Ricorsività, incompletezza e indecidibilità

Luca Motto Ros
luca.mottoros@unito.it

Versione del 2 novembre 2024

Indice

Queste note costituiscono gli appunti personali del docente per la parte corrispondente agli ultimi 3 CFU del corso di Istituzioni di Logica tenuto presso il Dipartimento di Matematica dell'Università degli Studi di Torino.

Le note sono largamente basate sui testi [AA19, AB18], ma si discostano da ciascuno di essi sotto vari punti di vista (principalmente per quel che riguarda la notazione e alcune dimostrazioni). Per quanto possibile, per ciascun risultato si è cercato di dare riferimenti precisi al corrispondente risultato in [AA19] e/o [AB18]: si tenga però conto che spesso la corrispondenza è sostanziale ma non completa per via delle variazioni adottate a cui si è accennato.

Resta inteso che la responsabilità di eventuali errori o imprecisioni in questo testo sono da attribuirsi unicamente al presente autore.

Capitolo 1

Cenni di ricorsività

1.1 Funzioni ricorsive

Notazione 1.1.1. Dato $k \in \mathbb{N}$ scriveremo $\vec{x}^k$ come *abbreviazione* (puramente tipografica) di $x_1, \dots, x_k$. Ad esempio, la scrittura $f(\vec{x}^k, y)$ sarà da leggersi $f(x_1, \dots, x_k, y)$. Nel caso degenere $k = 0$ il simbolo $\vec{x}^k$ andrà semplicemente soppresso, cosicché $f(\vec{x}^k, y)$ sarà da leggersi semplicemente $f(y)$. Quando il numero k sarà chiaro dal contesto scriveremo semplicemente $\vec{x}$ al posto di $\vec{x}^k$. Inoltre quando necessario identificheremo $\vec{x}^k$ con la tupla corrispondente $(\vec{x}^k) = (x_1, \dots, x_k)$, e similmente per $\vec{x}$.

Definizione 1.1.2. L'insieme $\mathcal{P}$ delle **funzioni primitive ricorsive** è la più piccola classe contenente

- la funzione costante nulla $c_0 \colon \mathbb{N} \to \mathbb{N} \colon x \mapsto 0$;
- la funzione successore $S \colon \mathbb{N} \to \mathbb{N} \colon x \mapsto x + 1$;
- le funzioni proiezione $U_i^k \colon \mathbb{N}^k \to \mathbb{N} \colon (x_1, \dots, x_k) \mapsto x_i$, per ogni $1 \leq i \leq k$ (in particolare, $U_1^1 \colon \mathbb{N} \to \mathbb{N} \colon x \mapsto x$ è la funzione identità, che denoteremo anche con id);

e chiusa per

- *composizione*: se $h \colon \mathbb{N}^k \to \mathbb{N}$ e $g_i \colon \mathbb{N}^\ell \to \mathbb{N}$ $(1 \leq i \leq k)$ con $h, g_i \in \mathcal{P}$, allora la funzione $f \colon \mathbb{N}^\ell \to \mathbb{N}$ definita da

  $$f(\vec{x}) = h(g_1(\vec{x}), \dots, g_k(\vec{x}))$$

  è in $\mathcal{P}$;
- *ricorsione (primitiva)*:[1] se $h \colon \mathbb{N}^{k+2} \to \mathbb{N}$ e $g \colon \mathbb{N}^k \to \mathbb{N}$ con $h, g \in \mathcal{P}$ allora la

[1] Questo schema include implicitamente il caso $k = 0$, ovvero quando $f \colon \mathbb{N} \to \mathbb{N}$ è definita da

$$\begin{cases} f(0) = n \\ f(y+1) = h(y, f(y)) \end{cases}$$

con $n \in \mathbb{N}$ e $h \colon \mathbb{N}^2 \to \mathbb{N}$. Infatti basta definire $f' \colon \mathbb{N}^2 \to \mathbb{N}$ per ricorsione ponendo

$$\begin{cases} f'(x, 0) = g'(x) \\ f'(x, y+1) = h'(x, y, f'(x, y)) \end{cases}$$

con $g' = c_n$ e $h'(x, y, z) = h(y, z)$, osservando poi che $f(y) = f'(y, y) = f'(U_1^1(y), U_1^1(y))$. (Il fatto che g' e h' siano primitive ricorsive è lasciato al lettore come utile esercizio.)

funzione $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ definita dalle condizioni

$$\begin{cases} f(\vec{x}, 0) = g(\vec{x}) \\ f(\vec{x}, y+1) = h(\vec{x}, y, f(\vec{x}, y)) \end{cases}$$

è in $\mathcal{P}$.

Le funzioni primitive ricorsive sono definite chiudendo un insieme di funzioni iniziali mediante operatori finitari. Dunque si tratta in realtà di una definizione ricorsiva di una successione $(\mathcal{P}_n)_{n\in\omega}$ di famiglie di funzioni (a priori parziali), dove $\mathcal{P}_0 = \{c_0, S\} \cup \{U_i^k \mid 1 \leq i \leq k\}$ e $\mathcal{P}_{n+1}$ è l'unione di $\mathcal{P}_n$ con tutte le funzioni che possono essere ottenute per composizione o ricorsione a partire da funzioni in $\mathcal{P}_n$ (con una sola applicazione di uno di questi schemi). Quindi $\mathcal{P}_n \subseteq \mathcal{P}_{n+1}$ e $\mathcal{P} = \bigcup_{n\in\mathbb{N}} \mathcal{P}_n$. Abbiamo perciò una nozione di altezza $\mathrm{ht}\colon \mathcal{P} \to \mathbb{N}$ che associa ad ogni funzione ricorsiva primitiva f il più piccolo $n \in \mathbb{N}$ tale che $f \in \mathcal{P}_n$ e si possono fare dimostrazioni per induzione su tale altezza. In questo modo si può dimostrare, ad esempio, che tutte le funzioni ricorsive primitive sono totali.

Esempio 1.1.3. Le seguenti funzioni sono primitive ricorsive:

- le funzioni costanti $c_n\colon \mathbb{N} \to \mathbb{N}\colon x \mapsto n$
- la somma
- il prodotto
- l'esponenziale $(x, y) \mapsto x^y$
- il fattoriale $x \mapsto x!$
- la funzione predecessore $\mathrm{pr}(x) = \begin{cases} 0 & \text{se } x = 0 \\ x - 1 & \text{altrimenti.} \end{cases}$
- le funzioni $\mathrm{sgn}(x) = \begin{cases} 0 & \text{se } x = 0 \\ 1 & \text{altrimenti.} \end{cases}$ e $\overline{\mathrm{sgn}}(x) = \begin{cases} 1 & \text{se } x = 0 \\ 0 & \text{altrimenti.} \end{cases}$
- la differenza troncata $x \mathbin{\dot{-}} y = \begin{cases} 0 & \text{se } x < y \\ x - y & \text{altrimenti.} \end{cases}$
- la funzione distanza $(x, y) \mapsto |x - y|$
- le funzioni minimo $\min(x, y)$ e massimo $\max(x, y)$ (insieme alle loro versioni $\min_k$ e $\max_k$ per insiemi di taglia $k > 2$)
- la funzione caratteristica dell'ordine $\chi_{\leq}$, la funzione caratteristica dell'uguaglianza $\chi_{=}$ e le loro varianti naturali $\chi_{\geq}$, $\chi_{<}$, ecc...

Le funzioni primitive ricorsive sono chiuse anche per altri operatori limitati ([AB18, Esercizio 2.15 e Proposizione 2.16]), tra cui:

- *Somme limitate.* Se $h\colon \mathbb{N}^{k+1} \to \mathbb{N}$ è primitiva ricorsiva lo è anche $f_1\colon \mathbb{N}^{k+1} \to \mathbb{N}$ definita da
$$f_1(\vec{x}, y) = \sum_{z \leq y} h(\vec{x}, z).$$
$$\left[\begin{cases} f_1(\vec{x}, 0) = h(\vec{x}, 0) \\ f_1(\vec{x}, y+1) = f_1(\vec{x}, y) + h(\vec{x}, y+1) \end{cases} \right]$$

- *Prodotti limitati.* Se $h\colon \mathbb{N}^{k+1} \to \mathbb{N}$ è primitiva ricorsiva lo è anche $f_2\colon \mathbb{N}^{k+1} \to \mathbb{N}$ definita da
$$f_2(\vec{x}, y) = \prod_{z \le y} h(\vec{x}, z).$$
$$\left[\begin{cases} f_2(\vec{x}, 0) = h(\vec{x}, 0) \\ f_2(\vec{x}, y+1) = f_2(\vec{x}, y) \cdot h(\vec{x}, y+1) \end{cases}\right]$$

- *Minimizzazione limitata.* Se $h\colon \mathbb{N}^{k+1} \to \mathbb{N}$ è primitiva ricorsiva lo è anche $f_3\colon \mathbb{N}^{k+1} \to \mathbb{N}$ definita da
$$f_3(\vec{x}, y) = \mu z \le y\, (h(\vec{x}, z) = 0),$$
dove
$$\mu z \le y\, (h(\vec{x}, z) = 0) = \begin{cases} \min\{z \le y \mid h(\vec{x}, z) = 0\} & \text{se esiste un tale } z \\ y+1 & \text{altrimenti.} \end{cases}$$
$$\left[f_3(\vec{x}, y) = \sum_{v \le y} \prod_{u \le v} \operatorname{sgn}(h(\vec{x}, u)).\right]$$

Si possono anche considerare minimizzazioni in cui la limitazione è determinata mediante una funzione ricorsiva primitiva. Se ad esempio $h\colon \mathbb{N}^{k+1} \to \mathbb{N}$ e $g\colon \mathbb{N}^k \to \mathbb{N}$ sono primitive ricorsive, lo è anche la funzione $f_3'\colon \mathbb{N}^k \to \mathbb{N}$ definita da
$$f_3'(\vec{x}) = \mu z \le g(\vec{x})\, (h(\vec{x}, z) = 0),$$
poiché $f_3'(\vec{x}) = f_3(\vec{x}, g(\vec{x}))$. Similmente, se h è come sopra e $g\colon \mathbb{N} \to \mathbb{N}$ è ricorsiva primitiva, allora lo è anche la funzione $f_3''\colon \mathbb{N}^{k+1} \to \mathbb{N}$ definita da
$$f_3''(\vec{x}, y) = \mu z \le g(y)\, (h(\vec{x}, z) = 0),$$
poiché $f_3''(\vec{x}) = f_3(\vec{x}, g(y))$. Ad esempio, è ricorsiva primitiva la funzione
$$f(\vec{x}, y) = \mu z < y\, (h(\vec{x}, z) = 0).$$
Osservazioni analoghe valgono per somme e prodotti limitati.

Esempio 1.1.4. Le seguenti funzioni sono primitive ricorsive:[2]

- la funzione $\operatorname{Quoz}(n, m)$ che calcola il quoziente della divisione intera di n per m se $m > 0$, e 0 altrimenti;
- la funzione $\operatorname{Res}(n, m)$ che dà il resto della divisione intera di n per m se $m > 0$, e n altrimenti;
- il minimo comune multiplo e il massimo comun divisore di due numeri.

Esempio 1.1.5 ([AA19, p. 141 e seguenti, p. 221])**.** La biezione[3] $\boldsymbol{J}\colon \mathbb{N}^2 \to \mathbb{N}\colon (x, y) \mapsto \frac{1}{2}(x+y)(x+y+1)+x$ e le sue inverse sinistra e destra $(\cdot)_0, (\cdot)_1\colon \mathbb{N} \to \mathbb{N}$ sono funzioni ricorsive primitive. Similmente, definendo per $k \ge 1$ le biezioni
$$\begin{aligned} &\boldsymbol{J}^1\colon \mathbb{N} \to \mathbb{N}\colon x \mapsto x \\ &\boldsymbol{J}^{k+1}\colon \mathbb{N}^{k+1} \to \mathbb{N}\colon (x_1, \dots, x_{k+1}) \mapsto \boldsymbol{J}(x_1, \boldsymbol{J}^k(x_2, \dots, x_{k+1})) \end{aligned}$$

[2] Si noti che le funzioni Quoz e Res sono definiti in modo tale che valga sempre
$$n = \operatorname{Quoz}(n, m) \cdot m + \operatorname{Res}(n, m)$$
per ogni $n, m \in \mathbb{N}$ (incluso il caso degenere $m = 0$).

[3] La funzione $\boldsymbol{J}$ è l'inversa dell'enumerazione triangolare di $\mathbb{N}^2$.

si dimostra che tutte le $\boldsymbol{J}^k$ e le loro inverse $(\cdot)^k_i$, $1 \leq i \leq k$, definite da $\boldsymbol{J}^k((x)^k_1, \dots, (x)^k_k) = x$ sono funzioni ricorsive primitive. Si osservi anche che per ogni $k \geq 1$ e $x_1, \dots, x_k \in \mathbb{N}$

$$\boldsymbol{J}^k(x_1, \dots, x_k) \geq x_i \quad \text{per ogni } 1 \leq i \leq k \tag{1.1}$$

e in particolare $\boldsymbol{J}(x, y) > x, y$ se $(x, y) \neq (0, 0)$ e $(x, y) \neq (0, 1)$. (Si ha invece $\boldsymbol{J}(0, 0) = 0$ e $\boldsymbol{J}(0, 1) = 1$.)

L'**operatore** μ (operatore di minimizzazione *non limitato*) porta la funzione (parziale) $h \colon \mathbb{N}^{k+1} \to \mathbb{N}$ nella funzione (parziale) $f \colon \mathbb{N}^k \to \mathbb{N}$

$$f(\vec{x}) = \mu z \, (h(\vec{x}, z) = 0),$$

dove si intende che f è definita sull'argomento $\vec{x}$ se e solo se esiste $z \in \mathbb{N}$ tale che $h(\vec{x}, z) = 0$ *e h è definita su ogni $(\vec{x}, u)$ con $u \leq z$*; in tal caso, il valore $f(\vec{x})$ è il più piccolo di tali z.

Definizione 1.1.6 ([AB18, Definizione 2.16])**.** La collezione delle **funzioni (μ-)ricorsive** $\mathcal{R}$ è la più piccola classe contenente le funzioni c_0, S, U^k_i e chiusa per composizione, ricorsione e minimizzazione (ovvero applicazioni dell'operatore μ).

Date due funzioni (parziali) ricorsive $g, h \colon \mathbb{N}^k \to \mathbb{N}$ scriviamo

$$g(\vec{x}) \simeq h(\vec{x}),$$

o anche solo $g \simeq h$, per dire che $\operatorname{dom}(g) = \operatorname{dom}(h)$ e $g(\vec{x}) = h(\vec{x})$ per ogni $\vec{x} \in \operatorname{dom}(g)$.

Osservazione 1.1.7. A differenza delle funzioni primitive ricorsive, che sono sempre totali, le funzioni ricorsive sono potenzialmente parziali. Quando dunque si effettua una composizione di funzioni ricorsive h, g_i per ottenere la funzione

$$f(\vec{x}) \simeq h(g_1(\vec{x}), \dots, g_k(\vec{x}))$$

si intende che $\vec{x} \in \operatorname{dom}(f)$ se e solo se $\vec{x} \in \operatorname{dom}(g_i)$ per ogni $1 \leq i \leq k$ e $(g_1(\vec{x}), \dots, g_k(\vec{x})) \in \operatorname{dom}(h)$ (ovvero f è definita sulle tuple su cui effettivamente si può svolgere il calcolo a destra dell'uguaglianza). Discorso analogo vale per le funzioni $f \colon \mathbb{N}^{k+1} \to \mathbb{N}$ definite per ricorsione quando le funzioni $h \colon \mathbb{N}^{k+2} \to \mathbb{N}$ e $g \colon \mathbb{N}^k \to \mathbb{N}$ siano parziali. In particolare, si osservi che il dominio di una tale f risulterà sempre essere chiuso verso il basso rispetto all'ultima coordinata: se $(\vec{x}, y) \in \operatorname{dom}(f)$, allora $(\vec{x}, z) \in \operatorname{dom}(f)$ per ogni $z \leq y$.

Osservazione 1.1.8. Come già sottolineato, nella Definizione 1.1.6 si intende che il μ-operatore e gli schemi di composizione e ricorsione vengano applicati anche a funzioni ricorsive parziali. Tuttavia, restringendo l'uso del μ-operatore e della ricorsione solo a funzioni *totali* si otterrebbe esattamente la stessa classe di funzioni: questo segue dal Teorema di Forma Normale di Kleene 1.5.3 (si veda l'Osservazione 1.5.4).

In particolare, $\mathcal{P} \subseteq \mathcal{R}$. Si può dimostrare che l'inclusione precedente è propria: ad esempio, la funzione di Ackermann $\operatorname{Ack} \colon \mathbb{N}^2 \to \mathbb{N}$ definita da

$$\operatorname{Ack}(m, n) = \begin{cases} n + 1 & \text{se } m = 0 \\ \operatorname{Ack}(m - 1, 1) & \text{se } m > 0 \text{ e } n = 0 \\ \operatorname{Ack}(m - 1, \operatorname{Ack}(m, n - 1)) & \text{se } m > 0 \text{ e } n > 0 \end{cases}$$

è ricorsiva ma non ricorsiva primitiva. Ovviamente le funzioni ricorsive sono anche chiuse per somme limitate, prodotti limitati e minimizzazioni limitate.

Proposizione 1.1.9 ([AB18, Corollario 2.11])**.** *Sia $f \colon \mathbb{N} \to \mathbb{N}$ una funzione totale iniettiva. Se f è ricorsiva, allora la funzione (parziale) f^{-1} è ricorsiva.*

Dimostrazione. Sia $h' \colon \mathbb{N}^2 \to \mathbb{N} \colon (x, y) \mapsto |f(y) - x|$ e si noti che h' è ricorsiva e totale. Quindi è ricorsiva anche $f^{-1}(x) = \mu y\, (h'(x, y) = 0)$. □

In particolare, le biezioni ricorsive da $\mathbb{N}$ in se stesso formano un gruppo.

Tesi di Church. *Una funzione è "calcolabile" (da un computer) se e solo se è ricorsiva.*

Tutte le nozioni viste sin qui si possono estendere in maniera naturale a funzioni $f \colon \mathbb{N}^k \to \mathbb{N}^\ell$ anche quando $\ell > 1$: una tale funzione si dice ricorsiva (primitiva) se e solo se lo sono tutte le funzioni $f_i = U_i^\ell \circ f$ per $1 \le i \le \ell$. Si noti che le $f_i \colon \mathbb{N}^k \to \mathbb{N}$ sono le uniche funzioni tali che

$$f(\vec{x}) = (f_1(\vec{x}), \dots, f_\ell(\vec{x})).$$

In particolare, se $\boldsymbol{J}^k$ è come nell'Esempio 1.1.5 si ha che $(\boldsymbol{J}^k)_i^{-1} = (\cdot)_i^k$, per cui anche le funzioni $(\boldsymbol{J}^k)^{-1} \colon \mathbb{N} \to \mathbb{N}^k$ sono ricorsive primitive. Si può anche osservare che $f \colon \mathbb{N}^k \to \mathbb{N}^\ell$ è ricorsiva (primitiva) se e solo se lo è la funzione $\boldsymbol{J}^\ell \circ f \colon \mathbb{N}^k \to \mathbb{N}$.

Tutti i risultati di questa sezione continuano a valere, *mutatis mutandis*, in questo setup più ampio.

1.2 Insiemi ricorsivi

Identifichiamo sottoinsiemi di $\mathbb{N}^k$ e predicati k-ari su $\mathbb{N}$. In particolare, se P è un tale insieme/predicato scriveremo indifferentemente

$$(x_1, \dots, x_k) \in P$$

oppure

$$P(x_1, \dots, x_k)$$

per dire che il predicato P vale per la tupla $(x_1, \dots, x_k)$.

Definizione 1.2.1 (cfr. [AB18, Definizione 4.1])**.** Un insieme/predicato $P \subseteq \mathbb{N}^k$ si dice **ricorsivo** (**primitivo**) se la sua funzione caratteristica $\chi_P \colon \mathbb{N}^k \to \mathbb{N}$ è una funzione ricorsiva (primitiva).

Si noti che $P \subseteq \mathbb{N}^k$ è ricorsivo (primitivo) se e solo se lo è $\boldsymbol{J}^k[P] \subseteq \mathbb{N}$. Esempi di predicati binari ricorsivi primitivi sono le relazioni $=$, $\le$, $\ge$, $<$ e così via (cfr. l'ultimo punto dell'Esempio 1.1.3).

Proposizione 1.2.2 ([AB18, Proposizioni 4.4, 4.5 e 4.6])**.** *La collezione degli insiemi ricorsivi (primitivi) è chiusa per*

- Sostituzioni ricorsive (totali). *Se $P \subseteq \mathbb{N}^k$ è ricorsivo (primitivo) e le $g_i \colon \mathbb{N}^\ell \to \mathbb{N}$, $1 \le i \le k$, sono funzioni ricorsive (primitive)* totali, *allora anche il predicato $R \subseteq \mathbb{N}^\ell$ definito da*

  $$R(\vec{x}) \iff P(g_1(\vec{x}), \dots, g_k(\vec{x}))$$

  è un sottoinsieme ricorsivo (primitivo).

- Intersezione (= congiunzione), unione (= disgiunzione), complemento (= negazione). *Se $P, Q \subseteq \mathbb{N}^k$ sono ricorsivi (primitivi), allora lo sono anche $P \cap Q$, $P \cup Q$ e ${\sim}P = \mathbb{N}^k \setminus P$.*

Inoltre, tale classe è chiusa anche per quantificazioni limitate, ovvero se $P \subseteq \mathbb{N}^{k+1}$ è ricorsivo (primitivo) allora lo sono anche i predicati R_1 e R_2 definiti da

$$R_1(\vec{x}, y) \iff \forall z \leq y \, P(\vec{x}, z)$$

e

$$R_2(\vec{x}, y) \iff \exists z \leq y \, P(\vec{x}, z)$$

Dimostrazione.

$$\begin{aligned}
\chi_R(\vec{x}) &\simeq \chi_P(g_1(\vec{x}), \dots, g_k(\vec{x})) \\
\chi_{P \cap Q}(\vec{x}) &\simeq \chi_P(\vec{x}) \cdot \chi_Q(\vec{x}) \\
\chi_{P \cup Q}(\vec{x}) &\simeq \operatorname{sgn}(\chi_P(\vec{x}) + \chi_Q(\vec{x})) \\
\chi_{\sim P}(\vec{x}) &\simeq \overline{\operatorname{sgn}}(\chi_P(\vec{x})) \\
\chi_{R_1}(\vec{x}, y) &\simeq \prod_{z \leq y} \chi_P(\vec{x}, z) \\
\chi_{R_2}(\vec{x}, y) &\simeq \operatorname{sgn}\left(\sum_{z \leq y} \chi_P(\vec{x}, y)\right)
\end{aligned}$$ □

Anche le quantificazioni limitate ammettono le varianti discusse dopo gli operatori di somma/prodotto/minimizzazione limitata, ovvero la limitazione può essere determinata da una qualche funzione ricorsiva (primitiva), *purché essa sia totale.*

Esempio 1.2.3. Ogni insieme finito è ricorsivo primitivo. Se ad esempio $P = \{a_1, \dots, a_n\} \subseteq \mathbb{N}$ allora

$$P(x) \iff c_{a_1}(x) = x \vee \ldots \vee c_{a_n}(x) = x.$$

Esempio 1.2.4. Il predicato "x è un numero primo" è primitivo ricorsivo in quanto può essere espresso a partire da predicati ricorsivi primitivi usando connettivi booleani e quantificatori limitati come segue

$$\neg(x = 1) \wedge \forall u \leq x \, \forall v \leq x \, (u \cdot v = x \to u = 1 \vee v = 1). \tag{1.2}$$

Si noti anche che la funzione $m \mapsto p_m$ che enumera in ordine crescente i numeri primi è ricorsiva primitiva. Infatti

$$\begin{cases} p_0 = 2 \\ p_{y+1} = h(p_y) \end{cases}$$

dove $h(x) = \mu z \leq S(x!)$ ("z è primo" $\wedge\ z > x$).

Gli insiemi ricorsivi possono anche essere usati per dare nuovi operatori/schemi di definizione per le funzioni ricorsive (primitive), ad esempio:

- *Definizione per casi.* Se $P_1, \dots, P_n \subseteq \mathbb{N}^k$ sono predicati ricorsivi (primitivi) a due a due disgiunti e $f_i \colon \mathbb{N}^k \to \mathbb{N}$, $1 \leq i \leq n$, sono funzioni ricorsive (primitive) totali, allora la funzione $f \colon \mathbb{N}^k \to \mathbb{N}$ definita da

$$f(\vec{x}) = \begin{cases} f_1(\vec{x}) & \text{se } P_1(\vec{x}) \\ f_2(\vec{x}) & \text{se } P_2(\vec{x}) \\ \vdots & \\ f_n(\vec{x}) & \text{se } P_n(\vec{x}) \\ 0 & \text{altrimenti.} \end{cases}$$

  è ricorsiva (primitiva).

$$[f(\vec{x}) \simeq \chi_{P_1}(\vec{x}) \cdot f_1(\vec{x}) + \ldots + \chi_{P_n}(\vec{x}) \cdot f_n(\vec{x}).]$$

- *Minimizzazione su un predicato ricorsivo.* Se $P \subseteq \mathbb{N}^{k+1}$ è un predicato ricorsivo, la funzione $f\colon \mathbb{N}^k \to \mathbb{N}$ definita da
$$f(\vec{x}) \simeq \mu y\, P(\vec{x}, y)$$
è ricorsiva. Si noti che tale funzione non è necessariamente totale (anche se la funzione caratteristica di P lo è), in quanto per alcuni $\vec{x}$ può darsi che non esista alcun y tale che $P(\vec{x}, y)$.
$$[f(\vec{x}) \simeq \mu y\, (\overline{\mathrm{sgn}}(\chi_P(\vec{x}, y)) = 0).]$$

Proposizione 1.2.5 (cfr. [AB18, Proposizione 4.2])**.** *Se $f\colon \mathbb{N}^k \to \mathbb{N}$ è una funzione ricorsiva (primitiva)* totale*, allora il suo grafo* $\mathrm{graph}(f) \subseteq \mathbb{N}^{k+1}$ *è ricorsivo (primitivo), dove*
$$\mathrm{graph}(f)(\vec{x}, y) \iff f(\vec{x}) = y.$$
Viceversa, se $f\colon \mathbb{N}^k \to \mathbb{N}$ è una funzione (parziale) e $\mathrm{graph}(f)$ *è ricorsivo, allora anche f è ricorsiva.*

Dimostrazione.
$$\chi_{\mathrm{graph}(f)}(\vec{x}, y) \simeq \chi_=(f(\vec{x}), y)$$
e
$$f(\vec{x}) \simeq \mu y\, \mathrm{graph}(f)(\vec{x}, y).$$
□

In particolare, una funzione *totale* $f\colon \mathbb{N}^k \to \mathbb{N}$ è ricorsiva (primitiva) se e solo se lo è $\mathrm{graph}(f)$.

1.3 Insiemi semiricorsivi

Definizione 1.3.1 ([AB18, Definizione 6.1])**.** Un insieme/predicato $P \subseteq \mathbb{N}^k$ è **semiricorsivo** se è la proiezione di un sottoinsieme ricorsivo di $\mathbb{N}^{k+1}$, ovvero se
$$P(\vec{x}) \iff \exists y\, R(\vec{x}, y)$$
per qualche $R \subseteq \mathbb{N}^{k+1}$ ricorsivo.

In particolare, ogni insieme ricorsivo è semiricorsivo (ma non vale il viceversa, si veda il Teorema 1.3.4). Inoltre, si ha nuovamente che $P \subseteq \mathbb{N}^k$ è semiricorsivo se e solo se lo è $\boldsymbol{J}^k[P] \subseteq \mathbb{N}$.

Proposizione 1.3.2 ([AB18, Teorema 6.4, Teorema 6.5 e Proposizione 6.8])**.** *La collezione degli insiemi semiricorsivi è chiusa per sostituzioni ricorsive (mediante funzioni* totali*), proiezioni (= quantificazioni esistenziali), intersezioni (= congiunzioni), unioni (= disgiunzioni) e quantificazioni limitate.*

Dimostrazione. Consideriamo il predicato $R \subseteq \mathbb{N}^\ell$ definito da
$$R(\vec{x}^\ell) \iff P(g_1(\vec{x}^\ell), \dots, g_k(\vec{x}^\ell)),$$
dove $P \subseteq \mathbb{N}^k$ è semiricorsivo e le $g_i\colon \mathbb{N}^\ell \to \mathbb{N}$ sono ricorsive totali. Sia inoltre $S \subseteq \mathbb{N}^{k+1}$ ricorsivo tale che $P(\vec{x}^k) \iff \exists y\, S(\vec{x}^k, y)$. Allora
$$R(\vec{x}^\ell) \iff \exists y\, S(g_1(\vec{x}^\ell), \dots, g_k(\vec{x}^\ell), y),$$
per cui R è semiricorsivo.

Sia ora $R \subseteq \mathbb{N}^k$ definito da
$$R(\vec{x}) \iff \exists z\, P(\vec{x}, z)$$

con $P \subseteq \mathbb{N}^{k+1}$ semiricorsivo. Sia inoltre $S \subseteq \mathbb{N}^{k+2}$ ricorsivo tale che $P(\vec{x}, z) \Longleftrightarrow \exists y\, S(\vec{x}, z, y)$. Allora

$$\begin{aligned} R(\vec{x}) &\iff \exists z \exists y\, S(\vec{x}, z, y) \\ &\iff \exists t\, (\exists z \leq t\, \exists y \leq t\, S(\vec{x}, z, y)). \end{aligned}$$

Siano $P, Q \subseteq \mathbb{N}^k$ semiricorsivi, e siano $R, S \subseteq \mathbb{N}^{k+1}$ ricorsivi tali che $P(\vec{x}) \Longleftrightarrow \exists y\, R(\vec{x}, y)$ e $Q(\vec{x}) \Longleftrightarrow \exists z\, S(\vec{x}, z)$. Allora

$$\begin{aligned} (P \cap Q)(\vec{x}) &\iff \exists y\, R(\vec{x}, y) \wedge \exists z\, S(\vec{x}, z) \\ &\iff \exists t\, [\exists y \leq t\, R(\vec{x}, y) \wedge \exists z \leq t\, S(\vec{x}, z)] \end{aligned}$$

e

$$\begin{aligned} (P \cup Q)(\vec{x}) &\iff \exists y\, R(\vec{x}, y) \vee \exists z\, S(\vec{x}, z) \\ &\iff \exists t\, [\exists y \leq t\, R(\vec{x}, y) \vee \exists z \leq t\, S(\vec{x}, z)]. \end{aligned}$$

Sia infine $P \subseteq \mathbb{N}^{k+1}$ semiricorsivo e siano $R_1, R_2 \subseteq \mathbb{N}^{k+1}$ definiti da

$$\begin{aligned} R_1(\vec{x}, y) &\iff \forall z \leq y\, P(\vec{x}, z) \\ R_2(\vec{x}, y) &\iff \exists z \leq y\, P(\vec{x}, z). \end{aligned}$$

Sia $S \subseteq \mathbb{N}^{k+2}$ tale che $P(\vec{x}, z) \Longleftrightarrow \exists u\, S(\vec{x}, z, u)$. Allora

$$\begin{aligned} R_1(\vec{x}, y) &\iff \forall z \leq y\, \exists u\, S(\vec{x}, z, u) \\ &\iff \exists t\, [\forall z \leq y\, \exists u \leq t\, S(\vec{x}, z, u)] \end{aligned}$$

e

$$\begin{aligned} R_2(\vec{x}, y) &\iff \exists z \leq y\, \exists u\, S(\vec{x}, z, u) \\ &\iff \exists u\, [\exists z \leq y\, S(\vec{x}, z, u)]. \end{aligned}$$ □

Osservazione 1.3.3. La dimostrazione precedente mostra che, a meno di equivalenza su $\mathbb{N}$, si può: esportare i quantificatori illimitati da qualunque connettivo booleano, portare i quantificatori illimitati all'esterno di quelli limitati e contrarre quantificatori illimitati dello stesso tipo in un unico quantificatore illimitato (seguito da eventuali quantificazioni limitate, se necessario). Più precisamente, la dimostrazione mostra come trattare il caso del quantificatore esistenziale (illimitato), ma un discorso analogo può essere fatto per il quantificatore universale (la verifica è lasciata al lettore). Alternativamente, il caso del quantificatore universale può essere ottenuto da quello del quantificatore esistenziale utilizzando le leggi di De Morgan e l'equivalenza tra $\forall z$ e $\neg \exists z \neg$.

Il seguente Teorema di Post caratterizza gli insiemi ricorsivi all'interno dei semiricorsivi.

Teorema 1.3.4 ([AB18, Teorema 6.6])**.** *Un insieme $P \subseteq \mathbb{N}^k$ è ricorsivo se e solo se sia P che $\sim P$ sono semiricorsivi.*

Dimostrazione. Una direzione segue dal fatto che gli insiemi ricorsivi sono chiusi per complemento. Per l'altra direzione, siano $R, S \subseteq \mathbb{N}^{k+1}$ predicati ricorsivi tali che $P(\vec{x}) \iff \exists y\, R(\vec{x}, y)$ e $\sim P(\vec{x}) \iff \exists y\, S(\vec{x}, y)$. La funzione

$$f \colon \mathbb{N}^k \to \mathbb{N} \colon \vec{x} \mapsto \mu y\, (R(\vec{x}, y) \vee S(\vec{x}, y))$$

è ricorsiva totale e tale che $P(\vec{x}) \iff R(\vec{x}, f(\vec{x}))$. Ne segue che P è ottenuto dal predicato ricorsivo R per sostituzione ricorsiva, quindi è anch'esso ricorsivo. □

Proposizione 1.3.5 ([AB18, Teorema 6.9])**.** *Un insieme $P \subseteq \mathbb{N}$ è semiricorsivo se e solo se $P = \emptyset$ oppure $P = \operatorname{rng}(f)$ per qualche $f : \mathbb{N} \to \mathbb{N}$ ricorsiva totale. Un risultato analogo vale per i sottoinsiemi di $\mathbb{N}^k$.*

Dimostrazione. L'insieme vuoto è chiaramente (semi)ricorsivo, quindi possiamo assumere $P \neq \emptyset$.

($\Rightarrow$) Sia $R \subseteq \mathbb{N}^2$ ricorsivo tale che $P(x) \iff \exists y\, R(x, y)$ e fissiamo $a \in P$. La funzione

$$f : \mathbb{N} \to \mathbb{N} : z \mapsto \begin{cases} (z)_0 & \text{se } R((z)_0, (z)_1) \\ a & \text{altrimenti} \end{cases}$$

è totale, ricorsiva e tale che $P = \operatorname{rng}(f)$.

($\Leftarrow$)

$$P(y) \iff \exists x\, (\operatorname{graph}(f)(x, y)).$$

□

In virtù della proposizione precedente, gli insiemi semiricorsivi vengono talvolta detti **ricorsivamente enumerabili**.

Proposizione 1.3.6 ([AB18, Teorema 6.10])**.** *Sia $P \subseteq \mathbb{N}$ un insieme* infinito*. Allora P è ricorsivo se e solo se $P = \operatorname{rng}(f)$ per qualche $f : \mathbb{N} \to \mathbb{N}$ ricorsiva, totale e crescente.*

Dimostrazione. ($\Rightarrow$) La funzione

$$\begin{cases} f(0) = \mu x\, P(x) \\ f(y+1) = \mu x\, (P(x) \wedge f(y) < x) \end{cases}$$

è ricorsiva, totale, crescente e tale che $P = \operatorname{rng}(f)$.

($\Leftarrow$)

$$P(y) \iff \exists x \leq y\, \operatorname{graph}(f)(x, y).$$

□

Si noti in particolare che se $P \subseteq \mathbb{N}$ è ricorsivo e infinito allora esiste una biezione ricorsiva $f : P \to \mathbb{N}$.

Proposizione 1.3.7 (cfr. Proposizione 1.2.5)**.** *Sia $f : \mathbb{N}^k \to \mathbb{N}$ una funzione parziale. Se $\operatorname{graph}(f)$ è semiricorsivo allora f è una funzione ricorsiva e $\operatorname{dom}(f)$ è semiricorsivo.*

Dimostrazione. Sia $R(\vec{x}, y, z) \subseteq \mathbb{N}^{k+2}$ ricorsivo tale che

$$\operatorname{graph}(f)(\vec{x}, y) \iff \exists z\, R(\vec{x}, y, z).$$

Dato $\vec{x} \in \mathbb{N}^k$, se $w \in \mathbb{N}$ è tale che $R(\vec{x}, (w)_0, (w)_1)$ allora $\vec{x} \in \operatorname{dom}(f)$ e $(w)_0 = f(\vec{x})$ poiché $(w)_1$ testimonia $(\vec{x}, (w)_0) \in \operatorname{graph}(f)$. Viceversa, se $\vec{x} \in \operatorname{dom}(f)$ allora esiste $w \in \mathbb{N}$ tale che $R(\vec{x}, (w)_0, (w)_1)$. Perciò

$$f(\vec{x}) \simeq (\mu w\, R(\vec{x}, (w)_0, (w)_1)_0.$$

Inoltre $\vec{x} \in \operatorname{dom}(f) \iff \exists y\, (\operatorname{graph}(f)(\vec{x}, y))$ ed è quindi semiricorsivo. □

1.4 Ricorsività su altri insiemi e codifiche

Definizione 1.4.1. Una **codifica** di un insieme numerabile D è una funzione iniettiva $\varphi : D \to \mathbb{N}$. La codifica si dice **ricorsiva** se $\operatorname{rng}(\varphi)$ è un sottoinsieme ricorsivo[4] di $\mathbb{N}$.

[4]Quindi per quanto detto sugli insiemi infiniti ricorsivi, se D non è finito si può assumere, se necessario, che φ sia in realtà una biezione tra D e $\mathbb{N}$.

Definizione 1.4.2. Siano $\varphi\colon D \to \mathbb{N}$ e $\psi\colon E \to \mathbb{N}$ codifiche ricorsive di due insiemi numerabili D e E. Allora un insieme $A \subseteq D$ si dice (**semi**)**ricorsivo** rispetto all codifica φ se tale è l'insieme $\varphi(A) \subseteq \mathbb{N}$. Similmente, una funzione $f\colon D^k \to E$ si dice **ricorsiva** (**parziale**) rispetto alle codifiche φ e ψ se lo è la funzione $f_\varphi\colon \mathbb{N}^k \to \mathbb{N}$ definita da

$$f_{\varphi,\psi}(x_1, \ldots, x_k) \simeq \psi(f(\varphi^{-1}(x_1), \ldots, \varphi^{-1}(x_n))).$$

Ad esempio, le funzioni $\boldsymbol{J}^k$ forniscono una codifica ricorsiva dell'insieme $\mathbb{N}^k$ (si noti che la nozione di ricorsività che si ottiene rispetto a tale codifica coincide con quella data in precedenza). Similmente la funzione

$$\varphi\colon \mathbb{Z} \to \mathbb{N}\colon z \mapsto \begin{cases} 2z & \text{se } z \geq 0 \\ -(2z+1) & \text{se } z < 0 \end{cases}$$

è una codifica di $\mathbb{Z}$ rispetto alla quale le funzioni di somma e prodotto (sugli interi) sono ricorsive.

Per ciò che segue saremo interessati a codifiche ricorsive dell'insieme $\mathbb{N}^{<\mathbb{N}}$ delle sequenze finite di numeri naturali. In particolare vorremo codifiche $\varphi\colon \mathbb{N}^{<\mathbb{N}} \to \mathbb{N}$ tali che

- $\mathrm{Seq} = \mathrm{rng}(\varphi)$ sia ricorsivo;
- esista una funzione ricorsiva $\ell\colon \mathbb{N} \to \mathbb{N}$ tale che $\ell(n) = \mathrm{length}(\varphi^{-1}(n))$ se $n \in \mathrm{Seq}$;
- esista una funzione ricorsiva $(\!(\cdot,\cdot)\!)\colon \mathbb{N}^2 \to \mathbb{N}$ tale che, posto $(\!(\cdot)\!)_i = (\!(i,\cdot)\!)$, si abbia $(\!(n)\!)_i =$ "l'i-esimo elemento di $\varphi^{-1}(n)$" se $n \in \mathrm{Seq}$ e $i < \ell(n)$;
- esiste una funzione ricorsiva $\mathrm{Conc}\colon \mathbb{N}^2 \to \mathbb{N}$ tale che $\mathrm{Conc}(n,m) = \varphi(\varphi^{-1}(n)^\frown\varphi^{-1}(m))$ se $n, m \in \mathrm{Seq}$ e $\mathrm{Conc}(n,m) = 0$ altrimenti. (L'operazione $s^\frown t$ denota la concatenazione delle sequenze finite s e t.)

Tali codifiche possono essere realizzate in tanti modi. Ad esempio, poiché la funzione $m \mapsto p_m$ che enumera i numeri primi è ricorsiva, si può codificare la generica sequenza $(x_1, \ldots, x_k)$ come

$$p_0^{x_1+1} \cdot \ldots \cdot p_{k-1}^{x_k+1}.$$

Oppure si può codificare $(x_1, \ldots, x_k)$ come

$$\boldsymbol{J}(k, \boldsymbol{J}^k(x_1, \ldots, x_k)).$$

(In entrambi i casi, la sequenza vuota viene convenzionalmente codificata nel numero 0.)

Dal punto di vista della ricorsività, tali codifiche sono perfettamente accettabili. Tuttavia, in entrambi i casi la definizione delle funzioni di codifica utilizza in maniera essenziale definizioni ricorsive (l'enumerazione dei numeri primi nel primo caso, la definizione delle funzioni $\boldsymbol{J}^k$ necessaria per definire $(\!(\cdot,\cdot)\!)$ nel secondo). Quando parleremo di definibilità in $\langle \mathbb{N}, +, \cdot \rangle$ e rappresentabilità nell'aritmetica di Robinson avremo invece bisogno di una codifica che, con l'eccezione di somma e prodotto (che saranno inclusi fin dall'inizio nel linguaggio), non usi lo schema di ricorsione per definire le funzioni di codifica e quelle ausiliarie: per questa ragione, introduciamo ora una codifica che utilizza la funzione β di Gödel, la quale a sua volta si basa sul seguente risultato noto come "teorema cinese dei resti".

Teorema 1.4.3 ([AA19, Theorem 8.28] oppure [AB18, Teorema 14.8])**.** *Se $1 < c_0, \ldots, c_k \in \mathbb{N}$ sono a due a due coprimi, allora per ogni $a_0, \ldots, a_k \in \mathbb{N}$ esiste un unico $0 \leq x < \prod_{i \leq k} c_i$ tale che*

$$x \equiv a_i \mod c_i$$

per ogni $i \leq k$.

Dimostrazione. Per ogni $i \leq k$ troviamo innanzitutto $x_i \in \mathbb{N}$ tale che

$$\begin{cases} x_i \equiv 1 \mod c_i \\ x_i \equiv 0 \mod c_j \quad \text{per ogni } j \leq k \text{ con } j \neq i. \end{cases}$$

Poiché c_i e $\prod_{\substack{j \leq k \\ j \neq i}} c_j$ sono coprimi, l'identità di Bezout

$$z c_i + w \prod_{\substack{j \leq k \\ j \neq i}} c_j = 1$$

ammette una soluzione $(z, w) \in \mathbb{Z}^2$ con $w \geq 0$: basta allora porre $x_i = w \prod_{\substack{j \leq k \\ j \neq i}} c_j$.

Per trovare l'x cercato, basterà ora porre

$$x = \sum_{i \leq k} a_i x_i$$

e calcolare la sua classe di resto rispetto a $\prod_{i \leq k} c_i$. □

Denotiamo la relazione di divisibilità su $\mathbb{N}$ con il simbolo $|$, ovvero $n \mid m$ se e solo se $m = nk$ per qualche $k \in \mathbb{N}$.

Lemma 1.4.4 ([AA19, Lemma 8.29] oppure [AB18, Lemma 14.9])**.** *Sia $y \in \mathbb{N}$ tale che $k' \mid y$ per ogni $1 \leq k' \leq k$ e sia $c_i = (i+1)y + 1$ con $i \leq k$. Allora i numeri c_i sono a due a due coprimi.*

Dimostrazione. Supponiamo per assurdo che esista p primo tale che $p \mid c_i$ e $p \mid c_j$ per $i < j \leq k$. Allora $p \mid (c_j - c_i) = (j - i)y$, quindi $p \mid (j - i)$ oppure $p \mid y$. Ma siccome $j - i \leq k$, per ipotesi $(j - i) \mid y$: da questo segue che in entrambi i casi $p \mid y$. Perció c_i è congruente a 1 modulo p, contraddicendo la scelta di p. □

Osservazione 1.4.5. Si osservi che se $y \geq a_i$ per ogni $i \leq k$, allora $a_j < c_i$ per ogni $i, j \leq k$.

La seguente funzione β, introdotta da Gödel, è chiaramente ricorsiva primitiva.[5]

Definizione 1.4.6 ([AA19, Definition 8.30], cfr. anche [AB18, Definizione 14.10])**.** La funzione $\beta \colon \mathbb{N}^2 \to \mathbb{N}$ è definita da

$$\beta(m, i) = \mathrm{Res}((m)_0, (i+1)(m)_1 + 1).$$

Si osservi che, usando (1.1), per ogni $m, i \in \mathbb{N}$ si ha

$$\beta(m, i) \leq (m)_0 \leq m \tag{1.3}$$

e inoltre $\beta(m, i) < m$ se $m \neq 0$.

Lemma 1.4.7 ([AA19, Lemma 8.31], cfr. anche [AB18, Lemma 14.12])**.** *Per ogni $k \geq 0$ ed ogni $(a_0, \dots, a_k) \in \mathbb{N}^{k+1}$ esiste $m \in \mathbb{N}$ tale che $\beta(m, i) = a_i$ per ogni $i \leq k$.*

Dimostrazione. Sia $y = q!$ dove $q = \max_{k+2}(k, a_0, \dots, a_k)$. Per il Lemma 1.4.4, i numeri $c_i = (i+1)y + 1$ sono a due a due coprimi, e per l'Osservazione 1.4.5 sono maggiori di ciascun a_j. Per il Teorema 1.4.3, esiste un x tale che $x \equiv a_i \bmod c_i$ per ogni $i \leq k$; poiché $a_i < c_i$, si ha $a_i = \mathrm{Res}(x, c_i)$. Basta dunque porre $m = \boldsymbol{J}(x, y)$. □

[5]Le note [AA19] e [AB18] definiscono la funzione β in maniera leggermente differente tra di loro: nel primo testo la coppia (c, d) vience codificata in un unico numero m utilizzando la funzione $\boldsymbol{J}$, mentre nel secondo si definisce direttamente β come funzione ternaria. Noi seguiremo la prima notazione, presentando quindi β come funzione binaria.

Definiamo ora la codifica $\varphi\colon \mathbb{N}^{<\mathbb{N}} \to \mathbb{N}$. Data la sequenza $s = (a_1, \dots, a_k)$, possiamo definire il suo codice $\varphi(s) = \langle\!\langle a_1, \dots, a_k \rangle\!\rangle \in \mathbb{N}$ come il più piccolo m tale che

$$\beta(m, 0) = k \wedge \forall 1 \leq i \leq k\, (\beta(m, i) = a_i).$$

In questo modo le funzioni lunghezza $\ell(x) = \beta(x, 0)$ e decodifica $(\!(i, x)\!) = \beta(x, i+1)$ sono entrambe ricorsive primitive. Inoltre, risulta ricorsivo primitivo anche l'insieme

$$\mathrm{Seq} = \{m \in \mathbb{N} \mid \neg\exists m' < m\, (\ell(m') = \ell(m) \wedge \forall i < \ell(m)\, [(\!(m')\!)_i = (\!(m)\!)_i])\}. \tag{1.4}$$

Si osservi anche che $\langle\!\langle\rangle\!\rangle = 0$ (ovvero la sequenza vuota $\emptyset$ è per costruzione codificata nel numero 0) e che se $k \geq 1$

$$\langle\!\langle a_1, \dots, a_k \rangle\!\rangle > a_j$$

per ogni $a_1, \dots, a_k \in \mathbb{N}$ ed ogni $1 \leq j \leq k$. (Questo segue dal fatto che $\beta(m, i) < m$ se $m \neq 0$.)

Per completare la codifica, dobbiamo introdurre un apposito operatore di concatenazione (nei codici), ovvero una funzione ricorsiva primitiva $\mathrm{Conc}\colon \mathbb{N}^2 \to \mathbb{N}$ tale che

$$\mathrm{Conc}(m, n) = \langle\!\langle \varphi^{-1}(m)^\frown \varphi^{-1}(n) \rangle\!\rangle \tag{1.5}$$

se $m, n \in \mathrm{Seq}$. (Il valore $\mathrm{Conc}(n, m)$ quando $m \notin \mathrm{Seq}$ o $n \notin \mathrm{Seq}$ è del tutto irrilevante.) Similmente, definiremo una funzione ricorsiva primitiva $\mathrm{IS}\colon \mathbb{N}^2 \to \mathbb{N}$ tale che se $m \in \mathrm{Seq}$ e $l \leq \ell(m)$ allora

$$\mathrm{IS}(m, l) = \langle\!\langle \varphi^{-1}(m) \restriction l \rangle\!\rangle, \tag{1.6}$$

ovvero $\mathrm{IS}(m, l)$ è il codice del segmento iniziale di lunghezza l della sequenza codificata da m. Dunque IS sarà la controparte (nei codici) dell'operazione di restrizione su sequenze finite (IS sta per *initial-segment*).

Proposizione 1.4.8 ([AA19, Proposition 11.10])**.** *(1) Esiste una funzione ricorsiva primitiva $B\colon \mathbb{N}^2 \to \mathbb{N}$ tale che per ogni $a_1, \dots, a_k \in \mathbb{N}$*

$$\langle\!\langle a_1, \dots, a_k \rangle\!\rangle \leq B(k, \max_k(a_1, \dots, a_k)).$$

(2) Per ogni $k \geq 1$, la funzione $\varphi \restriction \mathbb{N}^k\colon \mathbb{N}^k \to \mathbb{N}\colon (a_1, \dots, a_k) \mapsto \langle\!\langle a_1, \dots, a_k \rangle\!\rangle$ è ricorsiva primitiva.

(3) Esistono funzioni Conc *e* IS *ricorsive primitive che soddisfano* (1.5) *e* (1.6)*, rispettivamente.*

Dimostrazione. 1. Sia $w(k, n) = (\max(k, n))!$ e definiamo

$$B(k, n) = \boldsymbol{J}\left(\prod_{i \leq k} c(i, k, n), w(k, n)\right),$$

dove $c(i, k, n) = (i+1)w(k, n) + 1$. Le funzioni w, c e B sono tutte ricorsive primitive. Il numero m che si ottiene applicando il Lemma 1.4.7 alla sequenza $(a_0, a_1, \dots, a_k)$ con $a_0 = k$ sarà per costruzione minore o uguale a $B(k, \max_k(a_1, \dots, a_k))$. Poiché per definizione $\langle\!\langle a_1, \dots, a_k \rangle\!\rangle$ è il più piccolo di tali m, la funzione B è come richiesta.

2. Fissiamo $k \geq 1$. Consideriamo la funzione ricorsiva primitiva

$$g\colon \mathbb{N}^k \to \mathbb{N}\colon (a_1, \dots, a_k) \mapsto \max_k(a_1, \dots, a_k).$$

Allora poiché

$$\varphi(a_1, \dots, a_k) = \mu z \leq B(k, g(a_1, \dots, a_k))\, (\ell(z) = k \wedge \forall i < k\, [(\!(z)\!)_i = a_{i+1}]),$$

si ha che anche $\varphi \restriction \mathbb{N}^k\colon \mathbb{N}^k \to \mathbb{N}$ è ricorsiva primitiva.

3. Per quanto riguarda la funzione Conc, consideriamo quella definita da

$$\begin{aligned}\mathrm{Conc}(x,y) = \mu z\,[\ell(z) = \ell(x)+\ell(y)\\ \forall i < \ell(x)\,[(\!(z)\!)_i = (\!(x)\!)_i] \wedge \forall j < \ell(y)\,[(\!(z)\!)_{\ell(x)+j} = (\!(y)\!)_j]].\end{aligned}$$

Essa soddisfa (1.5) ed è certamente ricorsiva. Per dimostrare che è anche ricorsiva *primitiva*, è sufficiente trovare una funzione ricorsiva primitiva $g\colon \mathbb{N}^2 \to \mathbb{N}$ tale che per ogni $x, y \in \mathrm{Seq}$

$$\begin{aligned}\mathrm{Conc}(x,y) = \mu z \le g(x,y)\,[\ell(z) = \ell(x)+\ell(y)\\ \forall i < \ell(x)\,[(\!(z)\!)_i = (\!(x)\!)_i] \wedge \forall j < \ell(y)\,[(\!(z)\!)_{\ell(x)+j} = (\!(y)\!)_j]].\end{aligned}$$

Usando (1.3) si ha che la funzione definita da $h(u) = \max((\!(u)\!)_0, \dots, (\!(u)\!)_{\ell(u)-1})$ si può scrivere come

$$h(u) = \mu v \le u\,[\forall i < \ell(u)\,(\beta(u, i+1) \le v)],$$

ed è quindi ricorsiva primitiva. Perciò sono ricorsive primitive anche le funzioni

$$\begin{aligned}w(x,y) &= (\max\nolimits_3(h(x), h(y), \ell(x)+\ell(y)))!\\ c(i,x,y) &= (i+1)w(x,y)+1.\end{aligned}$$

Come nella dimostrazione del primo punto della proposizione, basta allora porre

$$g(x,y) = \boldsymbol{J}\left(\prod_{i \le \ell(x)+\ell(y)} c(i,x,y), w(x,y)\right).$$

Infine, la funzione IS definita da

$$\mathrm{IS}(m,l) = \mu y \le m\,(\ell(y) = l \wedge \forall j < l\,[(\!(y)\!)_j = (\!(m)\!)_j]).$$

è chiaramente ricorsiva primitiva e soddisfa (1.6). □

Sfruttando questa codifica, possiamo ora dire che una funzione $F\colon \mathbb{N}^{<\mathbb{N}} \to \mathbb{N}^{<\mathbb{N}}$ è ricorsiva (primitiva) se lo è la funzione $\langle\!\langle a_1, \dots, a_k\rangle\!\rangle \mapsto \langle\!\langle F(a_1, \dots, a_k)\rangle\!\rangle$ (e similmente per funzioni $F\colon (\mathbb{N}^{<\mathbb{N}})^k \to \mathbb{N}^{<\mathbb{N}}$ con $k \ge 1$). Allo stesso modo possiamo introdurre il concetto di insieme/predicato (semi)ricorsivo $P \subseteq (\mathbb{N}^{<\mathbb{N}})^k$.

1.5 Alcune applicazioni della codifica di sequenze

Data $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$, sia $f^{\mathrm{m}}\colon \mathbb{N}^{k+1} \to \mathbb{N}$ la **funzione memoria**[6] (**associata ad** f) definita da

$$f^{\mathrm{m}}(\vec{x}, y) = \langle\!\langle f(\vec{x}, 0), \dots, f(\vec{x}, y)\rangle\!\rangle.$$

Si osservi che affinché f^{m} sia definita su $(\vec{x}, y)$, si dovrà avere $(\vec{x}, z) \in \mathrm{dom}(f)$ per ogni $z \le y$. In particolare, $\mathrm{dom}(f^{\mathrm{m}}) = \mathrm{dom}(f)$ se e solo se $\mathrm{dom}(f)$ è chiuso verso il basso rispetto all'ultima coordinata; questo accade, ad esempio, quando f è definita per ricorsione.

Lemma 1.5.1 ([AA19, Lemma 11.15])**.** *Sia $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ tale che se $(\vec{x}, y) \in \mathrm{dom}(f)$, allora $(\vec{x}, z) \in \mathrm{dom}(f)$ per ogni $z \le y$ (cosicché $\mathrm{dom}(f) = \mathrm{dom}(f^{\mathrm{m}})$). Allora f è ricorsiva (primitiva) se e solo se lo è f^{m}.*

[6] L'apice m sta per "memoria", poiché $f^{\mathrm{m}}(\vec{x}, y)$ ricorda tutti i valori $f(\vec{x}, y')$ per ogni $y' \le y$.

Dimostrazione. ($\Rightarrow$)

$$\begin{cases} f^{\mathrm{m}}(\vec{x},0) = \langle\!\langle f(\vec{x},0)\rangle\!\rangle \\ f^{\mathrm{m}}(\vec{x},y+1) = \mathrm{Conc}(f^{\mathrm{m}}(\vec{x},y), \langle\!\langle f(\vec{x},y+1)\rangle\!\rangle) \end{cases}$$

(Si osservi che nella definizione di f^{m} la funzione di codifica $\langle\!\langle \ldots \rangle\!\rangle$ è usata solo su seguenze di lunghezza uno: dunque quel che si sta usando è in realtà la funzione $\varphi \restriction \mathbb{N}^1 \colon \mathbb{N} \to \mathbb{N}$, che è ricorsiva primitiva per la Proposizione 1.4.8(2).)

($\Leftarrow$)

$$f(\vec{x},y) = (\!(f^{\mathrm{m}}(\vec{x},y))\!)_y. \qquad \square$$

Lo schema di ricorsione può essere generalizzato come segue.

Proposizione 1.5.2 ([AA19, Proposition 11.17], cfr. anche [AB18, Teorema 2.17])**.** *Siano $g \colon \mathbb{N}^k \to \mathbb{N}$ e $h \colon \mathbb{N}^{k+2} \to \mathbb{N}$ funzioni ricorsive (primitive). Allora la funzione $f \colon \mathbb{N}^{k+1} \to \mathbb{N}$ definita da*

$$\begin{cases} f(\vec{x},0) = g(\vec{x}) \\ f(\vec{x},y+1) = h(\vec{x},y,f^{\mathrm{m}}(\vec{x},y)). \end{cases}$$

è anch'essa ricorsiva (primitiva).

Dimostrazione. Basta osservare che la funzione memoria f^{m} associata ad f è definita per ricorsione primitiva (ovvero nel senso della Definizione 1.1.2) da

$$\begin{cases} f^{\mathrm{m}}(\vec{x},0) = \langle\!\langle g(\vec{x})\rangle\!\rangle \\ f^{\mathrm{m}}(\vec{x},y+1) = \mathrm{Conc}(f^{\mathrm{m}}(\vec{x},y), \langle\!\langle h(\vec{x},y,f^{\mathrm{m}}(\vec{x},y))\rangle\!\rangle), \end{cases}$$

e poi applicare il Lemma 1.5.1. $\square$

Si osservi che anche nel caso della definizione per ricorsione che utilizza la funzione memoria, il dominio della funzione risultante sarà chiuso verso il basso rispetto all'ultima coordinata.

Il risultato seguente è il celebre Teorema di Forma Normale di Kleene, che non dimostreremo in queste note. Osserviamo però che la sua dimostrazione utilizza in maniera essenziale la possibilità di "tenere traccia" delle computazioni fatte fino ad un dato momento, ovvero quella che noi abbiamo chiamato "funzione memoria" associata ad una data funzione ricorsiva.

Teorema 1.5.3 ([AA19, Theorem 11.30], cfr. anche [AB18, Teorema 8.3])**.** *Per ogni $k \geq 1$ esiste un predicato ricorsivo primitivo $T_k \subseteq \mathbb{N}^{k+2}$ ed una funzione ricorsiva primitiva $U \colon \mathbb{N} \to \mathbb{N}$ tale che per ogni funzione (parziale) ricorsiva $f \colon \mathbb{N}^k \to \mathbb{N}$ esiste un $e \in \mathbb{N}$ per il quale*

$$f(\vec{x}) \simeq U(\mu y\, T_k(e,\vec{x},y)).$$

Osservazione 1.5.4. In particolare, ogni funzione ricorsiva si può scrivere utilizzando un'unica applicazione dell'operatore μ ad una funzione ricorsiva (primitiva) *totale*, ovvero a $\overline{\mathrm{sgn}} \circ \chi_{T_k}$. Anche lo schema di ricorsione verrà utilizzato soltanto nella definizione di T_k e U: essendo questi ricorsivi primitivi, tutte le ricorsioni necessarie a definire (la forma canonica di) f sono applicate a funzioni *totali.*

Proposizione 1.5.5. *Se $f \colon \mathbb{N}^k \to \mathbb{N}$ è una funzione (parziale) ricosiva, allora* $\mathrm{graph}(f) \subseteq \mathbb{N}^{k+1}$ *è un predicato semiricorsivo e quindi anche* $\mathrm{dom}(f)$ *è semiricorsivo.*

Dimostrazione. Sia $e \in \mathbb{N}$ tale che $f(\vec{x}) \simeq U(\mu y\, T_k(e, \vec{x}, y))$. Allora $(\vec{x}, z) \in \mathrm{graph}(f)$ se e solo se

$$\exists y\,[T_k(e, \vec{x}, y) \land \forall w < y\, \neg T_k(e, \vec{x}, w) \land z = U(y)].$$

Inoltre $\mathrm{dom}(f)(\vec{x}) \Longleftrightarrow \exists z\,(\mathrm{graph}(f)(\vec{x}, z))$. □

Corollario 1.5.6. *Una funzione (parziale)* $f\colon \mathbb{N}^k \to \mathbb{N}$ *è ricorsiva se e solo se* $\mathrm{graph}(f)$ *è semiricorsivo.*

Proposizione 1.5.7 (cfr. [AB18, Proposizione 6.3 e Corollario 8.4])**.** *Un insieme* $P \subseteq \mathbb{N}^k$ *è semiricorsivo se e solo se* $P = \mathrm{dom}(f)$ *per qualche funzione ricorsiva parziale* $f\colon \mathbb{N}^k \to \mathbb{N}$.

Dimostrazione. Basta dimostrare che se $P \subseteq \mathbb{N}^k$ è semiricorsivo allora esiste $f\colon \mathbb{N}^k \to \mathbb{N}$ ricorsiva (parziale) tale che $\mathrm{dom}(f) = P$. Sia $R \subseteq \mathbb{N}^{k+1}$ un predicato ricorsivo tale che $P(\vec{x}) \Longleftrightarrow \exists y\, R(\vec{x}, y)$. Allora $f\colon \mathbb{N}^k \to \mathbb{N}\colon \vec{x} \mapsto \mu y\, R(\vec{x}, y)$ è come richiesta. □

Proposizione 1.5.8. *Sia* $f\colon \mathbb{N}^k \to \mathbb{N}$ *ricorsiva. Se* $\mathrm{dom}(f)$ *è ricorsivo allora esiste* $g\colon \mathbb{N}^k \to \mathbb{N}$ *ricorsiva totale tale che* $f \simeq g \restriction \mathrm{dom}(f)$.

Dimostrazione. Sia $e \in \mathbb{N}$ tale che $f(\vec{x}) \simeq U(\mu y\, T_k(e, \vec{x}, y))$ e si osservi che $\mathrm{dom}(f) = \exists y\, T_k(e, \vec{x}, y)$. Essendo $\mathrm{dom}(f)$ ricorsivo, la funzione $h\colon \mathbb{N}^{k+1} \to \mathbb{N}$ definita da

$$h(\vec{x}, y) = \begin{cases} \overline{\mathrm{sgn}}(\chi_{T_k}(e, \vec{x}, y)) & \text{se } \exists y\, T_k(e, \vec{x}, y) \subseteq \mathbb{N}^k \\ 0 & \text{altrimenti.} \end{cases}$$

è ricorsiva totale e tale che per ogni $\vec{x} \in \mathbb{N}^k$ esiste $y \in \mathbb{N}$ tale che $h(\vec{x}, y) = 0$. Segue facilmente che $g\colon \mathbb{N}^k \to \mathbb{N}$ definita da

$$g(\vec{x}) = U(\mu y\,(h(\vec{x}, y) = 0))$$

è ricorsiva totale e $g \restriction \mathrm{dom}(f) = f$. □

Corollario 1.5.9. *Sia* $f\colon \mathbb{N}^k \to \mathbb{N}$ *tale che* $\mathrm{dom}(f)$ *è ricorsivo. Le seguenti affermazioni sono equivalenti:*

(1) f *è ricorsiva;*

(2) $\mathrm{graph}(f)$ *è ricorsivo;*

(3) $\mathrm{graph}(f)$ *è semiricorsivo.*

Dimostrazione. L'unica implicazione ancora da dimostrare è (1) $\Rightarrow$ (2). Sia g ricorsiva totale tale che $g \restriction \mathrm{dom}(f) \simeq f$, cosicché $\mathrm{graph}(g)$ è ricorsivo per la Proposizione 1.2.5. Allora

$$\mathrm{graph}(f)(\vec{x}, y) \quad \Longleftrightarrow \quad \mathrm{dom}(f)(\vec{x}) \land \mathrm{graph}(g)(\vec{x}, y).$$ □

1.6 Gerarchia aritmetica

Definizione 1.6.1. Sia $n \geq 1$. Un predicato $P \subseteq \mathbb{N}^k$ è Σ^0_n se esiste $R \subseteq \mathbb{N}^{k+n}$ ricorsivo tale che

$$P(\vec{x}) \quad \Longleftrightarrow \quad \exists y_1 \forall y_2 \exists y_3 \forall y_4 \ldots Q_n y_n\, R(\vec{x}, y_1, \ldots, y_n)$$

con $Q_n = \forall$ se n è pari e $Q_n = \exists$ se n è dispari.

Dualmente, un predicato $P \subseteq \mathbb{N}^k$ è Π^0_n se esiste $R \subseteq \mathbb{N}^{k+n}$ ricorsivo tale che

$$P(\vec{x}) \iff \forall y_1 \exists y_2 \forall y_3 \exists y_4 \dots Q_n y_n \, R(\vec{x}, y_1, \dots, y_n)$$

con $Q_n = \exists$ se n è pari e $Q_n = \forall$ se n è dispari.

Un predicato P è Δ^0_n se è sia Σ^0_n che Π^0_n.

Infine, diciamo che il predicato $P \subseteq \mathbb{N}^k$ è **aritmetico** se è Σ^0_n oppure Π^0_n per qualche $n \geq 1$.

In particolare, un insieme è semiricorsivo se e solo se è Σ^0_1, gli insiemi Π^0_n sono esattamente i complementari degli insiemi Σ^0_n e gli insiemi Σ^0_{n+1} sono le proiezioni degli insiemi Π^0_n. Per il Teorema 1.3.4 di Post, si ha dunque che gli insiemi ricorsivi sono esattamente gli insiemi Δ^0_1. Quindi gli insiemi aritmetici sono la più piccola classe di insiemi contenente gli insiemi ricorsivi e chiusa per complementi e proiezioni.

Utilizzando quanto visto nella dimostrazione della Proposizion 1.3.2 (si veda anche l'Osservazione 1.3.3), si verifica facilmente per induzione su $n \geq 1$ che tutte le classi precedentemente definite sono chiuse per sostituzioni ricorsive (mediante funzioni totali), intersezioni (= congiunzioni), unioni (= disgiunzioni) e quantificazioni limitate. Inoltre le classi Σ^0_n sono chiuse per quantificazioni esistenziali (= proiezioni), quelle Π^0_n sono chiuse per quantificazioni universali, mentre le classi Δ^0_n sono chiuse per complementi (quindi sono algebre di Boole). Valgono le inclusioni

$$\Sigma^0_n, \Pi^0_n \subseteq \Delta^0_{n+1} \subseteq \Sigma^0_{n+1}, \Pi^0_{n+1}.$$

Da queste osservazioni, segue facilmente che gli insiemi aritmetici sono la più piccola classe contenente gli insiemi (semi)ricorsivi e chiusa per operatori logici (connettivi e quantificatori).

Capitolo 2

Definibilità nel modello standard

2.1 Complessità delle definizioni

La struttura $\langle \mathbb{N}, +, \cdot \rangle$ verrà chiamata *modello standard* dell'aritmetica. Il linguaggio scelto, ovvero $L = \{+, \cdot\}$, è piuttosto minimale, ma si noti che a partire da esso si possono definire, ad esempio:

- la relazione d'ordine: "$x \leq y$" $\Longleftrightarrow \varphi_{\leq}(x, y)$, dove $\varphi_{\leq}(x, y)$ è la L-formula $\exists z\,(z + x = y)$
- il numero 0: "$x = 0$" $\Longleftrightarrow x + x = x$
- il numero 1: "$x = 1$" $\Longleftrightarrow x \cdot x = x \wedge \neg($"$x = 0$"$)$
- la funzione successore: "$S(x) = y$" $\Longleftrightarrow \exists w\,($"$w = 1$" $\wedge\, y = x + w)$

e così via.

Notazione 2.1.1. Se $L \supseteq \{+, \cdot\}$, t è un L-termine e ψ è una L-formula, scriveremo

$$\exists w \leq t\,\psi$$
$$\forall w \leq t\,\psi$$

come abbreviazioni per, rispettivamente,

$$\exists w\,(\varphi_{\leq}(w, t) \wedge \psi)$$
$$\forall w\,(\varphi_{\leq}(w, t) \rightarrow \psi).$$

Le espressioni del tipo $\exists z \leq t$ e $\forall z \leq t$ vengono dette (informalmente) quantificazioni limitate.

Definizione 2.1.2. Sia $L \supseteq \{+, \cdot\}$. Una L-formula si dice Δ_0 se appartiene alla più piccola collezione di L-formule contenente le formule atomiche e chiusa per connettivi e quantificatori limitati.

Una L-formula si dice Σ_1 se appartiene alla più piccola collezione di L-formule contenente le formule Δ_0 e chiusa per congiunzioni, disgiunzioni, quantificazioni limitate e quantificazioni esistenziali. Dualmente, una L-formula si dice Π_1 se appartiene alla più piccola collezione di L-formule contenente le formule Δ_0 e chiusa per congiunzioni, disgiunzioni quantificazioni limitate e quantificazioni universali.

Sia $n \geq 1$. Una L-formula si dice Σ_{n+1} se appartiene alla più piccola collezione di L-formule contenente le formule Π_n e chiusa per congiunzioni, disgiunzioni quantificazioni limitate e quantificazioni esistenziali. Dualmente, una L-formula si dice Π_{n+1} se appartiene alla più piccola collezione di L-formule contenente le formule Σ_n e chiusa per congiunzioni, disgiunzioni, quantificazioni limitate e quantificazioni universali.

Le classi Σ_n, Π_n e Δ_0 si intendono chiuse a meno di equivalenza logica. Ad esempio, si dimostra per induzione su $n \geq 1$ che la negazione di una Σ_n-formula è (logicamente equivalente a) una Π_n-formula e viceversa.

Definizione 2.1.3. Un insieme $P \subseteq \mathbb{N}^k$ si dice **Γ-definibile** (dove Γ è una tra $\Delta_0, \Sigma_n, \Pi_n$ con $n \geq 1$) se esiste una Γ-formula $\varphi(x_1, \dots, x_k)$ tale che

$$P = \{(a_1, \dots, a_k) \in \mathbb{N}^k \mid \langle \mathbb{N}, +, \cdot \rangle \models \varphi[a_1, \dots, a_k]\}.$$

Un predicato si dice **Δ_n-definibile** se è sia Σ_n-definibile che Π_n-definibile.

Una funzione $f\colon \mathbb{N}^k \to \mathbb{N}$ si dice **Γ-definibile** (dove Γ è una tra $\Delta_0, \Sigma_n, \Pi_n, \Delta_n$) se il suo grafo $\operatorname{graph}(f) \subseteq \mathbb{N}^{k+1}$ è un predicato Γ-definibile.

Esempio 2.1.4. I predicati "$x = 0$" e "$x = 1$" sono chiaramente Δ_0-definibili, così come lo sono i predicati "$x = n$" (ovvero gli insiemi $\{n\}$) per qualunque $0 \neq n \in \mathbb{N}$ poiché

$$\text{“}x = n\text{”} \iff \exists y \leq x \, (\text{“}y = 1\text{”} \land x \doteq \underbrace{y + \dots + y}_{n \text{ volte}}).$$

Di conseguenza, qualunque insieme finito $A = \{n_1, \dots, n_k\} \subseteq \mathbb{N}$ è Δ_0-definibile dalla formula

$$\text{“}x = n_1\text{”} \lor \dots \lor \text{“}x = n_k\text{”}.$$

[Se $k = 0$ allora $A = \emptyset$ è definito dalla formula $\neg(x \doteq x)$.]

Segue dall'esempio precedente che un predicato $P \subseteq \mathbb{N}^k$ è Γ-definibile con parametri se e solo se è Γ-definibile senza parametri.

Esempio 2.1.5. La relazione d'ordine è Δ_0-definibile in quanto

$$\text{“}x \leq y\text{”} \iff \exists w \leq y \, (x \doteq w). \tag{2.1}$$

Infatti, per la Notazione 2.1.1 la formula $\exists w \leq y \, (x \doteq w)$ è un'abbreviazione per $\exists w (\varphi_{\leq}(w, y) \land x \doteq w)$, ovvero

$$\exists w (\exists z (z + w \doteq y) \land x \doteq w).$$

La funzione successore è Δ_0-definibile poiché

$$\text{“}S(x) = y\text{”} \iff \exists z \leq y \, (\text{“}z = 1\text{”} \land y \doteq x + z).$$

Anche il predicato "x è un numero primo" è Δ_0-definibile, come si verifica facilmente utilizzando quanto visto finora e la formula (1.2).

Osservazione 2.1.6. Si osservi che, utilizzando quanto visto nella dimostrazione della Proposizione 1.3.2 e nell'Osservazione 1.3.3, se $\varphi(x_1, \dots, x_k)$ è Σ_1 (rispettivamente, Σ_{n+1}) allora esiste una Δ_0-formula (rispettivamente, Π_n) $\psi(x_1, \dots, x_k, y)$ tale che in $\mathbb{N}$ la formula $\exists y \, \psi$ è equivalente a φ (ovvero esse definiscono lo stesso sottoinsieme di $\mathbb{N}^k$). Dunque a meno di equivalenza su $\mathbb{N}$ le formule Σ_n sono della forma

$$\exists y_1 \forall y_2 \dots Q y_n \, \psi(\vec{x}, y_1, \dots, y_n)$$

dove ψ è Δ_0 e $Q = \forall$ se n è pari e $Q = \exists$ se n è dispari. Analogo discorso vale per le formule Π_n.

Osservazione 2.1.7. Sia Γ una tra Σ^0_n, Π^0_n o Δ^0_n. Allora la collezione degli insiemi Γ-definibili è *per definizione* chiusa per intersezioni (= congiunzioni), unioni (= disgiunzioni) e quantificazioni limitate. Inoltre a collezione dei Σ^0_n-definibili è chiusa per proiezioni, mentre la collezione dei Δ^0_n-definibili è chiusa per complementi.

2.2 Ricorsività vs definibilità

Proposizione 2.2.1 ([AA19, Proposition 11.21 e Esercizio 11.60])**.** *Sia $\mathcal{F}$ la più piccola famiglia di funzioni contenente le funzioni U_i^k, $+$, $\cdot$, $\chi_\leq$ e chiusa per composizione e applicazioni dell'operatore μ a funzioni totali. Allora*

$$\mathcal{R} = \mathcal{F}.$$

Dimostreremo la Proposizione 2.2.1 attraverso una serie di lemmi.

Lemma 2.2.2. *Le funzioni* sgn *e* $\overline{\text{sgn}}$ *appartengno ad $\mathcal{F}$.*

Dimostrazione.
- $\overline{\text{sgn}}(x) = \chi_\leq(x + x, x)$
- $\text{sgn} = \overline{\text{sgn}} \circ \overline{\text{sgn}}$. □

Chiamiamo **$\mathcal{F}$-predicati** i $P \subseteq \mathbb{N}^\kappa$ tali che $\chi_P \in \mathcal{F}$. Si noti che se $P \subseteq \mathbb{N}^{k+1}$ è un $\mathcal{F}$-predicato, allora la funzione $f \colon \mathbb{N}^k \to \mathbb{N}$ definita da

$$f(\vec{x}) = \mu y\, P(\vec{x}, y)$$

appartiene ad $\mathcal{F}$ poiché $f(\vec{x}) = \mu y\, (\overline{\text{sgn}}(\chi_P(\vec{x}, y)) = 0)$. Inoltre, gli $\mathcal{F}$-predicati sono chiusi per sostituzioni mediante funzioni *totali* in $\mathcal{F}$: se $P \subseteq \mathbb{N}^k$ è un $\mathcal{F}$-predicato e $g_i \colon \mathbb{N}^\ell \to \mathbb{N}$, $1 \leq i \leq k$, sono funzioni in $\mathcal{F}$, allora $R \subseteq \mathbb{N}^\ell$ definito da

$$R(\vec{x}^\ell) \iff P(g_1(\vec{x}^\ell), \ldots, g_k(\vec{x}^\ell))$$

è un $\mathcal{F}$-predicato.

Lemma 2.2.3. *La collezione degli $\mathcal{F}$-predicati è chiusa per intersezioni (= congiunzioni), unioni (= disgiunzioni) e complementi (= negazioni). In particolare, le relazioni $\leq$, $\geq$, $=$, $\neq$, $<$, $>$, … sono $\mathcal{F}$-predicati.*

Dimostrazione.
- $\chi_{P\cap Q}(\vec{x}) = \chi_P(\vec{x}) \cdot \chi_Q(\vec{x})$
- $\chi_{P\cup Q}(\vec{x}) = \text{sgn}(\chi_P(\vec{x}) + \chi_Q(\vec{x}))$
- $\chi_{\sim P}(\vec{x}) = \overline{\text{sgn}}(\chi_P(\vec{x}))$. □

Lemma 2.2.4. *Le funzioni costanti c_n e la funzione successore S appartengono ad $\mathcal{F}$.*

Dimostrazione.
- $c_0(x) = \mu y\, (x = x + y)$
- $c_1(x) = \mu y\, (x \neq x + y)$
- $c_{n+1}(x) = c_n(x) + c_1(x)$
- $S(x) = x + c_1(x)$. □

Lemma 2.2.5. *Gli $\mathcal{F}$-predicati sono chiusi per quantificazioni limitate: se $P \subseteq \mathbb{N}^{k+1}$ è un $\mathcal{F}$-predicato lo sono anche $Q_1, Q_2 \subseteq \mathbb{N}^{k+1}$ definiti da*

$$\begin{aligned} Q_1(\vec{x}, y) &\iff \exists z \leq y\, P(\vec{x}, z) \\ Q_2(\vec{x}, y) &\iff \forall z \leq y\, P(\vec{x}, z). \end{aligned}$$

Dimostrazione. Sia $P_1 \subseteq \mathbb{N}^{k+2}$ l'$\mathcal{F}$-predicato definito da

$$P_1(\vec{x}, y, z) \iff P(\vec{x}, z) \vee z > y,$$

cosicché la funzione $h_1 : \mathbb{N}^{k+1} \to \mathbb{N} : (\vec{x}, y) \mapsto \mu z\, P_1(\vec{x}, y, z)$ è totale e appartiene ad $\mathcal{F}$. Allora

$$Q_1(\vec{x}, y) \iff h_1(\vec{x}, y) \leq y.$$

è un $\mathcal{F}$-predicato.

Similmente, sia $P_2 \subseteq \mathbb{N}^{k+2}$ l'$\mathcal{F}$-predicato definito da

$$P_2(\vec{x}, y, z) \iff \sim P(\vec{x}, z) \vee z > y,$$

cosicché la funzione $h_2 : \mathbb{N}^{k+1} \to \mathbb{N} : (\vec{x}, y) \mapsto \mu z\, P_2(\vec{x}, y, z)$ è totale e appartiene ad $\mathcal{F}$. Allora

$$Q_2(\vec{x}, y) \iff h_2(\vec{x}, y) > y.$$

è un $\mathcal{F}$-predicato. □

Segue ad esempio che se $f : \mathbb{N}^k \to \mathbb{N}$ è totale e appartiene ad $\mathcal{F}$ e $P \subseteq \mathbb{N}^{k+1}$ è un $\mathcal{F}$-predicato, lo sono anche $Q_1', Q_2' \subseteq \mathbb{N}^{k+1}$ definiti da

$$\begin{aligned} Q_1'(\vec{x}) &\iff \exists z \leq f(\vec{x})\, P(\vec{x}, z) \\ Q_2'(\vec{x}) &\iff \forall z \leq f(\vec{x})\, P(\vec{x}, z), \end{aligned}$$

poiché $Q_i'(\vec{x}) \iff Q_i(\vec{x}, f(\vec{x}))$. Più in generale, ogni volta che la quantificazione è limitata da un funzione totale in $\mathcal{F}$, il predicato risultante sarà un $\mathcal{F}$-predicato.

Lemma 2.2.6. *Le seguenti funzioni appartengono ad $\mathcal{F}$:*

- $\boldsymbol{J}$, $(\cdot)_0$, $(\cdot)_1$
- Res
- β, ℓ, $(\!(\cdot, \cdot)\!)$

Inoltre Seq *è un $\mathcal{F}$-predicato.*

Dimostrazione.

- $\boldsymbol{J}(x, y) = \mu z\, (z + z = (x + y)(x + y + c_1(x)) + x + x)$
  $(z)_0 = \mu x\, [\exists y \leq z\, (\boldsymbol{J}(x, y) = z)]$
  $(z)_1 = \mu y\, [\exists x \leq z\, (\boldsymbol{J}(x, y) = z)]$
- $\mathrm{Res}(n, m) = \mu r\, [\exists q \leq n\, (n = q \cdot m + r)]$
- $\beta(m, i) = \mathrm{Res}((m)_0, (i + c_1(m))(m)_1 + c_1(m))$
  $\ell(m) = \beta(m, c_0(m))$
  $(\!(i, x)\!) = \beta(x, i + c_1(x))$

Segue che la definizione di Seq in (1.4) mostra che esso è un $\mathcal{F}$-predicato. □

Lemma 2.2.7. $\mathcal{P} \subseteq \mathcal{F}$. *In particolare, i predicati ricorsivi primitivi sono $\mathcal{F}$-predicati.*

Dimostrazione. Per il Lemma 2.2.4 si ha $c_0, S \in \mathcal{F}$ e per definizione $U_i^k \in \mathcal{F}$. Poiché $\mathcal{F}$ è chiuso per composizione, basta far vedere che $\mathcal{F}$ è chiusa per ricorsione (applicata a funzioni totali, visto che tali sono tutte le funzioni ricorsive primitive).

Sia f definita per ricorsione a partire dalle funzioni (totali) $g, h \in \mathcal{F}$, ovvero

$$\begin{cases} f(\vec{x}, 0) = g(\vec{x}) \\ f(\vec{x}, y + 1) = h(\vec{x}, y, f(\vec{x}, y)). \end{cases}$$

La funzione f^{m} appartiene ad $\mathcal{F}$ poiché

$$f^{\mathrm{m}}(\vec{x}, y) = \mu m \,[\mathrm{Seq}(m) \wedge \ell(m) = y + c_1(y) \wedge (\!(m)\!)_0 = g(\vec{x}) \\ \wedge \forall i < y\, [(\!(m)\!)_{i+c_1(y)} = h(\vec{x}, i, (\!(m)\!)_i]].$$

Segue che anche $f \in \mathcal{F}$ poiché

$$f(\vec{x}, y) = (\!(f^{\mathrm{m}}(\vec{x}, y))\!)_y \qquad \square$$

Dimostrazione della Proposizione 2.2.1. Siccome $+$, $\cdot$ e $\chi_{\leq}$ sono ricorsive (primitive), si ha $\mathcal{F} \subseteq \mathcal{R}$.

Viceversa, data $f \in \mathcal{R}$ dimostriamo che $f \in \mathcal{F}$. Per il Teorema 1.5.3, sia $e \in \mathbb{N}$ tale che $f(\vec{x}) \simeq U(\mu y\, T_k(e, \vec{x}, y))$. Per il Lemma 2.2.7 si ha che T_k è un $\mathcal{F}$-predicato e $U \in \mathcal{F}$: perciò $f \in \mathcal{F}$ per le proprietà di chiusura di $\mathcal{F}$. $\square$

Teorema 2.2.8 ([AB18, Theorem 14.13, Osservazione 14.16 e Corollario 14.18])**.** *Ogni funzione (parziale) $f\colon \mathbb{N}^k \to \mathbb{N}$ ricorsiva è Σ_1-definibile in $\langle \mathbb{N}, +, \cdot \rangle$.*

Dimostrazione. ($\Rightarrow$) Le funzioni U^k_i, $+$, $\cdot$ sono addirittura Δ_0-definibili e lo è anche $\chi_{\leq}$ poiché se $\psi_{\leq}$ è la Δ_0-formula in (2.1) che definisce $\leq$ si ha

$$\chi_{\leq}(x, y) = z \iff (\psi_{\leq}(x, y) \wedge \text{“}z = 1\text{”}) \vee (\neg\psi_{\leq}(x, y) \wedge \text{“}z = 0\text{”}).$$

Basta allora dimostrare che la classe delle funzioni Σ_1-definibili è chiusa per composizione e minimizzazione su funzioni totali.

Supponiamo che $f(x_1, \ldots, x_\ell) \simeq h(g_1(x_1, \ldots, x_\ell), \ldots, g_k(x_1, \ldots, x_\ell))$ dove le funzioni h, g_i sono definite dalle Σ_1-formule $\varphi_h(z_1, \ldots, z_k, y)$, $\varphi_{g_i}(x_1, \ldots, x_\ell, z_i)$, rispettivamente. Allora f è definita dalla Σ_1-formula

$$\exists z_1 \ldots \exists z_k \left(\varphi_h(z_1, \ldots, z_k, y) \wedge \bigwedge_{1 \leq i \leq k} \varphi_{g_i}(x_1, \ldots, x_\ell, z_i) \right). \tag{2.2}$$

Supponiamo ora che $f(x_1, \ldots, x_k) \simeq \mu y\, (h(x_1, \ldots, x_k, y) = 0)$ con h totale e definibile dalla Σ_1-formula $\varphi_h(x_1, \ldots, x_k, y, z)$. Allora f è definibile dalla Σ_1-formula

$$\exists z\, (\varphi_h(x_1, \ldots, x_k, y, z) \wedge \text{“}z = 0\text{”}) \\ \wedge \forall w < y\, \exists z\, (\varphi_h(x_1, \ldots, x_k, w, z) \wedge \neg(\text{“}z = 0\text{”})). \tag{2.3}$$

$\square$

Corollario 2.2.9 (cfr. [AB18, Corollari 14.17 e 14.18])**.** *Un insieme è semiricorsivo se e solo se è Σ_1-definibile in $\langle \mathbb{N}, +, \cdot \rangle$.*

In particolare, una funzione (parziale) è Σ_1-definibile se e solo se il suo grafo è semiricorsivo.

Dimostrazione. Sia $P \subseteq \mathbb{N}^k$ semiricorsivo e $R \subseteq \mathbb{N}^{k+1}$ ricorsivo tale che $P(\vec{x}) \iff \exists y\, R(\vec{x}, y)$. La funzione χ_R, essendo ricorsiva, è definibile in $\langle \mathbb{N}, +, \cdot \rangle$ da una Σ_1-formula $\varphi(\vec{x}, y, z)$. Allora P è definito dalla Σ_1-formula

$$\exists y \exists w\, (\varphi(\vec{x}, y, w) \wedge \text{“}w = 1\text{”})$$

Viceversa, poiché $+$ e $\cdot$ sono ricorsive primitive e tale collezione di funzioni è chiusa per composizione, si ha che ogni termine $t(x_1, \ldots, x_\ell)$ nel linguaggio $L = \{+, \cdot\}$ induce la funzione ricorsiva primitiva $f_t\colon \mathbb{N}^\ell \to \mathbb{N}\colon (a_1, \ldots, a_\ell) \mapsto t^{\mathcal{N}}[a_1, \ldots, a_\ell]$, dove $\mathcal{N} = \langle \mathbb{N}, +, \cdot \rangle$. Quindi le L-formule atomiche definiscono predicati ricorsivi primitivi e per le proprietà di chiusura di tali insiemi segue che ogni predicato Δ_0-definibile è ricorsivo primitivo. Per le proprietà di chiusura degli insiemi semiricorsivi, segue che ogni insieme Σ_1-definibile è semiricorsivo. $\square$

Osservazione 2.2.10. Si può dimostrare che valgono le inclusioni proprie

$$\Delta_0\text{-definibili} \subsetneq \text{primitivi ricorsivi} \subsetneq \text{ricorsivi}.$$

Tuttavia, per l'Osservazione 2.1.6 le chiusure per proiezioni di tali classi coincidono tutte con la collezione degli insiemi semiricorsivi.

Combinando il risultato precedente con il Teorema 1.3.4 di Post si ottiene

Corollario 2.2.11. *Un insieme è ricorsivo se e solo se è Δ_1-definibile in $\langle \mathbb{N}, +, \cdot \rangle$.*

Con una semplice induzione su $n \geq 1$ si ottiene anche

Corollario 2.2.12 (cfr. [AB18, Corollario 14.19])**.** *Sia $n \geq 1$. Un insieme è Σ^0_n (rispettivamente: Π^0_n, Δ^0_n) se è solo se è Σ_n-definibile (rispettivamente: Π_n-definibile, Δ_n-definibile) in $\langle \mathbb{N}, +, \cdot \rangle$.*

In particolare, gli insiemi aritmetici sono esattamente gli insiemi definibili in $\langle \mathbb{N}, +, \cdot \rangle$.

Passando alle funzioni, combinando Teorema 2.2.8, Corollario 2.2.9, Proposizione 1.3.7, Corollario 2.2.11 e Corollario 1.5.9 si ricava

Corollario 2.2.13. *Per ogni funzione (parziale) $f\colon \mathbb{N}^k \to \mathbb{N}$ sono equivalenti:*

(1) f è ricorsiva;

(2) f è Σ_1-definibile (equivalentemente, $\mathrm{graph}(f)$ è semiricorsivo).

Se inoltre il dominio di f è ricorsivo (equivalentemente, Δ_1-definibile), le affermazioni precedenti sono equivalenti anche a

(3) f è Δ_1-definibile (equivalentemente, $\mathrm{graph}(f)$ è ricorsivo).

Osservazione 2.2.14. Il dominio di una funzione Σ_1-definibile è ovviamente Σ_1-definibile. Questo fornisce una dimostrazione alternativa della Proposizione 1.5.7. Ne consegue che il dominio di una funzione Σ_1-definibile è Δ_1-definibile se e solo se è Π_1-definibile.

Capitolo 3

Teorie formali dell'aritmetica

3.1 Aritmetica di Peano del second'ordine

Definizione 3.1.1 ([AB18, Sezione 15.1]). L'**aritmetica di Peano del second'ordine** PA_2 è la teoria nel linguaggio $L_2 = \{S, 0\}$ assiomatizzata al second'ordine dai seguenti assiomi:

(P1) $\forall x \forall y\, (S(x) = S(y) \to x = y)$ (S è iniettiva)

(P2) $\forall x\, \neg(S(x) = 0)$ (0 non ha predecessori)

(P3) $\forall P\, [P(0) \land \forall u\, (P(u) \to P(S(u))) \to \forall y\, P(y)]$ (Induzione)

Non è necessario avere simboli e assiomi riguardanti ordine, somma e prodotto perché essi possono essere definiti utilizzando apposite formule del second'ordine. Ad esempio:

- "$x \leq y$" è definito da
$$\forall P\, [P(x) \land \forall u\, (P(u) \to P(S(u))) \to P(y)];$$
- la relazione (funzionale) "$x + y = z$" è definita da
$$\forall P\, [P(x, 0, x) \land \forall u \forall v\, (P(x, u, v) \to P(x, S(u), S(v))) \to P(x, y, z)];$$
- la relazione (funzionale) "$x \cdot y = z$" è definita da
$$\forall P\, [P(x, 0, 0) \land \forall u \forall v\, (P(x, u, v) \to \forall w\, (\text{“}w = v+x\text{”} \to P(x, S(u), w))) \to P(x, y, z)],$$
dove "$w = v + x$" è definita come al punto precedente.

Il seguente teorema è dovuto a Dedekind.

Teorema 3.1.2 ([AB18, Teorema 15.7]). *Tutti i modelli di PA_2 sono isomorfi tra di loro.*

Il teorema di Dedekind non garantisce l'esistenza di un modello di PA_2: per questo serve assumere (nella metateoria) una qualche forma dell'assioma dell'infinito. Tuttavia, una volta stabilita l'esistenza di un modello, esso può essere identificato con $\langle \mathbb{N}, S, 0\rangle$ (il numero n sarà identificato con l'interpretazione nel modello del termine chiuso $\underbrace{S(S(\ldots S}_{n \text{ volte}}(0))))$: a meno di isomorfismo, esisterà dunque un unico modello di PA_2 — il modello standard $\langle \mathbb{N}, S, 0\rangle$.

Questo approccio all'aritmetica non è però soddisfacente, in quanto per la logica del second'ordine non vi è alcun calcolo logico che sia corretto e completo: non è dunque possibile garantire che si possano dimostrare tutte le conseguenze logiche di PA_2 (ovvero tutti gli enunciati veri in $\langle \mathbb{N}, S, 0\rangle$).

3.2 Aritmetica di Robinson e aritmetica di Peano del prim'ordine

Consideriamo il linguaggio del prim'ordine $L_Q = \{+, \cdot, S, 0\}$.

Definizione 3.2.1 ([AB18, Sezione 15.2])**.** L'**aritmetica di Robinson**[1] Q è la teoria nel linguaggio L_Q assiomatizzata da

(Q1) $\forall x \forall y\, (S(x) = S(y) \to x = y)$

(Q2) $\forall x\, \neg(0 = S(x))$

(Q3) $\forall x\, (\neg(x = 0) \to \exists z\, (x = S(z)))$

(Q4) $\forall x\, (x + 0 = x)$

(Q5) $\forall x \forall y\, (x + S(y) = S(x + y))$

(Q6) $\forall x\, (x \cdot 0 = 0)$

(Q7) $\forall x \forall y\, (x \cdot S(y) = x \cdot y + x)$

Definizione 3.2.2 ([AB18, Definizione 15.11])**.** L'**aritmetica di Peano** (**del prim'ordine**) PA_1, spesso denotata brevemente con PA, si ottiene aggiungendo a Q uno schema di assiomi di induzione $\mathsf{Ind}_{\varphi,x}$. Data una L_Q-formula del prim'ordine φ e una variabile x che occorra libera in φ, l'assioma $\mathsf{Ind}_{\varphi,x}$ è la chiusura universale[2] di

$$\varphi(0) \wedge \forall x\, (\varphi(x) \to \varphi(S(x))) \to \forall x\, \varphi(x), \qquad (\mathsf{Ind}_{\varphi,x})$$

dove $\varphi(0)$ e $\varphi(S(x))$ sono le formule ottenute da φ sostituendo la variabile x con i termini 0 e $S(x)$, rispettivamente.

Definizione 3.2.3. Chiamiamo **numerali** gli L-termini chiusi costruiti a partire da 0 e S. In particolare, dato $n \in \mathbb{N}$ indicheremo con[3] $\overline{n}$ il numerale $\underbrace{S(S(\ldots S}_{n \text{ volte}}(0)))$.

Sia M un modello di Q. Gli elementi di M vengono chiamati numeri: quelli della forma $\overline{n}^M$ per qualche $n \in \mathbb{N}$ vengono detti **numeri standard** (di M), gli eventuali altri elementi di M vengono detti invece **numeri non standard**. La **parte standard** di M è la sua restrizione a $\{\overline{n}^M \mid n \in \mathbb{N}\}$: questa risulta isomorfa mediante la mappa $\overline{n}^M \mapsto n$ al **modello standard** $\langle \mathbb{N}, +, \cdot, S, 0\rangle$ di Q (con le interpretazioni usuali dei simboli del linguaggio L), che è anche un modello di PA. Il modello M si dice **non standard** se non è isomorfo al modello standard o, equivalentemente, se ha elementi non standard.

Esempio 3.2.4. Definiamo una L_Q-struttura M nel modo seguente. Sia $\mathbb{Z}^+[X]$ l'insieme dei polinomi $p(X)$ nella variabile X a coefficienti in $\mathbb{Z}$ con coefficiente direttore non negativo. Dotiamo $\mathbb{Z}^+[X]$ delle usuali operazioni di somma e prodotto tra polinomi, dell'operazione successore $S^M(p(X)) = p(X) + 1$ e interpretiamo il simbolo 0 nel polinomio nullo, ovvero poniamo $0^M = 0$. Il modello M così costruito è un modello non standard di Q: i suoi numeri standard sono esattamente i polinomi costanti, mentre i numeri non standard sono tutti i polinomi non costanti (ovvero quelli di grado ≥ 1). Si osservi che M non è un modello di PA poiché $M \not\models \mathsf{Ind}_{\varphi,x}$

[1] In [AA19] la teoria che stiamo presentando viene denotata con R, mentre la notazione Q è riservata per una sua variante.

[2] La formula φ potrebbe avere altre variabili libere oltre a x. Queste si intendono quantificate universalmente all'esterno della formula in display.

[3] La definizione formale del termine $\overline{n}$ è data per ricorsione su $n \in \mathbb{N}$ ponendo $\overline{0} = 0$ e $\overline{n+1} = S(\overline{n})$.

dove φ è la formalizzazione in L dell'affermazione "x è pari oppure x è dispari", ovvero

$$\exists z\,(z + z = x \lor z + z = S(x)).$$

Infatti $M \models \varphi[0]$ e per ogni $p(X) \in M$ si ha $M \models \varphi[p(X)] \to \varphi[S^M(p(X))]$: tuttavia, né il polinomio X né il polinomio $S^M(X) = X + 1$ sono il doppio di qualche polinomio.

L'aritmetica di Robinson Q è assai debole. È sufficientemente forte da dimostrare che tutte le usuale proprietà di somma e prodotto valgono per i numeri standard, ma non è detto che esse valgano anche sulla parte non standard di un suo modello. Ad esempio, è possibile trovare modelli di Q in cui non vale la legge commutativa della somma. Nei modelli di PA, invece, molte proprietà esprimibili al prim'ordine si "trasferiscono" dalla parte standard a tutto il modello grazie al corrispondente assioma di induzione. Ad esempio, considerando la formula $\varphi(x)$

$$\forall y\,(x + y = y + x)$$

si ha che la formula vale[4] per $x = 0$ e che $\varphi(x) \to \varphi(S(x))$ per ogni x, quindi per $\mathsf{Ind}_{\varphi,x}$ in un modello di PA la somma risulta sempre commutativa.

Dunque la teoria di PA è un buon compromesso tra PA_2 e Q: è una teoria del prim'ordine (per cui si può utilizzare il teorema di correttezza e completezza per la logica del prim'ordine), ma, a differenza di Q, è sufficientemente potente per dimostrare molte delle proprietà di base dei numeri naturali. Di contro, la teoria Q ha il vantaggio tecnico di essere finitamente assiomatizzata, cosa che risulterà cruciale più avanti.

3.3 Rappresentabilità delle funzioni ricorsive in Q

Sia $L \supseteq L_Q$ un linguaggio che estende quello dell'aritmetica di Robinson. La relazione di dimostrabilità $\vdash$ si riferisce a qualunque calcolo logico (per la logica del prim'ordine) che sia corretto e completo. Se $\varphi(x_1, \ldots, x_k)$ è una L-formula e t_1, …, t_k sono L-termini, denotiamo con $\varphi(t_1/x_1, \ldots, t_k/x_k)$ la formula che si ottiene sostituendo in φ le occorrenze libere di ciascuna x_i con il corrispondente termine t_i (quando tale sostituzione è ammissibile). Quando le variabili x_1, …, x_k sono chiare dal contesto, scriviamo semplicemente $\varphi(t_1, \ldots, t_k)$ invece di $\varphi(t_1/x_1, \ldots, t_k/x_k)$.

Definizione 3.3.1 ([AA19, Definition 21.24], cfr. anche [AB18, Definizioni 15.44 e 15.46])**.** Sia T una L-teoria. La formula $\varphi(x_1, \ldots, x_k)$ **rappresenta**[5] **il *predicato*** $P \subseteq \mathbb{N}^k$ **in** T se per ogni $a_1, \ldots, a_k \in \mathbb{N}$

- se $(a_1, \ldots, a_k) \in P$ allora $T \vdash \varphi(\overline{a_1}, \ldots, \overline{a_k})$;
- se $(a_1, \ldots, a_k) \notin P$ allora $T \vdash \neg\varphi(\overline{a_1}, \ldots, \overline{a_k})$.

La formula $\varphi(x_1, \ldots, x_k, y)$ **rappresenta la *funzione* totale** $F\colon \mathbb{N}^k \to \mathbb{N}$ **in** T se per ogni $a_1, \ldots, a_k \in \mathbb{N}$

$$T \vdash \forall y\,[\varphi(\overline{a_1}, \ldots, \overline{a_k}, y) \leftrightarrow y = \overline{F(a_1, \ldots, a_k)}].$$

Un predicato o una funzione si dicono **rappresentabili in** T se esiste una formula che li rappresenta in T (la formula in questione non è necessariamente unica).

[4]Entrambe queste affermazioni richiedono a loro volta una dimostrazione per induzione. Ad esempio, per dimostrare $\varphi(0/x)$ si deve prima dimostrare che vale $\forall x(0 + x = x)$ usando il corrispindente assioma di induzione.

[5]Le note [AB18] parlano di *binumerabilità* anziché *rappresentabilità*.

Osservazione 3.3.2. La condizione nella definizione di rappresentabilità di una funzione F richiede solo che la formula definisca una funzione *quando ristretta ai numeri standard* (sui numeri non standard può anche essere soltanto una relazione). Tuttavia, tale condizione è più forte della mera richiesta di rappresentabilità del grafo di F, poiché quest'ultima non esclude invece che in qualche modello M di T ci possa essere qualche y nonstandard per cui valga $M \models \varphi(\overline{a_1}, \dots, \overline{a_k}, y)$ (oltre al numero standard $\overline{F(a_1, \dots, a_k)}$ che deriva dalla rappresentabilità ed è l'unico numero standard che può rendere vera la formula).

Osservazione 3.3.3. Se T è incoerente (cfr. Definizione 4.2.5), allora qualunque formula col giusto numero di variabili libere rappresenta qualunque predicato o funzione totale poiché $T \vdash \psi$ per ogni ψ. Quindi nelle dimostrazioni di rappresentabilità si può di fatto assumere che la teoria T sia coerente.

Scopo di questa sezione è mostrare che Q (e le sue estensioni) rappresentano tutte le funzioni totali ricorsive e tutti i predicati ricorsivi. In ciò che segue considereremo solo il linguaggio $L = L_Q$, per cui formule e termini vanno intesi come L_Q-formule e L_Q-termini, rispettivamente. Faremo continuamente uso del teorema di completezza, ovvero del fatto che per ogni L_Q-formula φ

$$\begin{aligned} Q \vdash \varphi &\iff Q \models \varphi \\ &\iff \text{per ogni } L_Q\text{-struttura } M, \text{ se } M \models Q \text{ allora } M \models \varphi. \end{aligned}$$

La dimostrazione del lemma seguente è lasciata al lettore come (facile) esercizio.

Lemma 3.3.4 (cfr. [AA19, Remark 21.25(c)])**.** *Se $P, R \subseteq \mathbb{N}^k$ sono rappresentabili in Q dalle formule φ e ψ, rispettivamente, allora anche $P \cap R$, $P \cup R$ e $\sim P$ sono rappresentati dalle formule $\varphi \wedge \psi$, $\varphi \vee \psi$ e $\neg\varphi$, rispettivamente. In particolare, gli insiemi rappresentabili in Q formano un'algebra di Boole.*

Osservazione 3.3.5. Il lemma precedente si applica a qualunque teoria del prim'ordine T.

Lemma 3.3.6 ([AA19, Lemma 21.26])**.** *Un predicato $P \subseteq \mathbb{N}^k$ è rappresentabile in Q (da una formula Δ_0) se e solo se la sua funzione caratteristica $\chi_P \colon \mathbb{N}^k \to \mathbb{N}$ è rappresentabile in Q (da una formula Δ_0).*

Dimostrazione. Se $\varphi(x_1, \dots, x_k)$ rappresenta P in Q allora la formula $\psi(x_1, \dots, x_k, y)$

$$(\varphi(x_1, \dots, x_k) \wedge y = \overline{1}) \vee (\neg\varphi(x_1, \dots, x_k) \wedge y = \overline{0})$$

rappresenta χ_P in Q. (Si noti che se φ è Δ_0 anche ψ lo è.) Infatti, fissiamo un modello $M \models Q$ e siano $a_1, \dots a_k \in \mathbb{N}$ arbitrari. Allora se $(a_1, \dots, a_k) \in P$ (ovvero $\chi_P(a_1, \dots, a_k) = 1$) si ha

$$M \models \varphi(\overline{a_1}, \dots, \overline{a_k})$$

da cui

$$M \models \psi(\overline{a_1}, \dots, \overline{a_k}, \overline{1})$$

e quindi, poiché $M \not\models \neg\varphi(\overline{a_1}, \dots, \overline{a_k})$ per l'ipotesi su $a_1, \dots, a_k$,

$$M \models \forall y\, (\psi(\overline{a_1}, \dots, \overline{a_k}, y) \leftrightarrow y = \overline{1}).$$

Se invece $(a_1, \dots, a_k) \notin P$ (ovvero $\chi_P(a_1, \dots, a_k) = 0$) allora

$$M \models \neg\varphi(\overline{a_1}, \dots, \overline{a_k})$$

da cui

$$M \models \psi(\overline{a_1}, \dots, \overline{a_k}, \overline{0})$$

e quindi, poiché $M \not\models \varphi(\overline{a_1}, \dots, \overline{a_k})$ per l'ipotesi su $a_1, \dots, a_k$,

$$M \models \forall y \, (\psi(\overline{a_1}, \dots, \overline{a_k}, y) \leftrightarrow y = \overline{0}).$$

Quindi in ogni caso

$$M \models \forall y \, (\psi(\overline{a_1}, \dots, \overline{a_k}, y) \leftrightarrow y = \overline{\chi_P(a_1, \dots, a_k)}),$$

da cui per l'arbitrarietà di M il teorema di completezza del calcolo logico scelto

$$Q \vdash \forall y \, (\psi(\overline{a_1}, \dots, \overline{a_k}, y) \leftrightarrow y = \overline{\chi_P(a_1, \dots, a_k)}).$$

Viceversa, se $\psi(x_1, \dots, x_k, y)$ rappresenta χ_P in Q allora la formula $\varphi(x_1, \dots, x_k)$

$$\psi(x_1, \dots, x_k, \overline{1})$$

rappresenta P in Q. (Si noti che se ψ è Δ_0 anche φ lo è.) Infatti, se $(a_1, \dots, a_k) \in P$ (ovvero $\chi_P(a_1, \dots, a_k) = 1$) allora

$$Q \vdash \forall y \, (\psi(\overline{a_1}, \dots, \overline{a_k}, y) \leftrightarrow y = \overline{1})$$

da cui, in particolare,

$$Q \vdash \psi(\overline{a_1}, \dots, \overline{a_k}, \overline{1}) \leftrightarrow \overline{1} = \overline{1}$$

e quindi, poiché $Q \vdash \forall x \, (x = x)$ e quindi $Q \vdash \overline{1} = \overline{1}$,

$$Q \vdash \varphi(\overline{a_1}, \dots, \overline{a_k}).$$

Se invece $(a_1, \dots, a_k) \notin P$ (ovvero $\chi_P(a_1, \dots, a_k) = 0$) allora

$$Q \vdash \forall y \, (\psi(\overline{a_1}, \dots, \overline{a_k}, y) \leftrightarrow y = \overline{0})$$

da cui, in particolare,

$$Q \vdash \psi(\overline{a_1}, \dots, \overline{a_k}, \overline{1}) \leftrightarrow \overline{1} = \overline{0}$$

e quindi, poiché per l'assioma (Q2) si deve avere $Q \vdash \neg(0 = S(0))$, ovvero $Q \vdash \neg(\overline{0} = \overline{1})$,

$$Q \vdash \neg\varphi(\overline{a_1}, \dots, \overline{a_k}).$$ □

Osservazione 3.3.7. Il lemma precedente si applica a qualunque teoria T tale che $T \vdash \neg(\overline{0} = \overline{1})$.

Cominciamo col vedere che in Q si possono rappresentare la somma, il prodotto e la funzione successore su $\mathbb{N}$. Si osservi che per dimostrare che una funzione $F \colon \mathbb{N}^k \to \mathbb{N}$ è rappresentata in una teoria T da una formula del tipo $f(x_1, \dots, x_k) = y$ con f simbolo di funzione k-ario nel linguaggio di T, è sufficiente mostrare che per ogni $a_1, \dots, a_k \in \mathbb{N}$

$$T \vdash f(\overline{a_1}, \dots, \overline{a_k}) = \overline{F(a_1, \dots, a_k)}.$$

Infatti, poiché il simbolo f compare nel linguaggio di T, ogni modello di T interpreterà tale simbolo in una funzione, da cui segue (per il teorema di completezza) che T dimostra che la formula $f(x_1, \dots, x_k) = y$ definisce una funzione (anche sui numeri nonstandard, che è più di quanto richiesto).

Per quanto riguarda la funzione successore $n \mapsto n + 1$ su $\mathbb{N}$ c'è poco da dire: la formula $S(x) = y$ rappresenta tale funzione in Q (o in qualunque altra teoria in un linguaggio $L \supseteq L_Q$) in quanto per definizione stessa di numerale si ha che $S(\overline{a})$ e $\overline{a+1}$ sono letteralmente lo stesso numerale, quindi $Q \vdash S(\overline{a}) = \overline{a+1}$ poiché $Q \vdash \forall x \, (x = x)$.

Lemma 3.3.8 ([AB18, Lemmi 15.24 e 15.25]). *La formula $x + y = z$ rappresenta la funzione somma $+$ in Q. La formula $x \cdot y = z$ rappresenta la funzione prodotto $\cdot$ in Q.*

Dimostrazione. Consideriamo prima il caso della somma e dimostriamo che per ogni $a, b, c \in \mathbb{N}$ tali che $a + b = c$ si ha $Q \vdash \overline{a} + \overline{b} = \overline{c}$.

Per induzione su $b \in \mathbb{N}$. Se $b = 0$ allora $c = a$ e $Q \vdash \overline{a} + \overline{0} = \overline{a}$ per (Q4) (si ricordi che per definizione $\overline{0} = 0$). Se $b > 0$ allora $a + (b - 1) = c - 1$ e per ipotesi induttiva $Q \vdash \overline{a} + \overline{b-1} = \overline{c-1}$, da cui $Q \vdash S(\overline{a} + \overline{b-1}) = S(\overline{c-1})$. Applicando (Q5), si ha allora $Q \vdash \overline{a} + S(\overline{b-1}) = S(\overline{c-1})$ da cui, ricordando che $S(\overline{b-1}) = \overline{b}$ e $S(\overline{c-1}) = \overline{c}$ si ha $Q \vdash \overline{a} + \overline{b} = \overline{c}$.

Il caso della moltiplicazione è simile. Siano $a, b, c \in \mathbb{N}$ con $a \cdot b = c$ e dimostriamo per induzione su $b \in \mathbb{N}$ che $Q \vdash \overline{a} \cdot \overline{b} = \overline{c}$. Il caso base $b = 0$ segue facilmente da (Q6). Se $b > 0$, allora $c = a \cdot (b-1) + a$ da cui, ponendo $c' = a \cdot (b-1)$ e utilizzando (Q7), l'ipotesi induttiva $Q \vdash \overline{a} \cdot \overline{b-1} = \overline{c'}$ e il fatto che $Q \vdash \overline{c'} + \overline{a} = \overline{c' + a}$ per quanto già dimostrato per la somma, si ottiene facilmente $Q \vdash \overline{a} \cdot S(\overline{b-1}) = \overline{c}$, ovvero $Q \vdash \overline{a} \cdot \overline{b} = \overline{c}$. □

Osservazione 3.3.9. Quanto osservato fin qui dimostra che se $M \models Q$ allora la biezione canonica $n \mapsto \overline{n}^M$ tra $\mathbb{N}$ e la parte standard di M è in realtà un isomorfismo tra L_Q-strutture.

Corollario 3.3.10 ([AB18, Corollario 15.27]). *Per ogni L-termine chiuso t esiste $n \in \mathbb{N}$ tale che $Q \vdash t = \overline{n}$.*

Dimostrazione. Per induzione sull'altezza di t. Se $\mathrm{ht}(t) = 0$ allora t è il termine 0, per cui $Q \vdash t = \overline{0}$ (poiché $Q \vdash \forall x\,(x = x)$ e, per definizione di numerale, $\overline{0} = 0$). Se $t = S(t')$ e $Q \vdash t' = \overline{n}$, allora per gli assiomi (logici) dell'uguaglianza $Q \vdash S(t') = S(\overline{n})$, ovvero $Q \vdash t = \overline{n+1}$. Se $t = t_1 + t_2$ (rispettivamente, $t = t_1 \cdot t_2$) e $Q \vdash t_1 = \overline{n_1}$ e $Q \vdash t_2 = \overline{n_2}$, allora $Q \vdash t = \overline{n_1 + n_2}$ (rispettivamente, $Q \vdash t = \overline{n_1 \cdot n_2}$) per gli assiomi dell'uguaglianza e il Lemma 3.3.8. □

Lemma 3.3.11 ([AA19, Lemma 19.28] oppure [AB18, Lemmi 15.28 e 15.29]). *La formula $x_1 = x_2$ rappresenta la relazione di uguaglianza $P = \{(n, m) \in \mathbb{N}^2 \mid n = m\}$.*

Dimostrazione. Se $a = b$ allora $\overline{a}$ e $\overline{b}$ sono lo stesso termine, per cui $Q \vdash \overline{a} = \overline{b}$ poiché $Q \vdash \forall x\,(x = x)$.

Siano ora $a, b \in \mathbb{N}$ distinti e assumiamo senza perdere generalità che $a < b$. Dimostriamo per induzione su $a \in \mathbb{N}$ che $Q \vdash \neg(\overline{a} = \overline{b})$. Poiché $b > 0$ si ha $\overline{b} = S(\overline{b-1})$. Se $a = 0$ (ovvero $\overline{a} = \overline{0} = 0$), allora $Q \vdash \neg(\overline{a} = S(\overline{b-1}))$ per (Q2), ovvero $Q \vdash \neg(\overline{a} = \overline{b})$. Se invece $a > 0$, allora $\overline{a} = S(\overline{a-1})$ e $a - 1 \neq b - 1$. Per ipotesi induttiva $Q \vdash \neg(\overline{a-1} = \overline{b-1})$ e quindi $Q \vdash \neg(S(\overline{a-1}) = S(\overline{b-1}))$ per (Q1), ovvero $Q \vdash \neg(\overline{a} = \overline{b})$. □

Osservazione 3.3.12. La seconda parte della dimostrazione precedente non è banale. Se ad esempio il simbolo S viene interpretato in un dato modello M nella funzione identità, allora per ogni $a, b \in \mathbb{N}$ si ha che $M \models \overline{a} = \overline{b}$ perché $\overline{a}^M = 0^M = \overline{b}^M$ (anche se quando $a \neq b$ si ha che $\overline{a} \neq \overline{b}$, ovvero i numerali $\overline{a}$ e $\overline{b}$ sono termini distinti perché contengono un diverso numero di S). Chiaramente un tale M non sarà un modello di Q.

Corollario 3.3.13 ([AB18, Lemma 15.30]). *Se t_1, t_2 sono L-termini chiusi, allora $Q \vdash t_1 = t_2$ oppure $Q \vdash \neg(t_1 = t_2)$.*

Passiamo ora a dimostrare che la formula $\varphi_{\leq}(x, y)$, ovvero $\exists z\,(z + x = y)$, rappresenta in Q l'ordine usuale su $\mathbb{N}$, ovvero il predicato $\{(n, m) \in \mathbb{N}^2 \mid n \leq m\}$.

Lemma 3.3.14 ([AB18, Lemma 15.32])**.** *Per ogni*[6] $n \in \mathbb{N}$

$$Q \vdash \forall x\,(\varphi_{\leq}(x, \overline{n}) \leftrightarrow x = \overline{0} \vee x = \overline{1} \vee \ldots \vee x = \overline{n}).$$

Dimostrazione. Fissiamo un modello $M \models Q$ e dimostriamo che per qualunque $n \in \mathbb{N}$ e qualunque $q \in M$

$$M \models \varphi_{\leq}[q, \overline{n}] \leftrightarrow q = \overline{0} \vee \ldots \vee q = \overline{n}.$$

L'implicazione da destra a sinistra segue dal Lemma 3.3.8 per cui basta dimostrare per induzione su $n \in \mathbb{N}$ che se per un dato $q \in M$ vale $M \models \varphi_{\leq}[q, \overline{n}]$ allora $M \models q = \overline{m}$ per qualche $m \leq n$.

Sia $n = 0$. Allora poiché per ipotesi $M \models \varphi_{\leq}[q, \overline{n}]$ si ha che $M \models z + q = \overline{0}$ per qualche $z \in M$. Se per assurdo $M \not\models q = \overline{0}$, allora per (Q3) si avrebbe $M \models q = S(y)$ per qualche $y \in M$, da cui $M \models z + S(y) = S(z + y)$ per (Q5) e quindi anche $M \models S(z + y) = \overline{0}$ per la scelta di y e z, contraddicendo (Q2).

Sia ora $n > 0$ e supponiamo che $M \models z+q = \overline{n}$ per qualche $z \in M$. Distinguiamo due casi. Se $M \models q = \overline{0}$ siamo a posto. Se invece $M \not\models q = \overline{0}$, allora per (Q3) si ha $M \models q = S(y)$ per un opportuno $y \in M$. Poiché $M \models z + S(y) = \overline{n}$, per (Q5) e $\overline{n} = S(\overline{n-1})$ si ha $M \models S(z + y) = S(\overline{n-1})$, da cui $M \models z + y = \overline{n-1}$ per (Q1). Quindi z testimonia che $M \models \varphi_{\leq}[y, \overline{n-1}]$, perciò per ipotesi induttiva $M \models y = \overline{m}$ per qualche $m \leq n - 1$, da cui $M \models q = \overline{m+1}$ per la scelta di y. Essendo $m + 1 \leq n$, la dimostrazione è completa. □

Il Lemma 3.3.14 implica che in qualunque modello M di Q, se un elemento $q \in M$ è minore o uguale (nel senso della relazione binaria definita in M da $\varphi_{\leq}$, che non deve necessariamente essere un ordine sui numeri non standard) ad un numero standard $\overline{n}^M$, allora $q = \overline{m}^M$ per qualche $m \leq n$. Dunque l'isomorfismo canonico tra $\mathbb{N}$ e i numeri standard di M preserva anche l'ordine $\leq$ (il cui corrispettivo in M è la restrizione ai numeri standard di M della relazione binaria su M definita dalla formula $\varphi_{\leq}(x, y)$).

Dal Lemma 3.3.14 segue anche segue

Corollario 3.3.15 ([AB18, Corollario 15.34], cfr. anche [AB18, Lemma 19.30])**.** *Sia $n \in \mathbb{N}$ e $\varphi(x)$ una L_Q-formula. Allora sono equivalenti:*

(1) $Q \vdash \varphi(\overline{a})$ *per ogni* $a \leq n$

(2) $Q \vdash \forall x \leq \overline{n}\, \varphi(x)$.

Similmente si ottiene l'analogo risultato per la quantificazione esistenziale limitata.

Osservazione 3.3.16. Come per tutti i risultati di questa sezione, il Corollario 3.3.15 continua a valere se sostituiamo Q con qualsiasi teoria $T \supseteq Q$ poiché in questo caso

$$T \supseteq Q \vdash \forall x\,(\varphi_{\leq}(x, \overline{n}) \leftrightarrow x = \overline{0} \vee x = \overline{1} \vee \ldots \vee x = \overline{n}).$$

Questo fatto, del tutto ovvio, viene sottolineato esplicitamente poiché verrà utilizzato nella dimostrazione del Teorema 4.2.14.

Lemma 3.3.17 ([AB18, Lemma 15.35])**.** *La formula $\varphi_{\leq}(x, y)$ rappresenta la relazione $\leq \subseteq \mathbb{N}^2$ in Q.*

[6] Essenzialmente, la condizione espressa in questo lemma corrisponde, nella terminologia di [AA19], al fatto che la teoria Q sia *order adequate with respect to* $\varphi_{\leq}(x, y)$. Il lemma compare dunque in quelle note come Teorema 19.32.

Dimostrazione. Siano $a, b \in \mathbb{N}$. Se $a \leq b$, allora $Q \vdash \overline{a} = \overline{0} \vee \ldots \vee \overline{a} = \overline{b}$: infatti $Q \vdash \forall x\,(x = x)$, e nella disgiunzione compare la formula atomica $\overline{a} = \overline{a}$ poiché $a \leq b$. Quindi $Q \vdash \varphi_{\leq}(\overline{a}, \overline{b})$ per il Lemma 3.3.14. Se invece $a \not\leq b$, ovvero $b < a$, allora $a \neq m$ per ogni $m \leq b$. Per il Lemma 3.3.11 si ha allora $Q \vdash \neg(\overline{a} = \overline{0}) \wedge \ldots \wedge \neg(\overline{a} = \overline{b})$, da cui $Q \vdash \neg\varphi_{\leq}(\overline{a}, \overline{b})$ per il Lemma 3.3.14. $\square$

Osservazione 3.3.18. Come osservato nell'Esempio 2.1.5, la formula $\varphi_{\leq}(x, y)$ (ovvero $\exists z\,(z + x = y)$) è logicamente equivalente alla Δ_0-formula $\varphi'_{\leq}(x, y)$

$$\exists w \leq y\,(x = w).$$

Quindi anche $\varphi'_{\leq}(x, y)$ rappresenta $\leq$ in Q.

Lemma 3.3.19 ([AB18, Lemma 15.35])**.** *Per ogni $b \in \mathbb{N}$*

$$Q \vdash \forall x\,(\varphi_{\leq}(x, \overline{b}) \vee \varphi_{\leq}(\overline{b}, x)).$$

Dimostrazione. Fissiamo un modello $M \models Q$ e dimostriamo per induzione su $b \in \mathbb{N}$ che per qualunque $q \in M$

$$M \models \varphi_{\leq}[q, \overline{b}] \vee \varphi_{\leq}[\overline{b}, q].$$

Se $b = 0$, allora $M \models q + \overline{0} = q$ per (Q4), quindi q stesso testimonia $M \models \varphi_{\leq}[\overline{b}, q]$, da cui segue il risultato desiderato.

Se $b > 0$ distinguiamo due casi. Se $M \models q = \overline{0}$, allora $\overline{b}$ testimonia che $M \models \varphi_{\leq}[q, \overline{b}]$ per (Q4). Altrimenti per (Q3) si ha che $M \models q = S(y)$ per un opportuno $y \in M$. Per ipotesi induttiva, $M \models \varphi_{\leq}[y, \overline{b-1}]$ oppure $M \models \varphi_{\leq}[\overline{b-1}, y]$. Nel primo caso, $M \models z + y = \overline{b-1}$ per un opportuno $z \in M$, da cui $M \models z + q = \overline{b}$ per (Q5), ovvero z testimonia $M \models \varphi_{\leq}[q, \overline{b}]$. Nel secondo caso, esiste $z \in M$ tale che $M \models z + \overline{b-1} = y$, da cui $M \models z + \overline{b} = q$ per (Q5) e quindi $M \models \varphi_{\leq}[\overline{b}, q]$. In ogni caso $M \models \varphi_{\leq}[q, \overline{b}] \vee \varphi_{\leq}[\overline{b}, q]$, come desiderato. $\square$

Corollario 3.3.20. *Per ogni $M \models Q$ ed ogni $q \in M$, se q è nonstandard allora q è strettamente maggiore (nel senso della relazione definita in M da $\varphi_{\leq}$) di qualunque numero standard.*

In ogni modello nonstandard M di Q in cui $S^M(q) \neq q$ per ogni $q \in M$, la relazione definita da $\varphi_{\leq}$ è mal fondata: se $q \in M$ è un numero nonstandard (in particolare, $q \neq 0^M$) deve avere un predecessore $q - 1$, ovvero un numero in M tale che $S^M(q - 1) = q$. Tale numero è certamente nonstandard, altrimenti anche q sarebbe standard. Ripetendo il ragionamento, si trovano ricorsivamente i numeri nonstandard $q-1, q-2, q-3, \ldots$ (dove $q-(i+1) \in M$ è tale che $S^M(q-(i+1)) = q-i$, da cui $q - (i + 1) \neq q - i$), per i quali si verifica che $M \models \varphi_{\leq}[q - (i + 1), q - i]$. Tuttavia, abbiamo il seguente risultato:

Lemma 3.3.21 ([AB18, Lemma 15.37])**.** *Sia M un modello di Q e sia $A \subseteq M$ un sottoinsieme di M contenente un numero standard $\overline{n}^M$. Allora esiste un numero standard $\overline{m}^M$ con $m \leq n$ che è un minimo di A, ovvero tale che per ogni $q \in A$ si ha $M \models \varphi_{\leq}[\overline{m}, q]$.*

Dimostrazione. Sia $A' = \{r \in A \mid M \models \varphi_{\leq}[r, \overline{n}]\}$. Per il Lemma 3.3.14, $A' \subseteq \{\overline{m}^M \mid m \leq n\}$: sia $m \leq n$ minimo tale che $\overline{m}^M \in A'$. Sia ora q un arbitrario elemento di A. Per il Lemma 3.3.19, $M \models \varphi_{\leq}[q, \overline{m}]$ oppure $M \models \varphi_{\leq}[\overline{m}, q]$. Ma nel primo caso $q = \overline{m'}^M$ per qualche $m' \leq m \leq n$ per il Lemma 3.3.14, quindi $M \models \varphi_{\leq}(\overline{m'}, \overline{n})$ per il Lemma 3.3.17. Poiché $\overline{m'}^M = q \in A$, segue $\overline{m'}^M \in A'$ e quindi $m \leq m'$ per minimalità di m. Ma allora $m' = m$ e quindi $q = \overline{m}^M$, da cui segue che $M \models \varphi_{\leq}[\overline{m}, q]$ per il Lemma 3.3.17. In ogni caso si ha quindi $M \models \varphi_{\leq}[\overline{m}, q]$ e la dimostrazione è conclusa. $\square$

Il teorema seguente può essere visto come un rafforzamento del Teorema 2.2.8 poiché si riferisce alla rappresentabilità nella teoria Q e non solo alla definibilità nel modello standard di Q.

Teorema 3.3.22 ([AA19, Theorem 19.31], cfr. anche [AB18, Teorema 15.47]). *Ogni funzione ricorsiva totale è rappresentata in Q da una formula Σ_1.*

Dimostrazione. Per la Proposizione 2.2.1, è sufficientemente dimostrare che

- le funzioni U_i^k, $+$, $\cdot$, $\chi_\leq$ sono rappresentate in Q da formule Σ_1;
- la collezione delle funzioni totali rappresentabili in Q da formule Σ_1 è chiusa per composizione e minimizzazione (applicata a funzioni totali).

Per il primo punto basta osservare che ciascuna U_i^k è rappresentata in Q dalla Δ_0-formula $\varphi_i^k(x_1, \ldots, x_k, y)$

$$x_1 = x_1 \land \ldots \land x_k = x_k \land y = x_i.$$

La somma e il prodotto sono rappresentate dalle corrispondenti formule atomiche per il Lemma 3.3.8. La relazione binaria $\leq$ è rappresentata dalla Δ_0-formula $\varphi'_\leq$ per il Lemma 3.3.17 e l'Osservazione 3.3.18, per cui anche $\chi_\leq$ è rappresentabile in Q da una Δ_0-formula per il Lemma 3.3.6.

Passiamo alla chiusura per composizione. Se la Σ_1-formula $\varphi(z_1, \ldots, z_k, y)$ rappresenta in Q una funzione k-aria H e le Σ_1-formule $\psi_i(x_1, \ldots, x_\ell, z_i)$ rappresentano in Q funzioni ℓ-arie G_i (con $1 \leq i \leq k$), allora la Σ_1-formula $\rho(x_1, \ldots, x_\ell, y)$

$$\exists z_1 \ldots \exists z_k \left(\varphi(z_1, \ldots, z_k, y) \land \bigwedge_{1 \leq i \leq k} \psi_i(x_1, \ldots, x_\ell, z_i) \right)$$

rappresenta la funzione

$$F \colon \mathbb{N}^\ell \to \mathbb{N} \colon (a_1, \ldots, a_\ell) \mapsto H(G_1(a_1, \ldots, a_\ell), \ldots, G_k(a_1, \ldots, a_\ell)).$$

Infatti, fissiamo $a_1, \ldots, a_\ell \in \mathbb{N}$ e sia $b = F(a_1, \ldots, a_\ell)$ e $c_i = G_i(a_1, \ldots, a_\ell)$. Allora

$$Q \vdash \rho(\overline{a_1}, \ldots, \overline{a_\ell}, \overline{b})$$

poiché $Q \vdash \psi_i(\overline{a_1}, \ldots, \overline{a_\ell}, \overline{c_i})$ per ogni $1 \leq i \leq k$ e $Q \vdash \varphi(\overline{c_1}, \ldots, \overline{c_k}, \overline{b})$. Questo mostra in particolare che

$$Q \vdash \forall y \, [y = \overline{b} \to \rho(\overline{a_1}, \ldots, \overline{a_\ell}, y)].$$

Viceversa, lavoriamo in un arbitrario modello M di Q e supponiamo che $M \models \rho[\overline{a_1}, \ldots, \overline{a_\ell}, q]$ per qualche $q \in M$. Allora devono esistere $r_1, \ldots, r_k \in M$ tali che $M \models \psi_i[\overline{a_1}, \ldots, \overline{a_\ell}, r_i]$ per ogni $1 \leq i \leq k$ e $M \models \varphi[r_1, \ldots, r_k, q]$. Ma per definizione di rappresentabilità, si deve allora avere $r_i = \overline{c_i}^M$, da cui anche $q = \overline{b}^M$. Per l'arbitrarietà di $q \in M$ si ha dunque

$$M \models \forall y \, [\rho(\overline{a_1}, \ldots, \overline{a_\ell}, y) \to y = \overline{b}],$$

da cui

$$Q \vdash \forall y \, [\rho(\overline{a_1}, \ldots, \overline{a_\ell}, y) \to y = \overline{b}].$$

per l'arbitrarietà di M (ed il teorema di completezza).

Infine consideriamo la chiusura per l'operatore μ. Se la Σ_1-formula $\psi(x_1, \ldots, x_k, z, w)$ rappresenta in Q la funzione totale $H \colon \mathbb{N}^{k+1} \to \mathbb{N}$, allora la funzione

$$F \colon \mathbb{N}^k \to \mathbb{N} \colon (a_1, \ldots, a_k) \mapsto \mu z \, (H(a_1, \ldots, a_k, z) = 0)$$

è rappresentata in Q dalla Σ_1-formula $\varphi(x_1,\ldots,x_k,y)$

$$\psi(x_1,\ldots,x_k,y,\overline{0}) \wedge \forall z \leq y\,[z = y \vee \exists w\,(\psi(x_1,\ldots,x_k,z,w) \wedge \neg(w = \overline{0}))].$$

Infatti, fissiamo $a_1,\ldots,a_k \in \mathbb{N}$ e sia[7] $b = F(a_1,\ldots,a_k)$, cosicché $H(a_1,\ldots,a_k,b) = 0$ e $H(a_1,\ldots,a_k,c) = d_c$ con $d_c \neq 0$ per ogni $c < b$. Per la scelta di ψ si ha che $Q \vdash \psi(\overline{a_1},\ldots,\overline{a_k},\overline{b},\overline{0})$ e per un arbitrario $c < b$ (usando il Lemma 3.3.11)

$$Q \vdash \psi(\overline{a_1},\ldots,\overline{a_k},\overline{c},\overline{d_c}) \wedge \neg(\overline{d_c} = \overline{0}),$$

da cui

$$Q \vdash \exists w\,(\psi(\overline{a_1},\ldots,\overline{a_k},\overline{c},w) \wedge \neg(w = \overline{0}))$$

e per il Lemma 3.3.15

$$Q \vdash \forall z \leq \overline{b}\,[z = \overline{b} \vee \exists w\,(\psi(\overline{a_1},\ldots,\overline{a_k},z,w) \wedge \neg(w = \overline{0}))].$$

Quindi $Q \vdash \varphi(\overline{a_1},\ldots,\overline{a_k},\overline{b})$, da cui segue anche

$$Q \models \forall y\,[y = \overline{b} \to \varphi(\overline{a_1},\ldots,\overline{a_k},y)].$$

Viceversa, lavoriamo in un arbitrario modello M di Q e supponiamo che $M \models \varphi[\overline{a_1},\ldots,\overline{a_k},q]$ per qualche $q \in M$. Vogliamo mostrare che $q = \overline{b}^M$: supponiamo per assurdo che questo non valga.

Claim 3.3.22.1. *Sia $d \in M$ tale che $M \models \varphi[\overline{a_1},\ldots,\overline{a_k},d]$. Se $\overline{c}^M \neq d$ è un numero standard tale che $M \models \varphi_{\leq}[\overline{c},d]$, allora $M \not\models \psi(\overline{a_1},\ldots,\overline{a_k},\overline{c},\overline{0})$.*

Dimostrazione del Claim. Poiché $M \models \varphi[\overline{a_1},\ldots,\overline{a_k},d]$ e $M \not\models \overline{c} = d$ si ha $M \models \exists w\,(\psi(\overline{a_1},\ldots,\overline{a_k},\overline{c},w) \wedge \neg(w = \overline{0}))$: sia $r \in M$ un testimone di ciò. Poiché ψ rappresenta H in Q, da $M \models \psi[\overline{a_1},\ldots,\overline{a_k},\overline{c},r]$ segue $M \models r = \overline{d_c}$ con $d_c = H(a_1,\ldots,a_k,c)$, per cui $M \models \neg(\overline{d_c} = \overline{0})$ dato che $M \models \neg[r = \overline{0}]$. Segue che $M \not\models \psi(\overline{a_1},\ldots,\overline{a_k},\overline{c},\overline{0})$ poiché ψ rappresenta H in Q. □

Si ricordi che, oltre ad avere $M \models \varphi[\overline{a_1},\ldots,\overline{a_k},q]$ per ipotesi, abbiamo già dimostrato $Q \vdash \varphi(\overline{a_1},\ldots,\overline{a_k},\overline{b})$, dunque $M \models \varphi(\overline{a_1},\ldots,\overline{a_k},\overline{b})$. Per il Lemma 3.3.19, $M \models \varphi_{\leq}[q,\overline{b}]$ oppure $M \models \varphi_{\leq}[\overline{b},q]$. Nel secondo caso, poiché per assurdo abbiamo assunto che $q \neq \overline{b}^M$ per il Claim 3.3.22.1 applicato con $d = q$ e $\overline{c} = \overline{b}$ si avrebbe $M \not\models \psi(\overline{a_1},\ldots,\overline{a_k},\overline{b},\overline{0})$, contraddicendo $M \models \varphi(\overline{a_1},\ldots,\overline{a_k},\overline{b})$. Dunque $M \models \varphi_{\leq}[q,\overline{b}]$, per cui $q = \overline{c}^M$ per qualche $c \leq b$ per il Lemma 3.3.14. Poiché per assurdo abbiamo assunto che $\overline{c}^M = q \neq \overline{b}^M$, applicando nuovamente il Claim 3.3.22.1 con $d = \overline{b}^M$ si avrebbe $M \not\models \psi[\overline{a_1},\ldots,\overline{a_k},q,\overline{0}]$, contraddicendo $M \models \varphi[\overline{a_1},\ldots,\overline{a_k},q]$. In entrambi i casi abbiamo raggiunto una contraddizione, quindi concludiamo che si deve avere $M \models q = \overline{b}$. Per l'arbitrarietà di $q \in M$ si ha

$$M \models \forall y\,[\varphi(\overline{a_1},\ldots,\overline{a_k},y) \to y = \overline{b}],$$

da cui

$$Q \vdash \forall y\,[\varphi(\overline{a_1},\ldots,\overline{a_k},y) \to y = \overline{b}].$$

per l'arbitrarietà di M (ed il teorema di completezza). □

Corollario 3.3.23. *Sia $L \supseteq L_Q$ un linguaggio del prim'ordine e T una L-teoria tale che $T \supseteq Q$.*

[7]Siccome il teorema riguarda solo funzioni *totali*, stiamo implicitamente assumendo che per ogni $a_1,\ldots,a_k \in \mathbb{N}^k$ esista $m \in \mathbb{N}$ tale che $H(a_1,\ldots,a_k,m) = 0$, cosicché esista sempre $b = F(a_1,\ldots,a_k)$ (ovvero la funzione F sia definita sull'intero $\mathbb{N}^k$).

- *Ogni funzione ricorsiva totale è rappresentata in T da una formula Σ_1.*
- *Ogni predicato ricorsivo è rappresentato in T sia da una formula Σ_1 che da una formula Π_1.*

Dimostrazione. Per il primo punto basta applicare il Teorema 3.3.22 e osservare che se una formula rappresenta una funzione (rispettivamente, un predicato) in Q, allora essa rappresenta la stessa funzione (rispettivamente, lo stesso predicato) in qualunque $T \supseteq Q$ poiché se $Q \vdash \varphi$ a maggior ragione $T \vdash \varphi$.

Sia $P \subseteq \mathbb{N}^k$ ricorsivo e $\varphi(x_1, \dots, x_k, y)$ una Σ_1-formula che rappresenta χ_P in T. Allora $\varphi(x_1, \dots, x_k, \overline{1})$ è una Σ_1-formula che rappresenta P in T (utilizziamo qui il fatto che $T \vdash \neg(\overline{0} \doteq \overline{1})$ poiché $T \supseteq Q$). Poiché gli insiemi ricorsivi sono chiusi per complemento, esiste anche Σ_1-formula che rappresenta $\sim P$ in T: la sua negazione sarà allora (logicamente equivalente a) una Π_1-formula che rappresenterà P in T. $\square$

Capitolo 4

Incompletezza e indecidibilità

4.1 Aritmetizzazione della sintassi

Sia
$$L = \mathrm{Rel} \cup \mathrm{Fun} \cup \mathrm{Cost}$$
un linguaggio del prim'ordine (al più) numerabile, dove Rel, Fun e Cost sono gli insiemi di simboli di, rispettivamente, relazione, funzione e costante e $\mathrm{ar}(\cdot)$ è la funzione che associa ad ogni simbolo in $\mathrm{Rel} \cup \mathrm{Fun}$ la sua arietà. Sia inoltre $\mathrm{Vbl} = \{v_i \mid i \in \mathbb{N}\}$ l'insieme delle variabili

Definizione 4.1.1. Una **buona codifica** per L è una codifica ricorsiva dell'insieme $D = L \cup \mathrm{Vbl} \cup \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \exists, \forall, \doteq\}$
$$\#\colon D \to \mathbb{N}$$
tale che

- $\#(v_i) = 2i$ per ogni $v_i \in \mathrm{Vbl}$;
- $\#(\neg) = 1$, $\#(\wedge) = 3$, $\#(\vee) = 5$, $\#(\rightarrow) = 7$, $\#(\leftrightarrow) = 9$, $\#(\exists) = 11$, $\#(\forall) = 13$, $\#(\doteq) = 15$;
- gli insiemi $\#[\mathrm{Rel}]$, $\#[\mathrm{Fun}]$ e $\#[\mathrm{Cost}]$, che verranno denotati nel seguito da $\mathrm{Rel}^{\#}$, $\mathrm{Fun}^{\#}$ e $\mathrm{Cost}^{\#}$, rispettivamente, sono ricorsivi primitivi;
- la funzione $a\colon \mathbb{N} \to \mathbb{N}$ tale che
$$a(n) = \begin{cases} \mathrm{ar}(s) & \text{se } n = \#(s) \text{ per qualche } s \in \mathrm{Rel} \cup \mathrm{Fun} \\ 0 & \text{altrimenti} \end{cases}$$
è ricorsiva primitiva.

È facile vedere che ogni linguaggio al più numerabile ammette una buona codifica.

A partire da $\#$, definiamo poi delle codifiche $\ulcorner t \urcorner$ per gli L-termini t per ricorsione sulla complessità (ovvero per ricorsione sull'altezza $\mathrm{ht}(t)$ di t):

- se t è della forma s per qualche simbolo $s \in \mathrm{Cost} \cup \mathrm{Vbl}$ poniamo $\ulcorner t \urcorner = \langle\!\langle \#(s) \rangle\!\rangle$;
- se t è della forma $f(t_1, \dots, t_k)$ per qualche $f \in \mathrm{Fun}$ con $\mathrm{ar}(f) = k$ poniamo $\ulcorner t \urcorner = \langle\!\langle \#(f), \ulcorner t_1 \urcorner, \dots, \ulcorner t_k \urcorner \rangle\!\rangle$.

Indichiamo con Term l'insieme degli L-termini e con $\mathrm{Term}^\#$ l'insieme delle loro codifiche, ovvero

$$\mathrm{Term}^\# = \{\ulcorner t \urcorner \mid t \in \mathrm{Term}\} \subseteq \mathbb{N}.$$

Chiaramente $0 \notin \mathrm{Term}^\#$ poiché $0 = \langle\!\langle\rangle\!\rangle$ mentre ogni elemento di $\mathrm{Term}^\#$ è per definizione la codifica di una sequenza non vuota. Osserviamo inoltre che per ogni $t, t' \in \mathrm{Term}$ si ha

1. $\mathrm{ht}(t) \leq \ulcorner t \urcorner$;
2. se t' è un sottotermine di t allora $\ulcorner t' \urcorner \leq \ulcorner t \urcorner$;
3. $\ulcorner t \urcorner = \ulcorner t' \urcorner$ se e solo se t e t' sono uguali;
4. se il simbolo s occorre in t allora $\#(s) \leq \ulcorner t \urcorner$.

Proposizione 4.1.2 ([AB18, Lemma 16.3])**.** $\mathrm{Term}^\#$ *è ricorsivo primitivo.*

Dimostrazione. La funzione $f = \chi_{\mathrm{Term}^\#} : \mathbb{N} \to \mathbb{N}$ può essere definita per ricorsione generalizzata ponendo

$$\begin{cases} f(0) = 0 \\ f(n+1) = h(n, f^{\mathrm{m}}(n)) \end{cases}$$

dove $h = \chi_R$ e $R \subseteq \mathbb{N}^2$ è il predicato ricorsivo primitivo seguente:

$$\begin{aligned} R(n,z) \quad \iff \quad & z \in \mathrm{Seq} \wedge \ell(z) = n+1 \wedge n+1 \in \mathrm{Seq} \\ & \wedge \Big[\Big(\ell(n+1) = 1 \wedge (\!(n+1)\!)_0 \in \mathrm{Cost}^\# \cup \mathrm{Vbl}^\# \Big) \\ & \qquad \vee \Big((\!(n+1)\!)_0 \in \mathrm{Fun}^\# \wedge \ell(n+1) = a((\!(n+1)\!)_0) + 1 \\ & \qquad\qquad \wedge \forall 1 \leq i < \ell(n+1) \, [(\!(z)\!)_{(\!(n+1)\!)_i} = 1] \Big) \Big]. \end{aligned}$$

[Si osservi che $\ell(n+1) \geq 1$ poiché $n+1 \neq 0 = \langle\!\langle\rangle\!\rangle$: quindi $(\!(n+1)\!)_i < n+1 = \ell(z)$ e $(\!(z)\!)_{(\!(n+1)\!)_i}$ è dunque l'$(\!(n+1)\!)_i$-esimo elemento della sequenza codificata da z. In particolare, quando $z = f^{\mathrm{m}}(n)$ si ha che $(\!(z)\!)_{(\!(n+1)\!)_i} = f((\!(n+1)\!)_i)$.] $\square$

Definiamo ora delle codifiche $\ulcorner \varphi \urcorner$ per le L-formule φ per ricorsione sulla complessità (ovvero per ricorsione sull'altezza $\mathrm{ht}(\varphi)$ di φ):

- se φ è della forma $t_1 = t_2$ con $t_1, t_2 \in \mathrm{Term}$ poniamo $\ulcorner \varphi \urcorner = \langle\!\langle \#(=), \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle\!\rangle$;
- se φ è della forma $R(t_1, \ldots, t_k)$ per qualche $R \in \mathrm{Rel}$ con $\mathrm{ar}(R) = k$ poniamo $\ulcorner \varphi \urcorner = \langle\!\langle \#(R), \ulcorner t_1 \urcorner, \ldots, \ulcorner t_k \urcorner \rangle\!\rangle$;
- se φ è della forma $\neg\psi$ poniamo $\ulcorner \varphi \urcorner = \langle\!\langle \#(\neg), \ulcorner \psi \urcorner \rangle\!\rangle$;
- se φ è della forma $\psi_1 \square \psi_2$ per qualche $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ poniamo $\ulcorner \varphi \urcorner = \langle\!\langle \#(\square), \ulcorner \psi_1 \urcorner, \ulcorner \psi_2 \urcorner \rangle\!\rangle$;
- se φ è della forma $Qv_i\,\psi$ per qualche $Q \in \{\exists, \forall\}$ e $v_i \in \mathrm{Vbl}$ poniamo $\ulcorner \varphi \urcorner = \langle\!\langle \#(Q), \#(v_i), \ulcorner \psi \urcorner \rangle\!\rangle$.

Indichiamo con Fml l'insieme delle L-formule e con $\mathrm{Fml}^\#$ l'insieme delle loro codifiche, ovvero

$$\mathrm{Fml}^\# = \{\ulcorner \varphi \urcorner \mid \varphi \in \mathrm{Fml}\} \subseteq \mathbb{N}.$$

Chiaramente $0 \notin \mathrm{Fml}^\#$ poiché $0 = \langle\!\langle\rangle\!\rangle$ mentre ogni elemento di $\mathrm{Fml}^\#$ è per definizione la codifica di una sequenza non vuota. Osserviamo inoltre che per ogni $\varphi, \psi \in \mathrm{Fml}$ si ha

1. $\mathrm{ht}(\varphi) \leq \ulcorner\varphi\urcorner$;
2. se ψ è una sottoformula di φ allora $\ulcorner\psi\urcorner \leq \ulcorner\varphi\urcorner$;
3. $\ulcorner\varphi\urcorner = \ulcorner\psi\urcorner$ se e solo se φ e ψ sono uguali;
4. se il simbolo s occorre in φ allora $\#(s) \leq \ulcorner\varphi\urcorner$.

Proposizione 4.1.3 ([AB18, Lemma 16.4])**.** $\mathrm{Fml}^{\#}$ *è ricorsivo primitivo.*

Dimostrazione. La funzione $f = \chi_{\mathrm{Fml}^{\#}} \colon \mathbb{N} \to \mathbb{N}$ può essere definita per ricorsione generalizzata ponendo

$$\begin{cases} f(0) = 0 \\ f(n+1) = h(n, f^{\mathrm{m}}(n)) \end{cases}$$

dove $h = \chi_R$ e $R \subseteq \mathbb{N}^2$ è il predicato ricorsivo primitivo seguente:

$$\begin{aligned} R(n,z) \quad \iff \quad & z \in \mathrm{Seq} \wedge \ell(z) = n+1 \wedge n+1 \in \mathrm{Seq} \\ & \wedge \Big[\Big((\!(n+1)\!)_0 = \#(\doteq) \wedge \ell(n+1) = 3 \\ & \qquad\qquad \wedge (\!(n+1)\!)_1 \in \mathrm{Term}^{\#} \wedge (\!(n+1)\!)_2 \in \mathrm{Term}^{\#} \Big) \\ & \quad \vee \Big((\!(n+1)\!)_0 \in \mathrm{Rel}^{\#} \wedge \ell(n+1) = a((\!(n+1)\!)_0) + 1 \\ & \qquad\qquad \wedge \forall 1 \leq i < \ell(n+1) \left((\!(n+1)\!)_i \in \mathrm{Term}^{\#} \right) \Big) \\ & \quad \vee \Big((\!(n+1)\!)_0 = \#(\neg) \wedge \ell(n+1) = 2 \wedge (\!(z)\!)_{(\!(n+1)\!)_1} = 1 \Big) \\ & \quad \vee \bigvee_{\square \in \{\wedge, \vee, \to, \leftrightarrow\}} \Big((\!(n+1)\!)_0 = \#(\square) \wedge \ell(n+1) = 3 \\ & \qquad\qquad \wedge (\!(z)\!)_{(\!(n+1)\!)_1} = 1 \wedge (\!(z)\!)_{(\!(n+1)\!)_2} = 1 \Big) \\ & \quad \vee \bigvee_{Q \in \{\exists, \forall\}} \Big((\!(n+1)\!)_0 = \#(Q) \wedge \ell(n+1) = 3 \\ & \qquad\qquad \wedge (\!(n+1)\!)_1 \in \mathrm{Vbl}^{\#} \wedge (\!(z)\!)_{(\!(n+1)\!)_2} = 1 \Big) \Big]. \end{aligned}$$

[Si osservi che $\ell(n{+}1) \geq 1$ poiché $n{+}1 \neq 0 = \langle\!\langle\rangle\!\rangle$: quindi $(\!(n{+}1)\!)_i < n{+}1 = \ell(z)$ e $(\!(z)\!)_{(\!(n+1)\!)_i}$ è dunque l'$(\!(n+1)\!)_i$-esimo elemento della sequenza codificata da z. In particolare, quando $z = f^{\mathrm{m}}(n)$ si ha che $(\!(z)\!)_{(\!(n+1)\!)_i} = f((\!(n+1)\!)_i)$.] $\square$

Ricordiamo che dati due termini $s, t \in \mathrm{Term}$ ed una variabile v_i, il termine $s(t/v_i)$ ottenuto sostituendo t a v_i è definito per ricorsione sull'altezza di s come segue:

- se $s = v_i$, allora $s(t/v_i) = t$;
- se $s \in \mathrm{Cost} \cup \mathrm{Vbl}$ ma $s \neq v_i$ allora $s(t/v_i) = s$;
- se $s = f(t_1, \ldots, t_k)$ con $f \in \mathrm{Fun}$ di arietà k e $t_1, \ldots, t_k \in \mathrm{Term}$, allora $s(t/v_i) = f(t_1(t/v_i), \ldots, t_k(t/v_i))$.

Similmente, data una formula $\varphi \in \mathrm{Fml}$, un termine $t \in \mathrm{Term}$ ed una variabile v_i, la formula $\varphi(t/v_i)$ ottenuta sostituendo t ad ogni occorrenza libera[1] di v_i in φ è definita per ricorsione sull'altezza di φ come segue:

[1] Tecnicamente andrebbe qui discussa la questione dell'ammissibilità di una sostituzione (ad esempio, non si può sostituire t a v_i se quest'ultima occorre dentro al raggio d'azione di un quantificatore che agisca su una variabile presente in t). Tuttavia, in ciò che segue effettueremo sostituzioni solo con t termine chiuso, per cui tali sostituzioni saranno sempre ammissibili: per semplicità di esposizione, ometteremo allora di inserire condizioni di ammissibilità nella definizione di $\varphi(t/v_i)$.

- se φ è della forma $t_1 = t_2$ allora $\varphi(t/v_i)$ è $t_1(t/v_i) = t_2(t/v_i)$;
- se φ è della forma $R(t_1, \dots, t_k)$ con $R \in \mathrm{Rel}$ di arietà k e $t_1, \dots, t_k \in \mathrm{Term}$, allora $\varphi(t/v_i)$ è $R(t_1(t/v_i), \dots, t_k(t/v_i))$;
- se φ è della forma $\neg\psi$ allora $\varphi(t/v_i)$ è $\neg\psi(t/v_i)$;
- se φ è della forma $\psi_1 \square \psi_2$ con $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ allora $\varphi(t/v_i)$ è $\psi_1(t/v_i) \square \psi_2(t/v_i)$;
- se φ è della forma $Qv_i\,\psi$ con $Q \in \{\exists, \forall\}$ allora $\varphi(t/v_i)$ è φ stessa;
- se φ è della forma $Qv_j\,\psi$ con $Q \in \{\exists, \forall\}$ e $j \neq i$ allora $\varphi(t/v_i)$ è $Qv_j\,\psi(t/v_i)$.

Proposizione 4.1.4 ([AB18, Lemma 16.5])**.** *Le funzioni* $\mathrm{sub}_{\mathrm{Term}}, \mathrm{sub}_{\mathrm{Fml}} \colon \mathbb{N}^3 \to \mathbb{N}$ *definite da*

$$\mathrm{sub}_{\mathrm{Term}}(n,i,m) = \begin{cases} \ulcorner s(t/v_i) \urcorner & \text{se } n = \ulcorner s \urcorner, m = \ulcorner t \urcorner \in \mathrm{Term}^{\#} \\ 0 & \text{altrimenti} \end{cases}$$

e

$$\mathrm{sub}_{\mathrm{Fml}}(n,i,m) = \begin{cases} \ulcorner \varphi(t/v_i) \urcorner & \text{se } n = \ulcorner \varphi \urcorner \in \mathrm{Fml}^{\#} \text{ e } m = \ulcorner t \urcorner \in \mathrm{Term}^{\#} \\ 0 & \text{altrimenti} \end{cases}$$

sono ricorsive primitive.

Dimostrazione. Definiamo $\mathrm{sub}_{\mathrm{Term}}$ per ricorsione generalizzata sulla prima variabile n, ovvero (ricordando che $0 = \langle\!\langle\rangle\!\rangle \notin \mathrm{Term}^{\#}$) poniamo

$$\begin{cases} \mathrm{sub}_{\mathrm{Term}}(0,i,m) = 0 \\ \mathrm{sub}_{\mathrm{Term}}(n+1,i,m) = h_{\mathrm{Term}}(\mathrm{sub}^{\mathrm{m}}_{\mathrm{Term}}(n,i,m), n, i, m) \end{cases}$$

dove $h_{\mathrm{Term}}(z,n,i,m)$ è definita per casi[2] dalle seguenti clausole:

- se $n+1, m \in \mathrm{Term}^{\#}$ e $\ell(n+1) = 1$ con $n+1 = \langle\!\langle 2i \rangle\!\rangle$ (ovvero $n+1 = \ulcorner v_i \urcorner$), allora $h_{\mathrm{Term}}(z,n,i,m) = m$;
- se $n+1, m \in \mathrm{Term}^{\#}$ e $\ell(n+1) = 1$ ma $n+1 \neq \langle\!\langle 2i \rangle\!\rangle$ (ovvero $n+1 = \ulcorner t \urcorner$ con $t \in \mathrm{Cost} \cup \mathrm{Vbl}$ ma $t \neq v_i$), allora $h_{\mathrm{Term}}(z,n,i,m) = n+1$;
- se $n+1, m \in \mathrm{Term}^{\#}$ e $\ell(n+1) = l > 1$, allora
$$h_{\mathrm{Term}}(z,n,i,m) = \langle\!\langle (\!(n+1)\!)_0, (\!(z)\!)_{(\!(n+1)\!)_1}, \dots, (\!(z)\!)_{(\!(n+1)\!)_{l-1}} \rangle\!\rangle.$$

[Come nelle Proposizioni 4.1.2 e 4.1.3, quando $z = \mathrm{sub}^{\mathrm{m}}_{\mathrm{Term}}(n,i,m)$ si ha che $z \in \mathrm{Seq}$ e $\ell(z) = n+1$. Poiché $(\!(n+1)\!)_j < n+1$ si ha che $(\!(z)\!)_{(\!(n+1)\!)_j}$ è l'$(\!(n+1)\!)_j$-esimo elemento di z, ovvero $\mathrm{sub}_{\mathrm{Term}}(j,i,m)$.]

Le condizioni che distinguono i vari casi nella definizione precedente sono ricorsivi primitivi e a due a due disgiunti; inoltre, in ciascuno caso la funzione utilizzata è ricorsiva primitiva. Perciò h_{Term} è ricorsiva primitiva, quindi lo è anche $\mathrm{sub}_{\mathrm{Term}}$.

In maniera analoga, definiamo $\mathrm{sub}_{\mathrm{Fml}}$ per ricorsione generalizzata sulla prima variabile n, ovvero (ricordando che $0 = \langle\!\langle\rangle\!\rangle \notin \mathrm{Fml}^{\#}$) poniamo

$$\begin{cases} \mathrm{sub}_{\mathrm{Fml}}(0,i,m) = 0 \\ \mathrm{sub}_{\mathrm{Fml}}(n+1,i,m) = h_{\mathrm{Fml}}(\mathrm{sub}^{\mathrm{m}}_{\mathrm{Fml}}(n,i,m), n, i, m) \end{cases}$$

dove $h_{\mathrm{Fml}}(z,n,i,m)$ è definita per casi dalle seguenti clausole:

[2] Si ricordi che se un dato argomento non soddisfa nessuna delle condizioni esplicitate in una definizione per casi, il valore della funzione su tale argomento sarà per definizione uguale a 0 (si veda pag. 12).

- se $n+1 \in \mathrm{Fml}^{\#}$, $m \in \mathrm{Term}^{\#}$ e $(\!(n+1)\!)_0 = \#(=)$ allora

  $h_{\mathrm{Fml}}(z,n,i,m) = \langle\!\langle (\!(n{+}1)\!)_0, \mathrm{sub}_{\mathrm{Term}}((\!(n{+}1)\!)_1, i, m), \mathrm{sub}_{\mathrm{Term}}((\!(n{+}1)\!)_2, i, m) \rangle\!\rangle;$

- se $n+1 \in \mathrm{Fml}^{\#}$, $m \in \mathrm{Term}^{\#}$ e $(\!(n+1)\!)_0 \in \mathrm{Rel}^{\#}$, posto $k = a((\!(n+1)\!)_0) = \ell(n+1) - 1$ definiamo

  $h_{\mathrm{Fml}}(z,n,i,m) = \langle\!\langle (\!(n{+}1)\!)_0, \mathrm{sub}_{\mathrm{Term}}((\!(n{+}1)\!)_1, i, m), \dots, \mathrm{sub}_{\mathrm{Term}}((\!(n{+}1)\!)_k, i, m) \rangle\!\rangle;$

- se $n+1 \in \mathrm{Fml}^{\#}$, $m \in \mathrm{Term}^{\#}$ e $(\!(n+1)\!)_0 = \#(\neg)$ allora

$$h_{\mathrm{Fml}}(z,n,i,m) = \langle\!\langle (\!(n+1)\!)_0, (\!(z)\!)_{(\!(n+1)\!)_1} \rangle\!\rangle;$$

- se $n{+}1 \in \mathrm{Fml}^{\#}$, $m \in \mathrm{Term}^{\#}$ e $(\!(n{+}1)\!)_0 = \#(\square)$ per qualche $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ allora

$$h_{\mathrm{Fml}}(z,n,i,m) = \langle\!\langle (\!(n+1)\!)_0, (\!(z)\!)_{(\!(n+1)\!)_1}, (\!(z)\!)_{(\!(n+1)\!)_2} \rangle\!\rangle;$$

- se $n+1 \in \mathrm{Fml}^{\#}$, $m \in \mathrm{Term}^{\#}$, $(\!(n+1)\!)_0 = \#(Q)$ per qualche $Q \in \{\exists, \forall\}$ e $(\!(n{+}1)\!)_1 = \#(v_i)$ allora $h_{\mathrm{Fml}}(z,n,i,m) = n{+}1$; se $n{+}1 \in \mathrm{Fml}^{\#}$, $m \in \mathrm{Term}^{\#}$, $(\!(n+1)\!)_0 = \#(Q)$ per qualche $Q \in \{\exists, \forall\}$ e $(\!(n+1)\!)_1 = \#(v_j)$ per qualche $j \neq i$ allora

$$h_{\mathrm{Fml}}(z,n,i,m) = \langle\!\langle (\!(n+1)\!)_0, (\!(n+1)\!)_1, (\!(z)\!)_{(\!(n+1)\!)_2} \rangle\!\rangle.$$

Argomentando come nel caso di $\mathrm{sub}_{\mathrm{Term}}$ si dimostra che la definizione data è corretta e che $\mathrm{sub}_{\mathrm{Fml}}$ è ricorsiva primitiva poiché h_{Fml} lo è. □

In maniera analoga si può ad esempio dimostrare che i predicati

$$\begin{aligned}
\mathrm{Free}^{\#}_{\mathrm{Term}} &= \{(i, \ulcorner t \urcorner) \mid v_i \text{ occorre (libera) nel termine } t\} \\
\mathrm{Free}^{\#}_{\mathrm{Fml}} &= \{(i, \ulcorner \varphi \urcorner) \mid v_i \text{ occorre libera nella formula } \varphi\}
\end{aligned}$$

sono ricorsivi primitivi, per cui risulta ricorsivo primitivo anche l'insieme

$$\mathrm{Enun}^{\#} = \{\ulcorner \sigma \urcorner \mid \sigma \text{ è un enunciato}\}$$

delle codifiche degli enunciati poiché

$$\mathrm{Enun}^{\#}(n) \iff \mathrm{Fml}^{\#}(n) \wedge \neg \exists i \leq n\, \mathrm{Free}^{\#}_{\mathrm{Fml}}(i, n).$$

(Si ricordi che se v_i occorre in φ allora $i \leq 2i = \#(v_i) \leq \ulcorner \varphi \urcorner$.)

Data una teoria del prim'ordine T (in un linguaggio L al più numerabile), indichiamo con

$$\mathrm{Teor}_T = \{\varphi \mid T \models \varphi\}$$

l'insieme delle conseguenze logiche (ovvero dei teoremi) di T e con

$$\mathrm{Teor}^{\#}_T = \{\ulcorner \varphi \urcorner \mid \varphi \in \mathrm{Teor}_T\}$$

la sua controparte mediante una buona codifica per L. Un insieme di enunciati $\mathrm{Ax}(T)$ si dice **sistema di assiomi** per T se $\mathrm{Teor}_T = \mathrm{Teor}_{\mathrm{Ax}(T)}$. Se $\mathrm{Ax}(T)$ è un sistema di assiomi per T, denotiamo con $\mathrm{Ax}^{\#}(T)$ l'insieme delle codifiche degli enunciati in $\mathrm{Ax}(T)$, ovvero

$$\mathrm{Ax}^{\#}(T) = \{\ulcorner \varphi \urcorner \mid \varphi \in \mathrm{Ax}(T)\}.$$

Definizione 4.1.5. Una teoria T si dice **ricorsivamente assiomatizzabile** se ammette un sistema di assiomi $\mathrm{Ax}(T)$ con $\mathrm{Ax}^{\#}(T)$ ricorsivo.

Vogliamo ora osservare che anche le dimostrazioni a partire dagli assiomi in $\mathrm{Ax}(T)$ possono essere codificate in maniera ricorsiva come opportuni numeri naturali. Per far ciò è necessario fissare un calcolo logico (con un numero finito di regole di deduzione) corretto e completo che sia "ricorsivo" nel senso seguente:

- l'insieme LogAx dei suoi assiomi logici deve essere tale che $\mathrm{LogAx}^{\#} = \{\ulcorner \varphi \urcorner \mid \varphi \in \mathrm{LogAx}\}$ sia ricorsivo;
- per ogni regola di deduzione γ con n premesse, il predicato
$$R^{\#}_{\gamma} = \{(\ulcorner \varphi_1 \urcorner, \dots, \ulcorner \varphi_n \urcorner, \ulcorner \psi \urcorner) \in (\mathrm{Fml}^{\#})^{n+1} \mid \psi \text{ si deduce da } \varphi_1, \dots, \varphi_n \text{ mediante la regola } \gamma\}$$
deve essere ricorsivo.

Tutti i calcoli logici più comuni sono sia completi che "ricorsivi" nel senso appena descritto, ma per fissare le idee possiamo pensare ad un sistema alla Hilbert-Ackermann, che prevede come unica regola di deduzione il *Modus Ponens*
$$\frac{\varphi \qquad \varphi \to \psi}{\psi} \tag{MP}$$
e il cui sistema di (infiniti) assiomi logici ha codifica $\mathrm{LogAx}^{\#}$ ricorsiva. In questo caso, si ha che
$$R^{\#}_{(\mathrm{MP})} = \{(n, m, k) \in \mathbb{N}^3 \mid n, m, k \in \mathrm{Fml}^{\#} \wedge m = \langle\!\langle \#(\to), n, k \rangle\!\rangle\}$$
In questo modo una dimostrazione di φ a partire da(gli assiomi di) T è una lista finita $\sigma \in (\mathrm{Fml})^{<\mathbb{N}}$ di formule, l'ultima delle quali è proprio φ e in cui ciascuna delle formule è un assioma logico, un assioma di T oppure è ottenuta da formule precedenti mediante la regola (MP). Più precisamente, dato un sistema di assiomi $\mathrm{Ax}(T)$ per T definiamo il predicato $\mathrm{Prov}_{\mathrm{Ax}(T)}$ come l'insieme delle coppie $(\sigma, \varphi) \in (\mathrm{Fml})^{<\mathbb{N}} \times \mathrm{Fml}$ tale che $\sigma = (\sigma_0, \dots, \sigma_{k-1})$ è una dimostrazione di φ a partire da $\mathrm{Ax}(T)$, ovvero

- $\mathrm{lh}(\sigma) = k \geq 1$ e $\sigma_{k-1} = \varphi$;
- per ogni $i < k$, $\sigma_i \in \mathrm{LogAx} \cup \mathrm{Ax}(T)$ oppure esistono $j_1, j_2 < i$ tali che σ_i si ottiene da σ_{j_1} e σ_{j_2} mediante (MP).

Codificando tutto nei numeri naturali si ottiene il predicato $\mathrm{Prov}^{\#}_{\mathrm{Ax}(T)} \subseteq \mathbb{N}^2$ definito da
$$\begin{aligned}\mathrm{Prov}^{\#}_{\mathrm{Ax}(T)}(n, m) \iff \; & m \in \mathrm{Fml}^{\#} \wedge n \in \mathrm{Seq} \wedge \ell(n) \geq 1 \wedge (\!(n)\!)_{\ell(n)-1} = m \\ & \wedge \forall i < \ell(n) \Big((\!(n)\!)_i \in \mathrm{LogAx}^{\#} \cup \mathrm{Ax}^{\#}(T) \\ & \vee \exists j_1 < i \, \exists j_2 < i \left(R^{\#}_{(\mathrm{MP})}((\!(n)\!)_{j_1}, (\!(n)\!)_{j_2}, (\!(n)\!)_i) \right)\Big).\end{aligned}$$

Si osservi che poiché il calcolo logico scelto è corretto e completo si ha anche
$$\mathrm{Teor}^{\#}_{T}(m) \iff \exists n \, \mathrm{Prov}^{\#}_{\mathrm{Ax}(T)}(n, m).$$

Dalle definizioni appena date risulta evidente che

Proposizione 4.1.6 ([AB18, Teorema 16.7])**.**

- *Se* $\mathrm{Ax}^{\#}(T)$ *è (semi)ricorsivo, anche* $\mathrm{Prov}^{\#}_{\mathrm{Ax}(T)}$ *lo è.*
- *Se* T *è ricorsivamente assiomatizzabile allora* $\mathrm{Teor}^{\#}_{T}$ *è semiricorsivo.*

4.2 Il primo teorema di incompletezza di Gödel

Fissiamo una buona codifica $\#$ per il linguaggio $L_Q = \{+, \cdot, S, 0\}$.

Lemma 4.2.1 ([AB18, Lemma 16.12])**.** *La funzione*

$$\mathrm{num}\colon \mathbb{N} \to \mathbb{N}\colon n \mapsto \ulcorner \overline{n} \urcorner$$

è ricorsiva primitiva.

Dimostrazione.

$$\begin{cases} \mathrm{num}(0) = \langle\!\langle \#(0) \rangle\!\rangle \\ \mathrm{num}(n+1) = \langle\!\langle \#(S), \mathrm{num}(n) \rangle\!\rangle. \end{cases} \qquad \square$$

Lemma 4.2.2 ([AB18, Lemma 16.13])**.** *Esiste una funzione ricorsiva primitiva $D\colon \mathbb{N} \to \mathbb{N}$ tale che per ogni L_Q-formula $\rho(v_0)$*

$$D(\ulcorner \rho \urcorner) = \ulcorner \rho(\overline{\ulcorner \rho \urcorner}/v_0) \urcorner.$$

Dimostrazione.

$$D(x) = \mathrm{sub}_{\mathrm{Fml}}(x, 0, \mathrm{num}(x)). \qquad \square$$

Il seguente lemma di diagonalizzazione sarà al centro di tutti i risultati principali di questo capitolo.

Lemma 4.2.3 ([AB18, Lemma 16.14])**.** *Per ogni L_Q-formula $\varphi(v_i)$ con v_i libera in φ esiste un L_Q-enunciato σ tale che*

$$Q \vdash \sigma \leftrightarrow \varphi(\overline{\ulcorner \sigma \urcorner}/v_i).$$

Dimostrazione. Sia $\psi(x, y)$ una (Σ_1-)formula che rappresenta in Q la funzione D del Lemma 4.2.2. Senza perdere generalità, possiamo assumere che $i \neq 0$ e che v_0, v_i non occorrano in ψ (altrimenti basta procedere con un'opportuna rinomina delle variabili).

Sia $\rho(v_0)$ la formula

$$\forall v_i\, (\psi(v_0, v_i) \to \varphi(v_i))$$

e σ l'enunciato

$$\rho(\overline{\ulcorner \rho \urcorner}/v_0), \tag{4.1}$$

ovvero

$$\forall v_i\, (\psi(\overline{\ulcorner \rho \urcorner}, v_i) \to \varphi(v_i)). \tag{4.2}$$

Supponiamo innanzitutto che $Q \vdash \sigma$. Poiché ψ rappresenta D in Q e $D(\ulcorner \rho \urcorner) = \ulcorner \rho(\overline{\ulcorner \rho \urcorner}/v_0) \urcorner$ si ha

$$Q \vdash \psi\left(\overline{\ulcorner \rho \urcorner}, \overline{\ulcorner \rho(\overline{\ulcorner \rho \urcorner}/v_0) \urcorner}\right).$$

Per (4.2), istanziando v_i con $\overline{\ulcorner \rho(\overline{\ulcorner \rho \urcorner}/v_0) \urcorner}$ si ha per Modus Ponens che

$$Q \vdash \varphi\left(\overline{\ulcorner \rho(\overline{\ulcorner \rho \urcorner}/v_0) \urcorner}/v_i\right),$$

ovvero per la definizione di σ in (4.1)

$$Q \vdash \varphi(\overline{\ulcorner \sigma \urcorner}/v_i).$$

Questo dimostra che

$$Q \vdash \sigma \to \varphi(\overline{\ulcorner \sigma \urcorner}/v_i).$$

Viceversa, per dimostrare che $Q \vdash \varphi(\overline{\ulcorner\sigma\urcorner}/v_i) \to \sigma$ mostriamo che in un arbitrario modello M di Q si ha che

$$\text{se } M \models \varphi(\overline{\ulcorner\sigma\urcorner}/v_i) \text{ allora } M \models \sigma.$$

Assumiamo dunque che

$$M \models \varphi(\overline{\ulcorner\sigma\urcorner}/v_i) \tag{4.3}$$

e dimostriamo innanzitutto che per ogni $q \in M$

$$M \models \psi[\overline{\ulcorner\rho\urcorner}, q] \to \varphi[q]. \tag{4.4}$$

Poiché ψ rappresenta D in Q e $M \models Q$, se $M \models \psi[\overline{\ulcorner\rho\urcorner}, q]$ si deve necessariamente avere (utilizzando nuovamente la definizione di σ in (4.1) per l'ultima uguaglianza)

$$q = \overline{D(\ulcorner\rho\urcorner)}^M = \overline{\ulcorner\rho(\overline{\ulcorner\rho\urcorner}/v_0)\urcorner}^M = \overline{\ulcorner\sigma\urcorner}^M$$

Per (4.3), si ha dunque $M \models \varphi[q]$ come desiderato.

Per l'arbitrarietà di $q \in M$ in (4.4) si ha ora che (4.2) è vera in M, ovvero $M \models \sigma$, che è ciò che dovevamo dimostrare. □

Osservazione 4.2.4. Se φ è una Π_1-formula, anche l'enunciato σ ottenuto nella precedente dimostrazione è Π_1.

Da ora in poi fissiamo un linguaggio del prim'ordine $L \supseteq L_Q$ al più numerabile ed una buona codifica # per L che estenda quella di L_Q (questo si può certamente fare poiché L_Q è finito).

Definizione 4.2.5. Una L-teoria T si dice **coerente** se non esiste una L-formula φ tale che $T \vdash \varphi \wedge \neg\varphi$ ed **incoerente** altrimenti.

Una L-teoria T si dice ω**-coerente** se non esiste una L-formula $\varphi(x)$ tale che $T \vdash \exists x\, \varphi(x)$ ma, al tempo stesso, $T \vdash \neg\varphi(\overline{n})$ per ogni $n \in \mathbb{N}$.

Si noti che se T è ω-coerente allora è anche coerente, poiché se fosse incoerente dimostrerebbe qualunque formula, incluse tutte quelle coinvolte nella definizione di ω-coerenza (per un φ arbitraria). Ci sono invece teorie che sono coerenti ma non ω-coerenti. Si osservi anche che se T ammette un modello standard (ovvero un L-modello che espanda il modello standard dell'aritmetica $\langle \mathbb{N}, +, \cdot, S, 0\rangle$ al linguaggio L di T) allora è anche ω-coerente.

Proposizione 4.2.6 (cfr. [AB18, Osservazione 16.19] per il secondo punto)**.**

(1) Siano $P \subseteq \mathbb{N}$ ed $R \subseteq \mathbb{N}^2$ tali che $P(x) \Longleftrightarrow \exists y\, R(x, y)$ con R ricorsivo. Sia $\psi(x, y)$ una formula che rappresenta R in una L-teoria T.

- *Se $n \in P$ allora $T \vdash \exists y\, \psi(\overline{n}, y)$.*
- *Se T è ω-coerente vale anche il viceversa, ovvero se per qualche $n \in \mathbb{N}$ vale $T \vdash \exists y\, \psi(\overline{n}, y)$ allora $n \in P$.*

(2) Similmente, se $\varphi(x)$ rappresenta un predicato $P \subseteq \mathbb{N}$ in una L-teoria ω-coerente T e σ è l'enunciato $\exists x\, \varphi(x)$, allora $T \vdash \sigma$ se e solo se σ è vero in $\mathbb{N}$, ovvero se e solo se $P \neq \emptyset$.

Dimostrazione. (1) Se $n \in P$ allora $R(n, m)$ per qualche $m \in \mathbb{N}$. Poiché ψ rappresenta R in T, si ha $T \vdash \psi(\overline{n}, \overline{m})$, da cui $T \vdash \exists y\, \psi(\overline{n}, y)$.

Viceversa, supponiamo che $T \vdash \exists y\, \psi(\overline{n}, y)$ ma $n \notin P$, ovvero $(n, m) \notin R$ per ogni $m \in \mathbb{N}$. Poiché ψ rappresenta R in T, si avrebbe allora $T \vdash \neg\psi(\overline{n}, \overline{m})$ per ogni $m \in \mathbb{N}$, per cui la formula $\varphi(y)$ data da $\psi(\overline{n}, y)$ testimonierebbe che T non è ω-coerente.

(2) Se σ è vero in $\mathbb{N}$ allora $n \in P$ per qualche $n \in \mathbb{N}$. Come nel punto precedente, si avrebbe allora $T \vdash \varphi(\overline{n})$ e quindi $T \vdash \exists x\, \varphi(x)$, ovvero $T \vdash \sigma$ (per questa direzione non serve assumere che T sia ω-coerente). Viceversa, se σ è falso in $\mathbb{N}$ allora $n \notin P$ per ogni $n \in \mathbb{N}$. Quindi $T \vdash \neg\varphi(\overline{n})$ per ogni $n \in \mathbb{N}$, per cui $T \nvdash \sigma$ poiché altrimenti $\varphi(x)$ violerebbe l'ω-coerenza di T.

□

Definizione 4.2.7. Una teoria T si dice **completa** se per ogni enunciato σ nel suo linguaggio si ha $T \vdash \sigma$ oppure $T \vdash \neg\sigma$. Se ciò non accade, si dice che T è **incompleta**; gli enunciati σ tali che $T \nvdash \sigma$ e $T \nvdash \neg\sigma$ si dicono **indipendenti** da T.

Si noti che poiché lavoriamo sempre con calcoli logici corretti e completi, dimostrare che σ è indipendente da T equivale a trovare due modelli M, N di T tali che $M \models \sigma$ e $N \models \neg\sigma$. Infatti da $M \models T \cup \{\sigma\}$ otteniamo che $T \nvdash \neg\sigma$, mentre da $N \models T \cup \{\neg\sigma\}$ otteniamo che $T \nvdash \sigma$.

Il seguente teorema viene chiamato **Primo teorema di incompletezza di Gödel**.

Teorema 4.2.8 ([AB18, Teorema 16.20])**.** *Sia $T \supseteq Q$ una L-teoria ω-coerente e ricorsivamente assiomatizzabile. Allora T è incompleta.*

Dimostrazione. Sia $\mathrm{Ax}(T)$ un sistema di assiomi per T con $\mathrm{Ax}^{\#}(T) \subseteq \mathbb{N}$ ricorsivo, cosicché $\mathrm{Prov}^{\#}_{\mathrm{Ax}(T)} \subseteq \mathbb{N}^2$ è ricorsivo per la Proposizione 4.1.6. Si ricordi che $\mathrm{Teor}^{\#}_T(m) \iff \exists n\, \mathrm{Prov}^{\#}_{\mathrm{Ax}(T)}(n,m)$. Per il Corollario 3.3.23 esiste una Σ_1-formula $\psi(x,y)$ (nel linguaggio L_Q) che rappresenta $\mathrm{Prov}^{\#}_{\mathrm{Ax}(T)}$ in T. Sia $\varphi(y)$ la L_Q-formula $\neg\exists x\, \psi(x,y)$ (si noti che $\varphi(y)$ è logicamente equivalente ad una formula Π_1) e applichiamo il Lemma 4.2.3 per ottenere un L_Q-enunciato σ_G, anch'esso logicamente equivalente a un Π_1-enunciato, tale che

$$T \supseteq Q \vdash \sigma_G \leftrightarrow \varphi(\overline{\ulcorner \sigma_G \urcorner}/y).$$

Dimostrariamo che $T \nvdash \sigma_G$ e $T \nvdash \neg\sigma_G$ (per cui T è incompleta).

Se per assurdo $T \vdash \sigma_G$, ovvero $\ulcorner \sigma_G \urcorner \in \mathrm{Teor}^{\#}_T$, per la Proposizione 4.2.6(1) si avrebbe

$$T \vdash \exists x\, \psi(x, \overline{\ulcorner \sigma_G \urcorner}),$$

ovvero

$$T \vdash \neg\varphi(\overline{\ulcorner \sigma_G \urcorner}/y),$$

da cui per la scelta di σ_G

$$T \vdash \neg\sigma_G.$$

Quindi T sarebbe incoerente, contraddicendo l'assunzione che T sia invece addirittura ω-coerente.

Il paragrafo precedente dimostra che $\ulcorner \sigma_G \urcorner \notin \mathrm{Teor}^{\#}_T$. Per la Proposizione 4.2.6(1) e l'ω-coerenza di T,

$$T \nvdash \exists x\, \psi(x, \overline{\ulcorner \sigma_G \urcorner}),$$

ovvero $T \nvdash \neg\varphi(\overline{\ulcorner \sigma_G \urcorner}/y)$, da cui $T \nvdash \neg\sigma_G$ per la scelta di σ_G. □

Poiché ogni teoria che ammetta $\mathbb{N}$ come modello è necessariamente ω-coerente, si ottiene:

Corollario 4.2.9 (cfr. [AB18, Teorema 16.15])**.** *Sia T una L-teoria ricorsivamente assiomatizzabile i cui assiomi siano veri in $\mathbb{N}$. Se T dimostra gli assiomi (Q1)–(Q7) di Q (ovvero T dimostra le proprietà di base di somma, prodotto, successore e 0 vere in $\mathbb{N}$), allora T è incompleta. In particolare, l'aritmetica di Peano PA è incompleta.*

Supponiamo che (una qualche espansione de) il modello standard $\langle \mathbb{N}, +, \cdot, S, 0\rangle$ sia un modello di una data teoria $T \supseteq Q$, cosicché, in particolare, T sia ω-coerente. Siano ψ, φ e σ_G come nella precedente dimostrazione. La formula $\psi(x, \overline{\ulcorner \sigma_G \urcorner})$ rappresenta in T il predicato

$$\{m \in \mathbb{N} \mid (m, \ulcorner \sigma_G \urcorner) \in \mathrm{Prov}^{\#}_{\mathrm{Ax}(T)}\},$$

ovvero l'insieme dei codici delle (eventuali) dimostrazioni di σ_G a partire dagli assiomi in $\mathrm{Ax}(T)$. Per la Proposizione 4.2.6(2), $\exists x\, \psi(x, \overline{\ulcorner \sigma_G \urcorner})$ è vero in $\mathbb{N}$ se e solo se $T \vdash \exists x\, \psi(x, \overline{\ulcorner \sigma_G \urcorner})$, ovvero se e solo se $T \vdash \neg\varphi(\overline{\ulcorner \sigma_G \urcorner})$, il che accade se e solo se $T \vdash \neg\sigma_G$. Avendo appena dimostrato che l'ultima affermazione è falsa, abbiamo che in $\mathbb{N}$ è falso $\exists x\, \psi(x, \overline{\ulcorner \sigma_G \urcorner})$, quindi è vero l'enunciato $\varphi(\overline{\ulcorner \sigma_G \urcorner})$. Essendo $\mathbb{N}$ un modello di T, si ha che σ_G è vero in $\mathbb{N}$. Questo mostra che

> Esiste un Π_1-enunciato σ_G (nel linguaggio L_Q) vero in $\mathbb{N}$ che T non è in grado di dimostrare (né, ovviamente, di refutare).

In contrasto a questo fatto si ha che

Proposizione 4.2.10 ([AB18, Lemma 15.43]). *Se σ è un Σ_1-enunciato (nel linguaggio L_Q) vero in $\mathbb{N}$, allora $Q \vdash \sigma$.*

Per dimostrare questo fatto, dimostriamo alcuni risultati preliminari. Diciamo che Q **decide** un enunciato σ se $Q \vdash \sigma$ oppure $Q \vdash \neg\sigma$ (ovvero σ non è indipendente da Q).

Per il Corollario 3.3.13 ogni formula atomica $t_1 = t_2$ con t_1, t_2 termini chiusi è decisa da Q.

Lemma 4.2.11 ([AB18, Lemma 15.38]). *Se Q decide φ e ψ allora decide anche $\varphi \wedge \psi$, $\varphi \vee \psi$ e $\neg\varphi$.*

Dimostrazione. Consideriamo solo il caso di $\varphi \wedge \psi$ (gli altri casi sono simili). Per ipotesi, si possono verificare solamente quattro casi:

- $Q \vdash \varphi$ e $Q \vdash \psi$;
- $Q \vdash \varphi$ e $Q \vdash \neg\psi$;
- $Q \vdash \neg\varphi$ e $Q \vdash \psi$;
- $Q \vdash \neg\varphi$ e $Q \vdash \neg\psi$.

Nel primo caso $Q \vdash \varphi \wedge \psi$, nei restanti tre $Q \vdash \neg(\varphi \wedge \psi)$: quindi in ogni caso Q decide $\varphi \wedge \psi$. □

Più in generale, Q decide ogni combinazione booleana di enunciati che non siano indipendenti da esso.

Lemma 4.2.12 ([AB18, Lemma 15.40]). *Sia t un L_Q-termine chiuso e $\varphi(x)$ una L_Q-formula tale Q decide ciascuno degli enunciati $\varphi(\overline{n})$ per $n \in \mathbb{N}$. Allora Q decide anche gli enunciati $\forall x \leq t\, \varphi(x)$ e $\exists x \leq t\, \varphi(x)$.*

Dimostrazione. Poiché $\exists x \leq t\, \varphi(x)$ è logicamente equivalente a $\neg\forall x \leq t\, \neg\varphi(x)$ basta mostrare che Q decide $\forall x \leq t\, \varphi(x)$. Per il Corollario 3.3.10 esiste $b \in \mathbb{N}$ tale che $Q \vdash t = \overline{b}$. Consideriamo gli enunciati $\varphi(\overline{n})$ con $n \leq b$, che per ipotesi sono tutti decisi da Q. Se $Q \vdash \varphi(\overline{n})$ per ciascuno di tali n, allora $Q \vdash \forall x \leq \overline{b}\, \varphi(x)$ per il Corollario 3.3.15 e quindi $Q \vdash \forall x \leq t\, \varphi(x)$. Se invece $Q \vdash \neg\varphi(\overline{n})$ per qualche $n \leq b$, allora $Q \vdash \exists x \leq \overline{b}\, \neg\varphi(x)$ per il Corollario 3.3.15 e quindi $Q \vdash \neg\forall x \leq t\, \varphi(x)$. □

Per induzione sulla complessità della L_Q-formule si ottiene quindi

Corollario 4.2.13 ([AB18, Corollario 15.41])**.** *La teoria Q decide ogni L_Q-enunciato (logicamente equivalente ad un enunciato) Δ_0.*

Proof of Proposition 4.2.10. Dimostriamo per induzione sulla complessità di una Σ_1-formula $\varphi(x_1,\dots,x_k)$ che per ogni $a_1,\dots,a_k \in \mathbb{N}$, se $\varphi(\overline{a_1},\dots,\overline{a_k})$ è vero in $\mathbb{N}$ allora $Q \vdash \varphi(\overline{a_1},\dots,\overline{a_k})$.

Se φ è Δ_0, allora Q decide $\varphi(\overline{a_1},\dots,\overline{a_k})$: essendo quest'ultimo vero in almeno un modello di Q (il modello standard) per ipotesi, si ha $Q \vdash \varphi(\overline{a_1},\dots,\overline{a_n})$.

Supponiamo ora che φ sia della forma $\psi_1 \wedge \psi_2$. Poiché per ipotesi $\varphi(\overline{a_1},\dots,\overline{a_k})$ è vera in $\mathbb{N}$, lo sono anche $\psi_1(\overline{a_1},\dots,\overline{a_k})$ e $\psi_2(\overline{a_1},\dots,\overline{a_k})$. Per ipotesi induttiva, $Q \vdash \psi_1(\overline{a_1},\dots,\overline{a_k})$ e $Q \vdash \psi_2(\overline{a_1},\dots,\overline{a_k})$, da cui $Q \vdash \varphi(\overline{a_1},\dots,\overline{a_k})$. Il caso della disgiunzione è trattato in maniera analoga.

Supponiamo ora che $\varphi(x_1,\dots,x_k)$ sia della forma $\forall y \leq t\, \psi(x_1,\dots,x_k,y)$, dove $t = t(x_1,\dots,x_k)$ è un L_Q- termine. Supponiamo che $\varphi(\overline{a_1},\dots,\overline{a_k})$ sia vera in $\mathbb{N}$. Per il Corollario 3.3.10 possiamo supporre[3] che il termine chiuso $t(\overline{a_1},\dots,\overline{a_k})$ sia della forma $\overline{b}$ per un opportuno $b \in \mathbb{N}$. Poiché per ipotesi $\varphi(\overline{a_1},\dots,\overline{a_k})$ è vera in $\mathbb{N}$, allora $\psi(\overline{a_1},\dots,\overline{a_k},\overline{m})$ è vera in $\mathbb{N}$ per ogni $m \leq b$. Per ipotesi induttiva, $Q \vdash \psi(\overline{a_1},\dots,\overline{a_k},\overline{m})$ per ogni $m \leq b$, da cui $Q \vdash \forall y \leq \overline{b}\, \psi(\overline{a_1},\dots,\overline{a_k}),y)$ per il Corollario 3.3.15. Il caso della quantificazione esistenziale limitata è simile.

Infine, supponiamo che $\varphi(x_1,\dots,x_k)$ sia della forma $\exists y\, \psi(x_1,\dots,x_k,y)$. Poiché per ipotesi $\varphi(\overline{a_1},\dots,\overline{a_k})$ è vera in $\mathbb{N}$, esiste $b \in \mathbb{N}$ tale che $\psi(\overline{a_1},\dots,\overline{a_k},\overline{b})$ è vera in $\mathbb{N}$. Per ipotesi induttiva $Q \vdash \psi(\overline{a_1},\dots,\overline{a_k},\overline{b})$, da cui $Q \vdash \exists y\, \psi(\overline{a_1},\dots,\overline{a_k},y)$. $\square$

Riassumendo quanto visto fin qui:

- Gli enunciati Σ_1 (quindi anche quelli Δ_0) veri in $\mathbb{N}$ sono dimostrabili in Q.
- Gli enunciati Δ_0 falsi in $\mathbb{N}$ sono refutabili in Q.
- Gli enunciati Σ_1 falsi in $\mathbb{N}$ non sono dimostrabili in Q, ma non è detto che Q li possa refutare (ovvero possono essere indipendenti, come lo è il Σ_1-enunciato $\neg\sigma_G$).
- Sia σ un enunciato tale che $Q \vdash \sigma \leftrightarrow \varphi_1$ e $Q \vdash \sigma \leftrightarrow \varphi_2$ con φ_1 enunciato Σ_1 e φ_2 enunciato Π_1. Per quanto visto finora se σ è vero in $\mathbb{N}$ allora è dimostrabile in Q, mentre se σ è falso in $\mathbb{N}$ allora è refutabile in Q (in particolare Q decide σ, ovvero σ non è indipendente da Q).

Quindi l'enunciato di Gödel ha complessità sintattica minima tra gli enunciati che non sono già decisi dall'aritmetica di Robinson Q.

Rosser dimostrò che l'ipotesi di ω-coerenza nel Primo teorema di incompletezza di Gödel 4.2.8 può essere indebolita come segue.

Teorema 4.2.14 ([AB18, Teorema 16.22])**.** *Ogni teoria $T \supseteq Q$ coerente e ricorsivamente assiomatizzabile è incompleta.*

Una dimostrazione indiretta di questo risultato verrà data nella prossima sezione. Per ottenere esplicitamente un enunciato indipendente da T si può procedere come segue.

Dimostrazione. Sia $\mathrm{Ax}(T)$ un sistema di assiomi per T con $\mathrm{Ax}^{\#}(T)$ ricorsivo. Consideriamo la funzione ricorsiva $f\colon \mathbb{N} \to \mathbb{N}\colon n \mapsto \langle\!\langle \#(\neg), n \rangle\!\rangle$, cosicché $f(\ulcorner \varphi \urcorner) = \ulcorner \neg\varphi \urcorner$ per ogni $\varphi \in \mathrm{Fml}$. Siano $\psi_1(x,y)$ e $\psi_2(x,y)$ due L_Q-formule che rappresentano

[3] Più precisamente, Q dimostra che $\forall y \leq t(\overline{a_1},\dots,\overline{a_k})\, \psi(\overline{a_1},\dots,\overline{a_k},y)$ è logicamente equivalente a $\forall y \leq \overline{b}\, \psi(\overline{a_1},\dots,\overline{a_k},y)$ per qualche $b \in \mathbb{N}$.

in Q (quindi anche in T) i predicati ricorsivi $\mathrm{Prov}^{\#}_{\mathrm{Ax}(T)}(n,m)$ e $\widehat{\mathrm{Prov}}^{\#}_{\mathrm{Ax}(T)}(n,m)$, rispettivamente, dove $\widehat{\mathrm{Prov}}^{\#}_{\mathrm{Ax}(T)}(n,m)$ è definito ponendo

$$\widehat{\mathrm{Prov}}^{\#}_{\mathrm{Ax}(T)}(n,m) \iff \mathrm{Prov}^{\#}_{\mathrm{Ax}(T)}(n,f(m)),$$

rispettivamente. Sia $\varphi(y)$ la L_Q-formula

$$\forall x\,(\psi_1(x,y) \to \exists z \leq x\,\psi_2(z,y))$$

e, utilizzando il Lemma 4.2.3, consideriamo un L_Q-enunciato σ tale che

$$T \supseteq Q \vdash \sigma \leftrightarrow \varphi(\overline{\ulcorner\sigma\urcorner}).$$

(Si osservi che prendendo ψ_1 di complessità Σ_1 e ψ_2 di complessità Π_1, l'enunciato σ diventa logicamente equivalente ad un enunciato Π_1 per l'Osservazione 4.2.4.) Dimostriamo che σ è indipendente da T.

Supponiamo per assurdo che $T \vdash \sigma$ e sia $n \in \mathbb{N}$ tale che $\mathrm{Prov}^{\#}_{\mathrm{Ax}(T)}(n,\ulcorner\sigma\urcorner)$. Per rappresentabilità $T \vdash \psi_1(\overline{n},\overline{\ulcorner\sigma\urcorner})$ da cui per scelta di σ e φ si ha $T \vdash \exists z \leq \overline{n}\,\psi_2(z,\overline{\ulcorner\sigma\urcorner})$. Per il Corollario 3.3.15 (insieme all'Osservazione 3.3.16), si ha che $T \vdash \psi_2(\overline{m},\overline{\ulcorner\sigma\urcorner})$ per qualche $m \leq n$. Allora $(m,\ulcorner\sigma\urcorner) \in \widehat{\mathrm{Prov}}^{\#}_{\mathrm{Ax}(T)}$ poiché in caso contrario $T \vdash \neg\psi_2(\overline{m},\overline{\ulcorner\sigma\urcorner})$ e T sarebbe incoerente. Segue che $\ulcorner\neg\sigma\urcorner = f(\ulcorner\sigma\urcorner) \in \mathrm{Teor}^{\#}_T$, ovvero $T \vdash \neg\sigma$, contro la coerenza di T.

Supponiamo ora che valga $T \vdash \neg\sigma$ e sia $m \in \mathbb{N}$ tale che $\widehat{\mathrm{Prov}}^{\#}_{\mathrm{Ax}(T)}(m,\ulcorner\sigma\urcorner)$. Per rappresentabilità $T \vdash \psi_2(\overline{m},\overline{\ulcorner\sigma\urcorner})$ da cui

$$T \vdash \forall x\,(\varphi_{\leq}(\overline{m},x) \to \exists z \leq x\,(\psi_2(z,\overline{\ulcorner\sigma\urcorner}))). \tag{4.5}$$

D'altra parte, poiché $T \vdash \neg\sigma$ si ha $T \vdash \neg\varphi(\overline{\ulcorner\sigma\urcorner})$ e quindi

$$T \vdash \exists x\,(\psi_1(x,\overline{\ulcorner\sigma\urcorner}) \wedge \neg\exists z \leq x\,\psi_2(z,\overline{\ulcorner\sigma\urcorner})) \tag{4.6}$$

per scelta di σ e φ. Inoltre

$$T \supseteq Q \vdash \forall x\,(\varphi_{\leq}(x,\overline{m}) \vee \varphi_{\leq}(\overline{m},x)) \tag{4.7}$$

per il Lemma 3.3.19. Combinando (4.5), (4.6) e (4.7) si ha che poiché T è coerente

$$T \vdash \exists x \leq \overline{m}\,(\psi_1(x,\overline{\ulcorner\sigma\urcorner}) \wedge \neg\exists z \leq x\,\psi_2(z,\overline{\ulcorner\sigma\urcorner})).$$

Per il Corollario 3.3.15 (insieme all'Osservazione 3.3.16), si ha dunque $T \vdash \psi_1(\overline{n},\overline{\ulcorner\sigma\urcorner})$ per qualche $n \leq m$, da cui $(n,\ulcorner\sigma\urcorner) \in \mathrm{Prov}^{\#}_{\mathrm{Ax}(T)}$ poiché in caso contrario $T \vdash \neg\psi_1(\overline{n},\overline{\ulcorner\sigma\urcorner})$ e T sarebbe incoerente. Segue che $\ulcorner\sigma\urcorner \in \mathrm{Teor}^{\#}_T$, ovvero $T \vdash \sigma$, contro la coerenza di T. □

4.3 Decidibilità

Si ricordi che quando T è ricorsivamente assiomatizzabile il predicato $\mathrm{Teor}^{\#}_T$ è semiricorsivo.

Definizione 4.3.1 ([AB18, Definizione 16.9]). Una teoria T in un linguaggio al più numerabile L si dice **decidibile** se $\mathrm{Teor}^{\#}_T \subseteq \mathbb{N}$ è ricorsivo; in caso contrario, T si dice **indecidibile**.

Si noti che se T è decidibile allora è anche ricorsivamente assiomatizzabile (basta prendere $\mathrm{Ax}(T) = \mathrm{Teor}_T$). Inoltre possiamo sempre assumere che T sia coerente, poiché in caso contrario $\mathrm{Teor}_T^\# = \mathrm{Enun}^\#$ sarebbe ricorsivo e quindi T sarebbe (banalmente) decidibile.

Teorema 4.3.2 ([AB18, Teorema 16.10])**.** *Sia T una teoria completa e ricorsivamente assiomatizzabile. Allora T è decidibile.*

Dimostrazione. Sia $\mathrm{Ax}(T)$ un sistema di assiomi per T con $\mathrm{Ax}^\#(T)$ ricorsivo. Per la Proposizione 4.1.6, il predicato $\mathrm{Prov}_{\mathrm{Ax}(T)}^\#$ è ricorsivo mentre $\mathrm{Teor}_T^\#$ è semiricorsivo. Consideriamo la funzione ricorsiva primitiva $f\colon \mathbb{N} \to \mathbb{N}\colon n \mapsto \langle\!\langle \#(\neg), n\rangle\!\rangle$, cosicché $f(\ulcorner\varphi\urcorner) = \ulcorner\neg\varphi\urcorner$ per ogni formula φ. Poiché come già osservato possiamo assumere che T sia coerente, per completezza di T si ha

$$\sim\mathrm{Teor}_T^\#(n) \iff n \notin \mathrm{Enun}^\# \vee \mathrm{Teor}_T^\#(f(n)).$$

Quindi il complementare di $\mathrm{Teor}_T^\#$ è anch'esso semiricorsivo, per cui $\mathrm{Teor}_T^\#$ è ricorsivo per il Teorema 1.3.4 di Post. □

Proposizione 4.3.3 ([AB18, Proposizione 16.34])**.** *Se T è una L-teoria decidibile allora lo è anche $T \cup \{\sigma\}$ per qualunque L-enunciato σ.*

Dimostrazione. Consideriamo la funzione ricorsiva primitiva

$$f\colon \mathbb{N} \to \mathbb{N}\colon n \mapsto \langle\!\langle \#(\to), \ulcorner\sigma\urcorner, n\rangle\!\rangle,$$

cosicché $f(\ulcorner\varphi\urcorner) = \ulcorner\sigma \to \varphi\urcorner$ per ogni formula φ. Allora

$$\mathrm{Teor}_{T\cup\{\sigma\}}^\#(n) \iff \mathrm{Teor}_T^\#(f(n)),$$

da cui il risultato. □

Un'**estensione finita** di una teoria T è una teoria T' *nello stesso linguaggio di* T che si ottiene aggiungendo a T un numero finito di assiomi.

Corollario 4.3.4 ([AB18, Corollario 16.35])**.** *Se un'estensione finita di una teoria T è indecidibile, allora anche T è indecidibile.*

Osservazione 4.3.5. Il viceversa non vale: la teoria dei campi è indecidibile, ma se aggiungiamo l'assioma che asserisce che il campo ha solo due elementi otteniamo una teoria decidibile.

Definizione 4.3.6 ([AB18, Definizione 16.36])**.** Una teoria T è **essenzialmente indecidibile** se ogni estensione coerente di T è indecidibile.

Se T è completa, allora T è essenzialmente indecidibile se e solo se è indecidibile poiché ogni estensione "propria" di T (ovvero ogni estensione in grado di dimostrare un enunciato che non fosse già un teorema di T) è incoerente. Inoltre se T è essenzialmente indecidibile allora ogni estensione coerente di T è essenzialmente indecidibile.

Teorema 4.3.7 ([AB18, Teorema 16.37])**.** *La teoria Q è essenzialmente indecidibile.*

Dimostrazione. Sia $T \supseteq Q$ coerente e supponiamo per assurdo che $\mathrm{Teor}_T^\#$ sia ricorsivo. Sia $\varphi(x)$ una L_Q-formula che rappresenta $\mathrm{Teor}_T^\#$ in Q (quindi anche in T). Per il Lemma 4.2.3 esiste un L_Q-enunciato σ tale che

$$T \supseteq Q \vdash \sigma \leftrightarrow \neg\varphi(\overline{\ulcorner\sigma\urcorner}).$$

(Si noti che poiché φ può essere presa di complessità Σ_1, anche σ è logicamente equivalente ad un enunciato Π_1 per l'Osservazione 4.2.4.)

Se $T \vdash \sigma$, ovvero $\ulcorner\sigma\urcorner \in \mathrm{Teor}^{\#}_T$, si avrebbe che $T \vdash \varphi(\overline{\ulcorner\sigma\urcorner})$ poiché φ rappresenta $\mathrm{Teor}^{\#}_T$ in $Q \subseteq T$. Ma allora $T \vdash \neg\sigma$ per la scelta di σ, contro la coerenza di T.

Viceversa, se $T \nvdash \sigma$, ovvero $\ulcorner\sigma\urcorner \notin \mathrm{Teor}^{\#}_T$, si avrebbe che $T \vdash \neg\varphi(\overline{\ulcorner\sigma\urcorner})$ poiché φ rappresenta $\mathrm{Teor}^{\#}_T$ in $Q \subseteq T$, da cui $T \vdash \sigma$ per la scelta di σ, contro l'assunzione $T \nvdash \sigma$.

Poiché in entrambi i casi $T \vdash \sigma$ e $T \nvdash \sigma$ raggiungiamo una contraddizione, possiamo concludere che $\mathrm{Teor}^{\#}_T$ non può essere ricorsivo. $\square$

Dimostrazione alternativa del Teorema 4.2.14. Sia $T \supseteq Q$ coerente e ricorsivamente assiomatizzabile. Se per assurdo T fosse completa, per il Teorema 4.3.2 sarebbe anche decidibile, contraddicendo il Teorema 4.3.7. $\square$

Teorema 4.3.8 ([AB18, Teorema 16.40])**.** *Ogni teoria decidibile e coerente T ha un'estensione decidibile, coerente e completa.*

Dimostrazione. L'idea è di definire per ricorsione una successione crescente di teorie

$$T = T_0 \subseteq T_1 \subseteq \ldots \subseteq T_n \subseteq \ldots$$

dove T_{n+1} si ottiene aggiungendo a T_n l'enunciato σ se e solo se $\ulcorner\sigma\urcorner = n+1$ e $T_n \nvdash \neg\sigma$. Per induzione su $n \in \mathbb{N}$ si verifica facilmente che ciascuna T_n è coerente: se σ è stato aggiunto a T_n per formare T_{n+1} ma $T_{n+1} \vdash \bot$ (dove $\bot$ è una contraddizione), poiché T_n era coerente per ipotesi induttiva si ha che $T_n \vdash \neg\sigma$, contro le regole di formazione di T_{n+1}.

La teoria $T_\infty = \bigcup_{n\in\mathbb{N}} T_n$ è dunque coerente. Inoltre, per ogni enunciato σ si ha che $\sigma \in T_\infty$ oppure $\neg\sigma \in T_\infty$. Se così non fosse, posto $n = \ulcorner\sigma\urcorner$ si avrebbe che $\ulcorner\sigma\urcorner \notin T_n$, ovvero $T_{n-1} \vdash \neg\sigma$; similmente, posto $m = \ulcorner\neg\sigma\urcorner$ si avrebbe che $\ulcorner\neg\sigma\urcorner \notin T_m$, ovvero $T_{m-1} \vdash \neg\neg\sigma$. Poiché $m \geq n$ (da cui $T_{m-1} \supseteq T_{n-1}$) si avrebbe allora che $T_{m-1} \vdash \neg\sigma \wedge \neg\neg\sigma$ e T_{m-1} sarebbe incoerente, contraddizione. Dunque T_∞ è completa e deduttivamente chiusa, ovvero $\mathrm{Teor}_{T_\infty} = T_\infty$. Resta da dimostrare che T_∞ è decidibile: poiché $\mathrm{Teor}^{\#}_{T_\infty} = T^{\#}_\infty$ dove $T^{\#}_\infty = \{\ulcorner\sigma\urcorner \mid \sigma \in T_\infty\}$, basta mostrare che $T^{\#}_\infty$ è ricorsivo.

Sia innanzitutto

$$\begin{aligned}\mathrm{Enun}^{\#}_{\uparrow}(n) \quad \iff \quad & n \in \mathrm{Seq} \wedge \forall i < \ell(n)\, [(\!(n)\!)_i \in \mathrm{Enun}^{\#}] \\ & \wedge (\ell(n) \geq 2 \rightarrow \forall i < \ell(n) - 1\, [(\!(n)\!)_i < (\!(n)\!)_{i+1}])\end{aligned}$$

l'insieme (dei codici) delle sequenze strettamente crescenti (nell'ordine dato dalla codifica) di enunciati: $\mathrm{Enun}^{\#}_{\uparrow}$ è chiaramente ricorsivo primitivo. Definiamo ora una funzione ricorsiva primitiva $g\colon \mathbb{N} \to \mathbb{N}$ tale che $g(n) =$ il codice di[4] $\bigvee_{1\leq i\leq k} \neg\sigma_i$ se $n = \langle\!\langle \ulcorner\sigma_1\urcorner, \ldots, \ulcorner\sigma_k\urcorner \rangle\!\rangle \in \mathrm{Enun}^{\#}_{\uparrow}$ e $g(n) = 0$ altrimenti. La definizione di g è per ricorsione generalizzata ponendo

$$\begin{cases} g(0) = 0 \\ g(n+1) = h(n, g^{\mathrm{m}}(n)) \end{cases}$$

dove $h(n, z)$ è definita per casi come segue:

[4]La disgiunzione generalizzata $\bigvee_{1\leq i\leq k} \varphi_i$ è definita per ricorsione su $k \geq 1$ ponendo $\bigvee_{1\leq i\leq 1} \varphi_i = \varphi_1$ e $\bigvee_{1\leq i\leq k+1} \varphi_i = \left(\bigvee_{1\leq i\leq k} \varphi_i\right) \vee \varphi_{k+1}$. La congiunzione generalizzata $\bigwedge_{1\leq i\leq k} \varphi_i$ è definita in maniera analoga.

- se $n+1 \in \mathrm{Enun}^{\#}_{\uparrow}$ e $\ell(n+1) = 1$ allora
$$h(n,z) = \langle\!\langle \#(\neg), (\!(n+1)\!)_0 \rangle\!\rangle;$$
- se $n+1 \in \mathrm{Enun}^{\#}_{\uparrow}$ e $\ell(n+1) > 1$, allora
$$h(n,z) = \langle\!\langle \#(\vee), (\!(z)\!)_{\mathrm{IS}(n+1,\ell(n+1)-1)}, \langle\!\langle \#(\neg), (\!(n+1)\!)_{\ell(n+1)-1} \rangle\!\rangle \rangle\!\rangle;$$
- in tutti gli altri casi, $h(n,z) = 0$

Poiché tutti i casi nella sua definizione sono ricorsivi primitivi (e le funzioni utilizzate in ciascun caso sono tutte ricorsive primitive), la funzione h è ricorsiva primitiva e quindi lo è anche g.

Definiamo ora $f \colon \mathbb{N} \to \mathbb{N}$ per ricorsione generalizzata ponendo
$$\begin{cases} f(0) = 0 \\ f(n+1) = \chi_R(n, f^{\mathrm{m}}(n)) \end{cases}$$
dove $R \subseteq \mathbb{N}^2$ è il predicato ricorsivo primitivo definito da $R(n,z)$ se e solo se
$$n+1 \in \mathrm{Enum}^{\#} \wedge \neg\exists k \leq n+1\, \exists s \leq B(k,n+1) \Big[s \in \mathrm{Enum}^{\#}_{\uparrow}$$
$$\wedge\, \ell(s) = k+1 \wedge (\!(s)\!)_k = n+1 \wedge \forall i < k\, [(\!(z)\!)_{(\!(s)\!)_i} = 1] \wedge g(s) \in \mathrm{Teor}^{\#}_T \Big].$$
(La funzione ricorsiva primitiva B che compare nella precedente definizione è come in Proposizione 1.4.8(1).)

Poiché per ipotesi $\mathrm{Teor}^{\#}_T$ è ricorsivo, anche il predicato R e la funzione f lo sono. Infine si verifica facilmente che $f = \chi_{T^{\#}_{\infty}}$: è infatti sufficiente notare che $\bigvee_{1\leq i\leq k} \neg\sigma_i$ è logicamente equivalente a $\left(\bigwedge_{1\leq i\leq k-1} \sigma_i\right) \to \neg\sigma_k$, per cui
$$T \vdash \bigvee_{1\leq i\leq k} \neg\sigma_i \iff T \cup \{\sigma_1, \dots, \sigma_{k-1}\} \vdash \neg\sigma_k. \qquad \square$$

4.4 Teorema di Tarski e Teorema di Church

Il seguente risultato di Tarski viene spesso presentato come "teorema dell'indefinibilità della verità".

Teorema 4.4.1 ([AB18, Teorema 16.38])**.** *Sia* $\mathrm{Th}(\langle \mathbb{N}, +, \cdot, S, 0\rangle)$ *la teoria del modello standard per l'aritmetica, ovvero l'insieme degli* L_Q*-enunciati veri in* $\mathbb{N}$*. Allora l'insieme dei loro codici*
$$\mathrm{Th}(\langle \mathbb{N}, +, \cdot, S, 0\rangle)^{\#} = \{\ulcorner\sigma\urcorner \mid \langle \mathbb{N}, +, \cdot, S, 0\rangle \models \sigma\}$$
non è definibile in $\mathbb{N}$*, ovvero non esiste alcuna* L_Q*-formula* $\varphi(x)$ *tale che per ogni* L_Q*-enunciato* σ *si abbia*
$$\sigma \in \mathrm{Th}(\langle \mathbb{N}, +, \cdot, S, 0\rangle) \iff \langle \mathbb{N}, +, \cdot, S, 0\rangle \models \varphi(\ulcorner\sigma\urcorner).$$

Dimostrazione. Se esistesse una tale $\varphi(x)$ allora per il Lemma 4.2.3 esisterebbe un enunciato σ tale che
$$Q \vdash \sigma \leftrightarrow \neg\varphi(\ulcorner\sigma\urcorner).$$
Allora poiché $\langle \mathbb{N}, +, \cdot, S, 0\rangle \models Q$ si avrebbe $\sigma \in \mathrm{Th}(\langle \mathbb{N}, +, \cdot, S, 0\rangle)$ se e solo se $\langle \mathbb{N}, +, \cdot, S, 0\rangle \models \neg\varphi(\ulcorner\sigma\urcorner)$ se e solo se $\sigma \notin \mathrm{Th}(\langle \mathbb{N}, +, \cdot, S, 0\rangle)$, contraddizione. $\square$

Il seguente teorema è invece dovuto a Church e viene talvolta presentato come "indecidibilità del calcolo dei predicati (relativo ad un opportuno linguaggio L)".

Teorema 4.4.2 ([AB18, Teorema 16.39])**.** *Il calcolo dei predicati in un linguaggio $L \supseteq L_Q$ è indecidibile, ovvero l'insieme*

$$\mathrm{Val}^{\#}(L) = \{\ulcorner \varphi \urcorner \mid \varphi \textit{ è un } L\textit{-enunciato logicamente valido}\}$$

non è ricorsivo.

Dimostrazione. Per definizione $\mathrm{Val}^{\#}(L) = \mathrm{Teor}_T^{\#}$ dove T è la L-teoria vuota: basta quindi mostrare che T è indecidibile. Poiché la teoria Q, vista come L-teoria, è un'estensione finita di T, dall'indecidibilità di Q segue l'indecidibilità di T per il Corollario 4.3.4. □

Osservazione 4.4.3. È possibile dimostrare analoghi teoremi con linguaggi di tipo diverso. Ad esempio, se L contiene un simbolo di relazione binario allora $\mathrm{Val}^{\#}(L)$ è nuovamente indecidibile. Lo stesso accade se L contiene un simbolo di funzione binario.

Appendice: Alcune funzioni ricorsive primitive

- Le funzioni costanti sono definite per composizione di funzioni iniziali: $c_n(x) = \underbrace{S(S(\dots S(}_{n \text{ volte}} c_0(x)))).$

- La somma è definita per ricorsione con $g(x) = \mathrm{id}(x) = U_1^1(x)$ e $h(u,v,w) = S(U_3^3(u,v,w))$:
$$\begin{cases} x + 0 = x \\ x + (y+1) = S(x+y). \end{cases}$$

- Il prodotto è definito per ricorsione con $g(x) = c_0(x)$ e $h(u,v,w) = U_3^3(u,v,w) + U_1^3(u,v,w)$:
$$\begin{cases} x \cdot 0 = 0 \\ x \cdot (y+1) = x \cdot y + x. \end{cases}$$

- $\begin{cases} x^0 = 1 \\ x^{y+1} = x^y \cdot x. \end{cases}$

- $\begin{cases} 0! = 1 \\ (y+1)! = y! \cdot (y+1). \end{cases}$

- $\begin{cases} \mathrm{pr}(0) = 0 \\ \mathrm{pr}(y+1) = y. \end{cases}$

- $\begin{cases} \mathrm{sgn}(0) = 0 \\ \mathrm{sgn}(y+1) = 1. \end{cases}$

  $\begin{cases} \overline{\mathrm{sgn}}(0) = 1 \\ \overline{\mathrm{sgn}}(y+1) = 0. \end{cases}$

- $\begin{cases} x \dot{-} 0 = x \\ x \dot{-} (y+1) = \mathrm{pr}(x \dot{-} y). \end{cases}$

- $|x - y| = (x \dot{-} y) + (y \dot{-} x).$

- $\min(x,y) = x \dot{-} (x \dot{-} y)$

  $\max(x,y) = x + (y \dot{-} x)$

  $\min_k(x_1, \dots, x_k) = \min(x_1, \min(x_2, \dots \min(x_{k-1}, x_k)))$

  $\max_k(x_1, \dots, x_k) = \max(x_1, \max(x_2, \dots \max(x_{k-1}, x_k)))$

- $\chi_{\leq}(x, y) = \overline{\text{sgn}}(x \dot{-} y)$
  $\chi_{=}(x, y) = \overline{\text{sgn}}(|x - y|)$
  $\chi_{\geq}(x, y) = \chi_{\leq}(y, x)$
  $\chi_{<}(x, y) = \text{sgn}(y \dot{-} x)$

Sfruttando la minimizzazione limitata si ha inoltre

- $\text{Quoz}(n, m) = \text{sgn}(m) \cdot \mu q \leq n\, (\chi_{\leq}((q + 1) \cdot m, n) = 0)$
- $\text{Res}(n, m) = n \dot{-} \text{Quoz}(n, m) \cdot m$
- $\text{mcm}(n, m) = \mu k \leq n \cdot m\, (\text{Res}(k, n) + \text{Res}(k, m) = 0)$
- $\text{MCD}(n, m) = n \dot{-} \mu k \leq n\, (\text{Res}(n, n \dot{-} k) + \text{Res}(m, n \dot{-} k) = 0)$
- $\boldsymbol{J}(x, y) = \left(\sum_{v \leq x+y} v\right) + x$
- $(z)_0 = z \dot{-} \sum_{v \leq h(z)} v$ con $h(z) = \mu w \leq z(\chi_{\leq}(\sum_{v \leq w+1} v, z) = 0)$
- $(z)_1 = h(z) \dot{-} (z)_0$

Bibliografia

[AA19] Alessandro Andretta. Elements of Mathematical Logic. *personal notes*, Version of September 3, 2019.

[AB18] Alessandro Berarducci. Calcolabilità e teoremi di incompletezza di Gödel. *note personali*, Versione del 7 gennaio 2018.