in L \leftrightarrow e \cdot x \downarrow)$
- L_1 e' **riducibile** a L_2 (notazione $L_1 \leq L_2$) sse esiste $f: \mathsf{X} \to \mathsf{X}$ totale e calcolabile t.c. $\forall x{:}\mathsf{X}.(x \in L_1 \leftrightarrow f(x) \in L_2)$.

L'indecidibilita' dell'halting problem $H \stackrel{\Delta}{=} \{(x, y) | x\ y \downarrow\}$ segue dal seguente risultato (e dalla proprieta' di chiusura per riduzione dei sottoinsiemi decidibili).

Theorem 9.4 (indecidibilita' dell'halting problem) *L'insieme $K \stackrel{\Delta}{=} \{x \in \mathsf{X} | x \cdot x \downarrow\}$ e'* indecidibile*, cioe' non esiste $d \in \mathsf{X}$ t.c. $d \cdot x = T$ se $x \in K$ e $d \cdot x = F$ se $x \notin K$.*

Proof La dimostrazione procede per assurdo. Supponiamo che d esista, allora possiamo definire (mediante S-m-n) $e \in \mathsf{X}$ t.c. $e\ x \simeq if(d \cdot x, \perp, I) \cdot x$, dove $\perp$ e I sono le TM che calcolano rispettivamente la funzione ovunque divergente e l'identita'. Vediamo che e non puo' appartenere ne' a K ne' al suo complementare:

- se $e \in K$ allora $e \cdot e \downarrow$, e quindi si deve avere $d \cdot e = F$, cioe' $e \notin K$ (assurdo);
- se $e \notin K$ allora $e \cdot e \uparrow$, e quindi si deve avere $d \cdot e = T$, cioe' $e \in K$ (assurdo).

∎

Proposition 9.5 *Se $L_1 \leq L_2$ e L_2 e' (semi-)decidibile, allora anche L_1 e' (semi-)decidibile.*

Il seguente teorema di Rice asserisce l'indecidibilita' delle proprieta' *estensionali* non banali dei programmi. Introduciamo un po' di terminolgia:

- $\mathsf{F} \subseteq \mathsf{X} \rightharpoonup \mathsf{X}$ e' l'insieme delle funzioni calcolabili in X

- fissato $A \subseteq \mathsf{F}$, il sottoinsieme $\langle A \rangle \subseteq \mathsf{X}$ e' t.c. $\langle M \rangle \in \langle A \rangle$ sse la funzione calcolata da M e' in A.

  Un linguaggio $L \subseteq \mathsf{X}$ e' detto una proprieta' estensional dei programmi sse e' della forma $\langle A \rangle$ con $A \subseteq \mathsf{F}$ (se A esiste e' univocamente determinato da L).

Theorem 9.6 (Rice) *Se $A \subset \mathsf{F}$, allora $\langle A \rangle$ e' decidibile sse A e' banale, cioe' $A = \emptyset$ o $A = \mathsf{F}$.*

Proof Si sfrutta la tecnica della riduzione, ovvero facciamo vedere che esiste una $g\colon \mathsf{X} \to \mathsf{X}$ totale e calcolabile t.c. $x \in K$ sse $g(x) \in \langle A \rangle$. Quindi se $\langle A \rangle$ fosse decidibile lo sarebbe anche K.
Supponiamo che A non sia banale e che $\perp \notin \langle A \rangle$ (altrimenti si considera il complementare di A), inoltre sia $a \in \langle A \rangle$. Sia f la funzione parziale calcolabile t.c.

$$f(x,y) \simeq \text{if } (x \cdot x) \downarrow \text{ then } a \cdot y$$

e g una funzione totale calcolabile (data dal Teorema S-m-n) t.c. $U(g(x),y) \simeq f(x,y)$. Allora g e' una riduzione di K ad $\langle A \rangle$. Infatti, se $x \in K$ allora $g(x)$ rappresenta la stessa funzione rappresentata da a e quindi $g(x) \in \langle A \rangle$. Se invece $x \notin K$ allora $g(x)$ rappresenta la funzione ovunque divergente, e quindi $g(x) \notin \langle A \rangle$. ∎

Definition 9.7 *Fissata una codifica $\langle x,y \rangle$ delle coppie di X (calcolata da una TM Pair), per ogni $L \subseteq \mathsf{X}$ e $f\colon \mathsf{X} \to \mathsf{X}$ definiamo*

- $\exists(L) = \{x\colon \mathsf{X} | \exists y\colon \mathsf{X}.\langle x,y \rangle \in L\}$ *detto* **la quantificazione esistenziale** *di L*
- $\exists_f(L) = \{x\colon \mathsf{X} | \exists y\colon \mathsf{X}.|y| \leq |f(x)| \wedge \langle x,y \rangle \in L\}$ *detto* **la quantificazione esistenziale** *di L limitata da f*

In modo analogo si definisce la quantificazione universale di L (limitata da f).

Proposition 9.8 *Il* **predicato T di Kleene**, *$T(\langle M \rangle, x, y) \stackrel{\Delta}{\Longleftrightarrow}$ "y codifica la computazione della TM M con input x", e' decidibile.*

Il predicato di Kleene e' utile per dimostrare alcuni dei seguenti risultati.

Theorem 9.9

- *L e' decidibile sse L ed il suo complementare $\overline{L}$ sono semidecidibili.*
- *L e' semidecidibile sse $L = \exists(R)$ per qualche R decidibile.*

Proof Le direzioni difficili di tali caratterizzazioni si dimostrano dando degli algoritmi che usano il predicato di Kleene.

- supponiamo che la TM $M1$ accetta L e la TM $M2$ accetta $\overline{L}$ allora una TM M che decide L e' data da

  ```
  M(x) = for y in X do
           if T(M1,x,y) and y accepting then accept
           if T(M2,x,y) and y accepting then reject
  ```

  prima o poi troveremo un y per cui uno dei due if e' vero.

- supponiamo che M accetta L, allora definiamo

  ```
  R(x,y) = T(<M>,x,y) and y accepting
  ```

  chiaramente R e' decidibile e $L = \exists(R)$.

∎

Theorem 9.10 *I sottoinsiemi decidibili sono chiusi per complemento, intersezione, unione, e quantificazione (esistenziale ed universale) limitata da una funzione totale calcolabile.*

Proof Siano $M1$ ed $M2$ TM che decidono i linguaggi L_1 ed L_2 allora

- il linguaggio $L_1 \cap L_2$ e' deciso dalla TM `M(x) = if M1(x) and M2(x) then accept else reject`
- il linguaggio $L_1 \cup L_2$ e' deciso dalla TM `M(x) = if M1(x) or M2(x) then accept else reject`

Sia M una TM che decide L e f totale calcolabile, allora

- $\overline{L}$ e' deciso dalla TM `M'(x) = if M(x) then reject else accept`
- $\exists_f(L)$ e' deciso dalla TM

```
M'(x) = n := |f(x)| -- f e' totale calcolabile
        for y in X with |y|<n do
         if M(<x,y>) then accept else continue
        reject
```

- $\forall_f(L)$ e' deciso dalla TM

```
M'(x) = n := |f(x)| -- f e' totale calcolabile
        for y in X with |y|<n do
         if M(<x,y>) then continue else reject
        accept
```

∎

Theorem 9.11 *I sottoinsiemi semidecidibili sono chiusi per intersezione, unione, quantificazione (universale ed esistenziale) limitata da una funzione totale e calcolabile e quantificazione esistenziale.*

Proof Siano $M1$ ed $M2$ TM che accettano i linguaggi L_1 ed L_2 allora

- il linguaggio $L_1 \cap L_2$ e' accettato dalla TM `M(x) = if M1(x) then if M2(x) then accept`
- il linguaggio $L_1 \cup L_2$ e' accettato dalla TM

```
M(x) = for y in X do
         if T(<M1>,x,y) and y accepting then accept
         if T(<M2>,x,y) and y accepting then accept
```

  una definizione alternativa di M e' data dalla *composizione parallela* di $M1$ ed $M2$

Sia M una TM che accetta L e f totale calcolabile, allora

- $\forall_f(L)$ e' accettato dalla TM

```
M'(x) = n := |f(x)| -- f e' totale calcolabile
        for y in X with |y|<n do
         if M(<x,y>) then continue
        accept
```

- $\exists(L)$ e' accettato dalla TM

```
M'(x) = for (y,z) in X do
         if T(<M>,<x,y>,z) and z accepting then accept
```

  si osservi che si ha un unico ciclo for, che enumera tutte le (codifiche) di coppie di stringhe.

- $\exists_f(L)$ e' semidecidibile perche' coincide con $\exists(L')$, dove $L' = \{\langle x, y\rangle \in \mathsf{X} | |y| \leq |f(x)| \wedge \langle x, y\rangle \in L\}$ e' semidecibile (poiche il test $|y| \leq |f(x)|$ e' decidibile.

∎

Theorem 9.12 *Le seguenti asserzioni su* $L \subseteq \mathsf{X}$ *sono equivalenti*

- *L e' semidecidibile, cioe' il dominio di una funzione parziale calcolabile f*
- *L e' l'immagine di una funzione parziale calcolabile g*
- *L e' vuoto o e' l'immagine di una funzione totale calcolabile h.*

Proof Facciamo vedere una catena di implicazioni. Data f definiamo `g(x)=if f(x) defined then x`.
Data g calcolata dalla TM M e $z \in L$ definiamo `h(x,y)=if T(<M>,x,y) and y accepting then g(x) else z`.
Data h definiamo `f(x)=for y in X do if h(y)=x then return(x)`. ∎

Theorem 9.13 *Le seguenti asserzioni su $L \subseteq \mathsf{X}$ sono equivalenti*

- *L e' decidibile, cioe' la funzione caratteristica f e' calcolabile*
- *L e' finito o e' l'immagine di una funzione totale calcolabile h strettamente crescente [rispetto all'ordine lineare dato da $x \leq y$ sse $|x| < |y|$ o ($|x| = |y|$ e $x \leq_{lex} y$), dove $\leq_{lex}$ e' l'ordine lessicografico indotto da un qualche ordine lineare su Σ.*

Mentre la tecnica della riducibilita' serve essenzialemnte a dimostrare risultati negativi (non decidibilita' e non semidecidibilita' di problemi), le proprieta' di chiusura servono soprattutto a dimostrare la decidibilita' e semidecidibilita' di un problema, in alternativa alla descrizione di una TM (o di un algoritmo ad alto livello).

9.1 Esercizi

Dimostrare le seguenti asserzioni

- $TOT = \{\langle M\rangle | f_M$ e' totale$\}$ non e' semidecidibile. TOT e' una proprieta' estensionale dei programmi, infatti $TOT = \langle C\rangle$ con $C = \{f \in \mathsf{F} | f$ e' totale$\}$, e quindi (per RIce) non e' decidibile. Traccia: dimostrare che $\overline{K} \leq TOT$ (usando S-m-n).
- $EM = \{\langle\langle M_1\rangle, \langle M_2\rangle\rangle | f_{M_1} = f_{M_2}\}$ non e' semidecidibile. Traccia: dimostrare che $TOT \leq EQ$ (usando S-m-n).
- Fissata $x \in \mathsf{X}$ si considerino le classi di funzioni parziali calcolabili $C_1 = \{f \in \mathsf{F} | f(x)\downarrow\}$ e $C_1 = \{f \in \mathsf{F} | f(x)\uparrow\}$, dire se $L_i = \langle C_i\rangle$ e' semidecidibile [per Rice non puo' essere decidibile].
- Fissata $x \in \mathsf{X}$ si consideri il linguaggio $L_x = \{y \in \times | \forall z.|z| < |y| \supset U(x,z)\downarrow\}$. Dimostrare che L_x e' decidibile [o e' finito o coincide con X].

  Dimostrare che esiste una g totale calcolabile t.c. per ogni x si ha che $g(x) = \langle M_x\rangle$ (per qualche TM M_x) e M_x ACCETTA L_x.

  Dimostrare che non puo' esistere una g totale calcolabile t.c. per ogni x si ha che $g(x) = \langle M_x\rangle$ (per qualche TM M_x) e M_x DECIDE L_x. Traccia: far vedere K sarebbe decidibile se tale g esistesse.