Appunti di Logica Matematica

tratti dalle lezioni e dagli appunti del corso di Logica Matematica tenuto negli anni accademici 2023/2024 e 2024/2025 dal professor Marcello Mamino all'università di Pisa

Giorgio Alamia
g.alamia@studenti.unipi.it

23 ottobre 2025

Indice

Introduzione

Questi sono gli appunti che ho scritto per uso personale nello studio del corso di Logica Matematica. In particolare sono stati redatti a partire dalle dispense scritte dal professor Marcello Mamino che ha tenuto il corso negli anni accademici 2023/2024 e 2024/2025 all'Università di Pisa, dalle dispense scritte dal professor Rosario Mennuni (che ha tenuto le lezioni della parte indicata come teoria dei modelli nell'anno 2023/2024) e dalle registrazioni delle lezioni tenute nei due anni accademici (ho usato soprattutto le risorse relative all'anno 2023/2024 ma alcune cose sono state tratte anche da quelle del 2024/2025).

In larga parte ho cercato al mio meglio di scrivere tutto ciò che è stato esposto nelle lezioni ma chiaramente ci saranno delle parti o mancanti o che ho interpretato male o altresì sbagliate; è importante quindi che io precisi che queste note non sono state sottoposte ad alcun tipo di revisione, e chiunque decida di usarle per facilitare il proprio studio fa questo 'a suo rischio e pericolo' di imbattersi in diversi errori di qualunque tipologia e gravità possibile o immaginabile.

Per quanto riguarda gli esercizi ho scritto negli appunti la maggior parte degli enunciati menzionati a lezione, ne ho svolti molti ma non tutti (diversi di questi sono stati svolti a lezione in almeno uno dei due anni a cui si riferiscono le note), ci sono però ancora più esercizi scritti nelle note.

In caso qualcuno noti degli errori o mancanze può inviarmi una mail per informarmi, all'indirizzo nella pagina del titolo o se questo non è più attivo anche ad altri miei indirizzi email come giorgioalamia@gmail.com; se deciderò di aggiornare il testo cercherò di caricare la versione più aggiornata sulla mia pagina `https://poisson.phc.dm.unipi.it/~alamia/`

Per quanto riguarda la struttura degli appunti cerco di seguire quella del corso da cui sono tratti, quindi ho suddiviso tutto in tre parti:

- La prima parte, per lo più introduttiva, descrive i predicati della logica del primo ordine (gli strumenti principali del corso) introducendo poi gli ultrafiltri ed ultraprodotti, strumenti usati per costruire modelli, ed il teorema di compattezza.
- La seconda parte introduce le regole di inferenza ed alcuni concetti e risultati fondamentali della teoria dei modelli: i teoremi di correttezza, completezza e compattezza (collegati alle regole di inferenza) concludendo con i teoremi di Löwenheim-Skolem.
- La terza parte è incentrata sulla computabilità, in particolare iniziamo vediamo due nozioni di computabilità diverse: la prima basata sulla ricorsione e la seconda basata sulle macchine di Turing; vedremo poi che le due sono equivalenti e concluderendo mostrando due interessanti risultati di computabilità (il teorema S_n^m ed il teorema del punto fisso). Proseguiamo poi introducendo la gerarchia aritmetica (un modo di categorizzare le formule aritmetiche) per poi dimostrare il lemma di diagonalizzazione di Gödel, questo con l'obbiettivo di dimostrare i due teoremi di incompletezza di Gödel, per poi concludere con una descrizione a grandi linee una soluzione al decimo problema di Hilbert. Visto che quest'ultimo capitolo sul decimo problema di Hilbert era stato considerato al di fuori del programma del corso non mi sono soffermato molto sugli appunti a riguardo, lasciando molte parti incomplete.

Versione I: 6 agosto 2025
Versione II: 26 settembre 2025
Versione III: 23 ottobre 2025

Parte I

Predicati del primo ordine

Capitolo 1

Linguaggi e formule

In questo capitolo descriviamo i primi strumenti essenziali per la logica.

In particolare vogliamo trasformare gli enunciati in oggetti matematici, le *formule*, per poterli manipolare e strudiare.

Definizione 1.0.1: *Alfabeto*

Un *alfabeto* è un insieme di simboli[1].

Definizione 1.0.2: *Linguaggio formale*

Dato un alfabeto A un A-*linguaggio* è un insieme di stringhe, cioè sequenze finite di simboli, i cui simboli sono tutti nell'alfabeto A.

Nota 1.0.1: *Stringa vuota* Solitamente la stringa vuota si indica con il simbolo ε e qualunque sia l'alfabeto A questa stringa può appartenere ad un A-linguaggio ma non è necessario che vi appartenga.

Definizione 1.0.3: *Linguaggio del primo ordine*

Definiamo *linguaggio del primo ordine*[2] una terna $L = (R, F, ar)$ dove:

- R è l'insieme dei simboli di relazione[3]
- F è l'insieme dei simboli di funzione
- ar è l'arietà, ovvero una funzione da $R \sqcup F$ in $\mathbb{N}$[4]

Per capire la distinzione tra i simboli di relazione e di funzione dobbiamo vedere cosa sono i termini e le formule, infatti i simboli di funzione saranno una componente dei termini, mentre quelli di relazione saranno una componente delle formule.

Esempio 1.0.2: *Linguaggio della teoria dei gruppi* Per rappresentare la teoria dei gruppi abbiamo bisogno dell'elemento neutro e, del prodotto $\cdot$ e dell'inverso $^{-1}$ che compongono l'alfabeto del linguaggio, vedremo che questi tre sono simboli di funzione con arietà rispettivamente zero, due ed uno.
In realtà servirebbe anche l'uguale, ma vedremo più avanti che questo sarà un simbolo di relazione

[1] Non abbiamo specificato cosa sono i simboli ma questo è perché non hanno un vero e proprio significato in se e per se, sono solo dei segnaposto di cui sappiamo dire se sono diversi o uguali fra loro. Al livello intuitivo sono le 'tracce di inchiostro che usiamo scrivendo'; volendo si potrebbero formalizzare ad esempio usando degli specifi insiemi ma in questo caso non c'è veramente bisogno di farlo

[3] in generale da ora in avanti scrivendo linguaggio si intende un linguaggio del primo ordine, non un linguaggio formale come dalla definizione (1.0.2)

[4] in questi appunti indicherò $\mathbb{N} = \mathbb{N}_0 = \mathbb{N} \cup 0$

con arietà due che per convenzione è sempre incluso nel linguaggio.

1.1 Termini e Formule

Vorremmo definire cosa sono le formule in un dato linguaggio, faremo questo con un procedimento ricorsivo a partire dai termini.

Definizione 1.1.1: *L-termine*

Dato un linguaggio del primo lordine $L = (R, F, ar)$ diciamo *L-termine* (o termine nel linguaggio L) una stringa nell'alfabeto:

$$F \sqcup \{x_i\}_{i\in\mathbb{N}} \sqcup \{\ (,\ ),\ ,\}$$

tale che, indicando con $\mathrm{Var} = \{x_i\}_{i\in\mathbb{N}}$ l'insieme dei simboli di variabile, la stringa è una tra le seguenti[5]:

- un simbolo di variabile $x_i \in \mathrm{Var}$;
- la stringa $f(t_1, \dots, t_n)$ dove $f \in F$, $n = ar(f)$[6] e tutti i t_i sono a loro volta L-termini.

Eventualmente un simbolo di funzione c può essere 0-ario, quindi anche tali simboli possono come le variabili fare da 'base' nella ricorsione dei termini infatti $c()$ è un termine che non richiede ricorsivamente l'esistenza di altri termini.

Definizione 1.1.2: *Simbolo di costante*

Diciamo che un simbolo di funzione c è un *simbolo di costante* se è 0-ario, ovvero se la sua arietà è $ar(c) = 0$.
Analogamente per un simbolo di relazione k se k è 0-ario diremo che k è un *simbolo di costante proposizionale*.

Nota 1.1.1 Se c è un simbolo di costante per definizione in un L-termine dovremmo indicarlo con $c()$ ma per semplicità lo indicheremo soltanto con c, omettendo le parentesi. Inoltre nei casi dove non ci sono fraintendimenti useremo la classica notazione infissa per le operazioni aritmetiche intese come simboli di funzione (ad esempio useremo $t_1 + t_2$ invece che $+(t_1, t_2)$) e ci prenderemo la libertà di usare altri nomi per le variabili invece di $x_0, x_1, x_2, \dots$ (ad esempio x, y, z).

Definizione 1.1.3: *L-formula*

Dato un linguaggio del primo lordine $L = (R, F, ar)$ diciamo *L-formula* (o formula nel linguaggio L) una stringa nell'alfabeto:

$$F \sqcup R \sqcup \{x_i\}_{i\in\mathbb{N}} \sqcup \{\ (,\ ),\ ,\ ,\ \top, \bot, \neg, \wedge, \vee, \to, \forall, \exists, ., =\}$$

in modo che sia una tra le seguenti[7]:

- una cosiddetta formula atomica, cioè una tra le seguenti:
  - la formula sempre vera $\top$ o la formula sempre falsa $\bot$;
  - una stringa $t_1 = t_2$ dove t_1 e t_2 sono due L-termini;
  - una stringa $r(t_1, \dots, t_n)$ dove $r \in R$, $n = ar(r)$ e tutti i t_i sono degli L-termini;
- un tra le seguenti

$$(\neg\varphi), \qquad (\varphi_1 \wedge \varphi_2), \qquad (\varphi_1 \vee \varphi_2), \qquad (\varphi_1 \to \varphi_2)$$

  dove $\varphi, \varphi_1, \varphi_2$ sono a loro volta L-formule

[6] Effettivamente stiamo usando una grammatica libera dal contesto per definire gli L-termini

- un tra le seguenti
$$(\forall x_i.\varphi), \qquad (\exists x_i.\varphi)$$
dove φ è a sua volta una L-formula ed x_i è un simbolo di variabile.

Osservazione 1.1.2 Notiamo che in questa definizione abbiamo usato una quantità ingente di parentesi, anche forse dove non sarebbero necessarie, l'idea di questo è di dare una maniera univoca di 'spacchettare' una formula nell'albero di sottoformule che la hanno creata, ma come detto all'inizio del capitolo il nostro obbiettivo nel definire le formule è di poterle all'interno di una teoria matematica, ad esempio ZF, all'atto pratico poi non sarà chiaramente bisogno di usare sempre tutte queste parentesi e simili formalismi ma potremo chiaramente usare notazioni più intuitive, come anticipato nella nota 1.1.1.
L'univocità in particolare è utile per impostare delle dimostrazioni per induzione strutturale (cioè per induzione sulla complessità delle formule) e per impostare costruzioni o definizioni per ricorsione strutturale.

Definizione 1.1.4: *Sottoformula*

Data una formula φ diciamo che ψ è *sottoformula* di φ se:

- $\psi \equiv \varphi$;
- se $\varphi \doteq (\neg\theta)$ e ψ è una sottoformula di θ allora ψ è una sottoformula di φ;
- se
$$\varphi \doteq (\theta \wedge \rho) \qquad \text{o} \qquad \varphi \doteq (\theta \vee \rho) \qquad \text{o} \qquad \varphi \doteq (\theta \to \rho)$$
e ψ è una sottoformula di θ oppure è una sottoformula di ρ allora ψ è una sottoformula di φ;
- se
$$\varphi \doteq (\forall x_k.\theta) \qquad \text{o} \qquad \varphi \doteq (\exists x_k.\theta)$$
e ψ è una sottoformula di θ allora ψ è una sottoformula di φ.

Definizione 1.1.5: *Variabili libere*

Se t è un termine definiamo $\mathrm{var}(t) \subset \{x_i\}_{i\in\mathbb{N}}$ a seconda di come è costruito t come:

- se $t \doteq c()$ è una costante allora $\mathrm{var}(t) = \varnothing$;
- se $t \doteq x_k$ è una variabile allora $\mathrm{var}(t) = \{x_k\}$;
- se $t \doteq f(t_1, \dots, t_n)$ allora $\mathrm{var}(t) = \bigcup_{i=1}^{n} \mathrm{var}(t_i)$.

Da questo se φ è una formula definiamo l'insieme delle sue *variabili libere* $\mathrm{vl}(\varphi) \subseteq \{x_i\}_{i\in\mathbb{N}}$ come:

- se $\varphi \doteq \top$ o $\varphi \doteq \bot$ allora $\mathrm{vl}(\psi) = \varnothing$.
- se $\varphi \doteq\ t_1 = t_2$ allora $\mathrm{vl}(\varphi) = \mathrm{var}(t_1) \cup \mathrm{var}(t_2)$
- se $\varphi \doteq r(t_1, \dots, t_n)$ allora $\mathrm{vl}(\varphi) = \bigcup_{i=1}^{n} \mathrm{var}(t_i)$
- se $\varphi \doteq (\neg\psi)$ allora $\mathrm{vl}(\varphi) = \mathrm{vl}(\psi)$
- se φ è una delle seguenti:
$$(\varphi_1 \wedge \varphi_2), \qquad (\varphi_1 \vee \varphi_2), \qquad (\varphi_1 \to \varphi_2)$$
allora $\mathrm{vl}(\varphi) = \mathrm{vl}(\varphi_1) \cup \mathrm{vl}(\varphi_2)$
- se φ è una delle seguenti:
$$(\forall x_i.\psi), \qquad (\exists x_i.\psi)$$
allora $\mathrm{vl}(\varphi) = \mathrm{vl}(\psi_1) \setminus \{x_i\}$

Esempio 1.1.3 Tornando all'esempio della teoria dei gruppi possiamo costruire la formula

$$\varphi \doteq \exists x_1 . x_2 = x_1 \cdot x_1$$

per dire che x_2 è un quadrato, dove $x_1 \cdot x_1$ è un termine con $\mathrm{var} = \{x_1\}$, $x_2 = x_1 \cdot x_1$ è una formula atomica con $\mathrm{vl} = \{x_1, x_2\}$ e $\mathrm{vl}(\varphi) = \{x_2\}$, infatti pur essendo x_1 dentro a φ questa è 'legata' dalla presenza di quell'*esiste*, quindi è ragionevole il nome di variabili *libere*.

Capitolo 2

Strutture e semantica

Adesso abbiamo definito le formule ma non vi abbiamo dato un vero e proprio significato, una semantica[1].

Chiaramente una formula potrebbe essere vera o falsa a seconda del contesto in cui ci troviamo, formalizziamo quindi il concetto di *struttura* per descrivere in generale le strutture algebriche (gruppi, campi, ordini...) per poi dire che cosa vuol dire che una struttura soddisfa una formula (o un insieme di formule) così da arrivare al concetto di *conseguenza logica*, cioè dire che tutte le strutture che soddisfano la formula φ soddisfano anche ψ.

Grazie al concetto di conseguenza logica possiamo parlare di *teorie* e dei loro *modelli*, cioè delle strutture che soddisfano una determinata teoria.

Definizione 2.0.1: *L-struttura*

Dato un linguaggio del primo lordine $L = (R, F, ar)$ diciamo *L-struttura* una coppia $M = (D, i)$ dove D è un insieme detto dominio o universo ed i è una funzione con dominio $R \sqcup F$ detta interpretazione con le seguenti proprietà:

- il dominio D è non vuoto;
- se $r \in R$ allora $i(r) \subseteq D^{ar(r)}$;
- se $f \in F$ allora $i(f) : D^{ar(f)} \to D$

Nota 2.0.1 Al livello di notazione invece di $i(r)$ ed $i(f)$ scriveremo rispettivamente r_M ed f_M, eventualmente omettendo la struttura al pedice se non c'è possibilità di confusione.

Esempio 2.0.2 Ancora una volta dato che la notazione formale è pesante nella maggior parte dei casi non la utilizzeremo, ad esempio se indichiamo la struttura $(\mathbb{Z}, 0, +, -, \cdot, <)$ è chiaro che stiamo parlando della struttura che ha come dominio $\mathbb{Z}$, il linguaggio $L(R, F, ar)$ con $R = \{<\}$, $F = \{0, +, -, \cdot\}$ e le rispettive arietà ovvie dove:

$$i(<) = \left\{(x, y) \in \mathbb{Z}^2 \;\middle|\; x < y\right\}$$

$$\begin{array}{ll} i(0) : \{\star\} \to \mathbb{Z}. & i(0)(\star) = 0 \\ i(-) : \mathbb{Z} \to \mathbb{Z}. & i(-)(n) = -n \\ i(+) : \mathbb{Z}^2 \to \mathbb{Z}. & i(+)(a, b) = a + b \\ i(\cdot) : \mathbb{Z}^2 \to \mathbb{Z}. & i(\cdot)(a, b) = a \cdot b \end{array}$$

ed usando la notazione della nota 2.0.1 $i(+)(a, b)$ sarà scritto come $a +_{\mathbb{Z}} b$ oppure se non ci sono fraintendimenti anche solo $a + b$.

[1] La parola semantica è un termine che viene usato in maniera generica per indicare il significato dei termini di un linguaggio formale in diversi ambiti scientifici, come ad esempio la semantica dei linguaggi di programmazione

2.1 Semantica di Tarski

Definizione 2.1.1: *Valutazione delle variabili*

Fissata una L-struttura[2] $M = (D, i)$ definiamo *ambiente* o *valutazione delle variabili in* M una funzione $v : \mathrm{Var} \to D$.
Data una valutazione delle variabili v, un elemento $a \in D$ ed un indice $j \in \mathbb{N}$ usiamo la notazione $v\left[a/x_j\right]$ per indicare una nuova valutazione delle variabili costruita ponendo

$$\forall\, k \in \mathbb{N}. v\left[a/x_j\right](x_k) = \begin{cases} v(x_k) & \text{se } k \neq j \\ a & \text{se } k = j \end{cases}$$

Definizione 2.1.2: *Semantica di Tarski*

Fissata una L-struttura $M = (D, i)$ data una valutazione delle variabili v definiamo $\{v\}\, t \in D$ per ogni termine t ponendo:

- se $t \doteq c()$ è una costante allora $\{v\}\, t = c_M$;
- se $t \doteq x_i$ è una variabile allora $\{v\}\, t = v(x_i)$;
- se $t \doteq f(t_1, \ldots, t_k)$ è un simbolo di funzione applicato a $k = ar(f)$ termini allora

$$\{v\}\, t = f_M(\{v\}\, t_1, \ldots, \{v\}\, t_k)$$

Con questo data una formula φ indichiamo $M \vDash \{v\}\, \varphi$ ovvero M *è un modello della valutazione* v *applicata a* φ (oppure M è un modello di φ nel contesto v) un valore di verità (vero o falso) ponendo:

- se $\varphi \doteq \top$ allora $M \vDash \{v\}\, \varphi$ è vero e se $\varphi \doteq \bot$ allora $M \vDash \{v\}\, \varphi$ è falso;
- se $\varphi \doteq\ t_1 = t_2$ con t_1 e t_2 due termini allora $M \vDash \{v\}\, t_1 = t_2$ è vero se $\{v\}\, t_1 = \{v\}\, t_2$;
- se $\varphi \doteq r(t_1, \ldots, t_k)$ è un simbolo di relazione applicato a $k = ar(r)$ termini allora $M \vDash \{v\}\, r(t_1, \ldots, t_k)$ è vero se
$$(\{v\}\, t_1, \ldots, \{v\}\, t_k) \in r_M$$
ed altrimenti $M \vDash \{v\}\, r(t_1, \ldots, t_k)$ è falso;
- se $\varphi \doteq \neg\psi$ allora $M \vDash \{v\}\, \neg\psi$ è vero se $M \vDash \{v\}\, \psi$ è falso ed altrimenti $M \vDash \{v\}\, \neg\psi$ è falso;
- se $\varphi \doteq \varphi_1 \wedge \varphi_2$ allora $M \vDash \{v\}\, \varphi_1 \wedge \varphi_2$ è vero se entrambe $M \vDash \{v\}\, \varphi_1$ e $M \vDash \{v\}\, \varphi_2$ sono vere ed altrimenti $M \vDash \{v\}\, \varphi_1 \wedge \varphi_2 = F$;
- se $\varphi \doteq \varphi_1 \vee \varphi_2$ allora $M \vDash \{v\}\, \varphi_1 \wedge \varphi_2$ è falso se entrambe $M \vDash \{v\}\, \varphi_1$ e $M \vDash \{v\}\, \varphi_2$ sono false ed altrimenti $M \vDash \{v\}\, \varphi_1 \vee \varphi_2$ è vero;
- se $\varphi \doteq \varphi_1 \to \varphi_2$ allora $M \vDash \{v\}\, \varphi_1 \to \varphi_2$ è falso se $M \vDash \{v\}\, \varphi_1$ è vero mentre $M \vDash \{v\}\, \varphi_2$ è falso ed altrimenti $M \vDash \{v\}\, \varphi_1 \to \varphi_2$ è vero;
- se $\varphi \doteq \forall\, x_i.\psi$ allora $M \vDash \{v\}\, \forall\, x_i.\psi$ è vero se per ogni elemento del dominio $a \in D$ è vero $M \vDash \left\{v\left[a/x_i\right]\right\}\psi$;
- se $\varphi \doteq \exists\, x_i.\psi$ allora $M \vDash \{v\}\, \exists\, x_i.\psi$ è vero se esiste un elemento del dominio $a \in D$ tale che è vero $M \vDash \left\{v\left[a/x_i\right]\right\}\psi$.

Nota 2.1.1 In pratica la semantica di Tarski ci da un 'programma' per valutare i termini e le formule. Chiaramente tutto questo si basa su diverse nozioni intuitive, è particolarmente evidente nei casi

[2] Quando non specifichiamo chi sia il linguaggio L supponiamo che sia un generico linguaggio del primo ordine $L = (R, F, ar)$; e questo vale anche nel caso in cui scriviamo termini, formule, strutture etc... senza esplicitare il prefisso L-

> dell'*uguale*, del *per ogni* e dell'*esiste*, però è anche vero che non è possibile fare molto meglio di questo, in un modo o nell'altro prima o poi bisogna risalire a qualcosa, come l'intuizione o una proprietà fisica o qualche altro fattore arbitrario nella scelta dei nostri sistemi.

Adesso abbiamo modo di verificare che fissato un contesto una formula ha un valore di verità specifico, però noi vorremmo poter dire che certe formule sono vere 'a prescindere' dal contesto, ad esempio vorremmo che qualunque contesto scegliamo nei numeri naturali non ci sia un numero che elevato al quadrato valga sette.

Proposizione 2.1.3

Data una formula φ se v_1 e v_2 sono valutazioni delle variabili che coincidono sulle variabili libere di φ allora M è un modello di φ nel contesto v_1 se e solo se lo è nel contesto v_2.

Dimostrazione. Sfruttiamo la costruzione ricorsiva delle formule per procedere per induzione strutturale sulle formule [3].

Per il passo base supponiamo che φ sia una formula atomica.

In questo caso avremo bisogno di un risultato analogo sui termini, cioè che se due valutazioni v_1 e v_2 coincidono sull'insieme $\mathrm{var}(t)$ allora $\{v_1\}\, t = \{v_2\}\, t$; quindi procediamo per induzione strutturale sulla complessità dei termini.

Per il passo base di questa induzione sui termini:

- se $t \doteq c()$ è una costante allora $\{v_1\}\, t = c_M = \{v_2\}\, t$
- se $t \doteq x_i$ è una variabile allora per ipotesi $\{v_1\}\, t = v_1(t) = v_2(t) = \{v_2\}\, t$

Poi per il passo induttivo di questa induzione sui termini se $t \doteq f(t_1, \dots, t_k)$ e se per ogni $i \in \{1, \dots, k\}$ vale $\{v_1\}\, t_i = \{v_2\}\, t_i$ allora

$$\{v_1\}\, t = f_M(\{v_1\}\, t_1, \dots, \{v_1\}\, t_k) = f_M(\{v_2\}\, t_1, \dots, \{v_2\}\, t_k) = \{v_2\}\, t$$

Tornando al passo base dell'induzione sulle formule in particolare chiaramente il risultato è vero se φ è la formula sempre vera o la formula sempre falsa; invece con $\varphi \doteq t_1 = t_2$ se v_1 e v_2 coincidono su $\mathrm{vl}(\varphi) = \mathrm{var}(t_1) \cup \mathrm{var}(t_2)$ allora per definizione è vero $M \vDash \{v_1\}\, t_1 = t_2$ se e solo se $\{v_1\}\, t_1 = \{v_1\}\, t_2$ e per il risultato intermedio sui termini valgono sia $\{v_1\}\, t_1 = \{v_2\}\, t_1$ che $\{v_1\}\, t_2 = \{v_2\}\, t_2$ ovvero $M \vDash \{v_1\}\, t_1 = t_2$ è vero se e solo se $M \vDash \{v_2\}\, t_1 = t_2$ è vero.

Altrimenti (sempre nel caso base) esiste una relazione $r \in R$ tale che $\varphi \doteq r(t_1, \dots, t_k)$ quindi se v_1 e v_2 coincidono su $\mathrm{vl}(\varphi) = \bigcup_{i=1}^{k} \mathrm{var}(t_k)$ allora per definizione $M \vDash \{v_1\}\, r(t_1, \dots, t_k)$ è vero se e solo se $(\{v_1\}\, t_1, \dots, \{v_1\}\, t_k) \in r_M$ ed ancora una volta per il risultato intermedio sui termini per ogni $i \in \{1, \dots, k\}$ vale $\{v_1\}\, t_i = \{v_2\}\, t_i$ quindi

$$(\{v_1\}\, t_1, \dots, \{v_1\}\, t_k) = (\{v_2\}\, t_1, \dots, \{v_2\}\, t_k)$$

ovvero $M \vDash \{v_1\}\, r(t_1, \dots, t_k)$ è vero se e solo se $M \vDash \{v_2\}\, r(t_1, \dots, t_k)$ è vero.

Per il passo induttivo dobbiamo di nuovo distinguere diversi casi:

1. se $\varphi \doteq \neg\psi$ e se la tesi è vera per ψ allora v_1 e v_2 coincidono su $\mathrm{vl}(\psi)$ quindi per l'ipotesi induttiva $M \vDash \{v_1\}\, \psi$ è vero se e solo se $M \vDash \{v_2\}\, \psi$ è vero ovvero anche $M \vDash \{v_1\}\, \varphi$ è vero se e solo se $M \vDash \{v_2\}\, \varphi$ è vero;
2. se $\varphi \doteq \varphi_1 \wedge \varphi_2$ e se la tesi è vera per φ_1 e φ_2 allora v_1 e v_2 coincidono su $\mathrm{vl}(\varphi_1) \cup \mathrm{vl}(\varphi_2)$ quindi per l'ipotesi induttiva sia $M \vDash \{v_1\}\, \varphi_1$ che $M \vDash \{v_1\}\, \varphi_2$ sono entrambi veri se e solo sesia $M \vDash \{v_2\}\, \varphi_1$ che $M \vDash \{v_2\}\, \varphi_2$ sono entrambi veri ovvero anche $M \vDash \{v_1\}\, \varphi$ è vero se e solo se $M \vDash \{v_2\}\, \varphi$;
3. il procedimento è perfettamente analogo al caso 2. anche per i casi $\varphi \doteq \varphi_1 \vee \varphi_2$ e $\varphi \doteq \varphi_1 \to \varphi_2$
4. se $\varphi \doteq \forall x_i.\psi$ e se la tesi è vera per ψ allora v_1 e v_2 coincidono su $\mathrm{vl}(\psi) \setminus \{x_1\}$ e per definizione $M \vDash \{v_1\}\, \varphi$ è vero se e solo se per ogni $a \in D$ è vero $M \vDash \left\{v_1 \left[{}^{a}/_{x_i}\right]\right\} \psi$ ma fissato $a \in D$ le due valutazioni $v_1 \left[{}^{a}/_{x_i}\right]$ e $v_2 \left[{}^{a}/_{x_i}\right]$ coincidono su $\mathrm{vl}(\psi)$ quindi fissato $a \in D$ è vero $M \vDash \left\{v_1 \left[{}^{a}/_{x_i}\right]\right\} \psi$ se e solo se è vero $M \vDash \left\{v_2 \left[{}^{a}/_{x_i}\right]\right\} \psi$ ovvero $M \vDash \{v_1\}\, \varphi$ è vero se e solo se $M \vDash \{v_2\}\, \varphi$ è vero;

[3] È la prima volta che usiamo questo argomento ma è utile farci particolare attenzione in quanto sarà utilizzato spesso

5. il procedimento è perfettamente analogo al caso 4. anche per il caso $\varphi \doteq \exists\, x_i.\psi$.

□

Definizione 2.1.4: *Formula chiusa*

Una formula φ si dice *enunciato* o *formula chiusa* se non ha variabili libere ($\mathrm{vl}(\varphi) = \varnothing$).

Corollario 2.1.4.1

Se φ è una formula chiusa allora date due qualunque valutazioni v_1 e v_2 vale $M \vDash \{v_1\}\,\varphi$ se e solo se $M \vDash \{v_2\}\,\varphi$.

Definizione 2.1.5

Data una struttura M ed una formula chiusa φ diciamo che M è *un modello di* φ (ovvero $M \vDash \varphi$) se in ogni contesto $v : \mathrm{Var} \to D$ vale $M \vDash \{v\}\,\varphi$.
Se invece $\mathrm{vl}(\varphi) = \{x_{i_1}, \dots, x_{i_n}\}$ allora allora diciamo che $M \vDash \varphi$ se M è un modello della formula chiusa

$$\forall\, x_{i_1} \dots \forall\, x_{i_n}.\varphi$$

Definizione 2.1.6: *Formula logicamente valida*

Una L-formula φ si dice *logicamente valida* se per ogni L-struttura M è vero $M \vDash \varphi$.

Esempio 2.1.2 Fissiamo una struttura $M = (S, P)$ dove P è l'unico simbolo del linguaggio ed è un simbolo di relazione unaria.
Vediamo come la semantica di Tarski interpreta

$$M \vDash \exists\, x.\,(P(x) \to \forall\, y.P(y)) \tag{2.1}$$

dove la parte in nero è effettivamente una formula nella teoria mentre quella in rosso è la notazione metateorica che usiamo per significare che M è, indipendentemente dal contesto, un modello della formula.
Come primo passo 'spacchettiamo' la notazione mostrando la presenza dei contesti

$$\forall\, v \in {}^{\mathbb{N}}S^{4}.M \vDash \{v\} \exists\, x.\,(P(x) \to \forall\, y.P(y))$$

dove ancora una volta tutti i simboli in rosso sono metateorici; adesso interpretando l'esiste otteniamo che

$$\forall\, v \in {}^{\mathbb{N}}S. \exists\, a \in S. M \vDash \{v\,[a/x]\}\,(P(x) \to \forall\, y.P(y))$$

quindi interpretando l'uguale si ottiene che

$$\forall\, v \in {}^{\mathbb{N}}S. \exists\, a \in S.\,(M \vDash \{v\,[a/x]\}\,P(x)) \to (M \vDash \{v\,[a/x]\}\,\forall\, y.P(y))$$

ed interpretando fino alla fine le formule rimaste si ottiene:

$$\forall\, v \in {}^{\mathbb{N}}S. \exists\, a \in S.\,(v\,[a/x]\,(x) \in P_M) \to \left(\forall\, b \in S. v\left[a/x, b/y\right](y) \in P_M\right)$$

e per definizione della valutazione delle variabili $v\,[a/x]\,(x) = a$ e $v\left[a/x, b/y\right](y) = b$ qualunque sia v, quindi possiamo rimuovere il $\forall\, v$ ottenendo che l'interpretazione con la semantica di Tarski della formula è

$$\exists\, a \in S.\,(a \in P_M) \to (\forall\, b \in S. b \in P_M)$$

ed è chiaro che al livello logico che questa vuol dire la stessa cosa della formula iniziale in nero (2.1).

[4] Con la notazione ${}^{A}B$ dove A e B sono insiemi indichiamo l'insieme delle funzioni da A in B

Esercizio 2.1 In quali strutture $M = (S, P)$ dove P è un solo predicato unario la formula dell'esempio precedente (2.1.2) è soddisfatta?

Svolgimento. Se per ogni elemento $a \in S$ vale l'ipotesi dell'implicazione allora tautologicamente vale anche la tesi dell'implicazione; ovvero la formula è vera.

Altrimenti essendo M una struttura S è non vuoto, quindi esiste $a \in S$ tale che l'ipotesi dell'implicazione è falsa da cui, indipendentemente dalla tesi, segue che con tale a l'implicazione è vera; cioè anche in questo caso la formula è vera.

Riassumendo la formula è soddisfatta in ogni struttura $M(S, P)$ valida nel dato linguaggio. □

2.2 Sostituzioni

Nelle formule algebriche possiamo sostituire le variabili con altre formule algebriche mantenendone il valore di verità, ad esempio nell'identità $(x-y)(x+y) = x^2 - y^2$ potremmo sostituire $3x$ ad y ottenendo $(x-3x)(x+3x) = x^2 - (3x)^2$ ovvero $-8x^2 = -8x^2$ che è ancora una identità valida.

Questo non è vero in generale nelle formule logiche, infatti un controesempio è la formula $\exists y.x < y$ che nei numeri naturali è vera ma se ad x sostituiamo $y+1$ otteniamo $\exists y.y+1 < y$ che nei numeri naturali è falsa.

Questo è detto problema della cattura delle variabili in quanto viene dal fatto che abbiamo già 'utilizzato' la y.

In altri ambiti, soprattutto nell'informatica, risolvere questo problema senza imporsi limitazioni troppo forti può essere complesso ma in questo caso ci basterà limitarsi ad usare nomi diversi per le variabili in casi specifici e questo non porterà alcuna vera limitazione.

Definizione 2.2.1: *Sostituibilità*

Data una L-formula φ, un L-termine t si dice *sostituibile per* x_k *in* φ se nessuna occorrenza libera di x_k in φ si trova in una sottoformula del tipo $\forall x_i.\psi$ o $\exists x_i.\psi$ dove x_i è una variabile in $\mathrm{var}(t)$.
Più formalmente definiamo la sostituibilità per ricorsione strutturale dicendo che t è sostituibile per x_k in φ:

- se φ è atomica;
- se $\varphi \doteq \neg\psi$ con t sostituibile per x_k in ψ;
- se
$$\varphi \doteq \psi \wedge \theta \quad \text{o} \quad \varphi \doteq \psi \vee \theta \quad \text{o} \quad \varphi \doteq \psi \to \theta$$
con t sostituibile per x_k sia in ψ che in θ;
- se
$$\varphi \doteq \exists x_i.\psi \quad \text{o} \quad \varphi \doteq \forall x_i.\psi$$
se $x_k \notin \mathrm{vl}(\varphi)$ oppure se $x_k \in \mathrm{vl}(\varphi)$ ed $x_i \notin \mathrm{var}(t)$ con t sostituibile per x_k in ψ.

Definizione 2.2.2: *Sostituzione*

Dati una L-formula φ, un L-termine t ed una variabile x_k tali che t è sostituibile per x_k in φ definiamo $\varphi\left[{}^{t}\!/_{x_k}\right]$ cioè φ *con* t *sostituito per* x_k come la formula che si ottiene da φ rimpiazzando ogni occorrenza libera in φ del termine x_k con il termine t.

Nota 2.2.1 Formalmente non abbiamo usato la notazione classica $\varphi(x)$ ma in generale scrivere $\varphi(x, y, z)$ sarà un modo per anticipare che più avanti vorremo scegliere dei termini t_1, t_2, t_3 per scrivere $\varphi(t_1, t_2, t_3)$ al posto della più complessa formula formale $\varphi\left[{}^{t_1}\!/_{x}, {}^{t_2}\!/_{y}, {}^{t_3}\!/_{z}\right]$.

Lemma 2.2.3

Le sostituzioni commutano con le valutazioni, ovvero se t è un termine sostituibile per x_i nella formula φ allora data una valutazione delle variabili v:

$$M \vDash \{v\}\,\varphi\left[{}^{t}\!/_{x_i}\right] \quad \Longleftrightarrow \quad M \vDash \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}\varphi$$

Esercizio 2.2 Dimostrare il lemma precedente.
(Suggerimento: procedere per induzione strutturale su φ)

Svolgimento. Procediamo per induzione strutturale su φ.

Per il passo base chiaramente se $\varphi \doteq \top$ o $\varphi \doteq \bot$ non c'è nulla da dimostrare.

Sempre nel passo base se $\varphi \doteq t_1 = t_2$ allora per la semantica di Tarski vale $M \vDash \{v\}\,\varphi\left[{}^{t}\!/_{x_i}\right]$ se e solo se

$$\{v\}\,t_1\left[{}^{t}\!/_{x_i}\right] = \{v\}\,t_2\left[{}^{t}\!/_{x_i}\right] \tag{2.2}$$

Usiamo un ulteriore ragionamento per induzione (questa volta sulla complessità del termine s) per vedere che

$$\{v\}\,s\left[{}^{t}\!/_{x_i}\right] = \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}s$$

- per il passo base se $s \doteq c$ è una costante allora non c'è niente da dimostrare in quanto la valutazione di s non dipende da v e la sostituzione non cambia il termine;
- sempre per il passo base se $s \doteq x_j$ con $j \neq i$ vale la stessa cosa del caso costante;
- per concludere il passo base se $s \doteq x_i$ allora per definizione di sostituzione $\{v\}\,s\left[{}^{t}\!/_{x_i}\right] = \{v\}\,t$ e per definizione della valutazione vale

$$\{v\}\,t = \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}x_i \quad \left(= \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}s\right)$$

- per il passo induttivo se $s = f(t_1, \ldots, t_k)$ dove f è un simbolo di funzione k-ario e se per ipotesi induttiva la tesi vale per $t_1, \ldots, t_k$ allora

$$\{v\}\,s\left[{}^{t}\!/_{x_i}\right] = \{v\}\,f\left(t_1\left[{}^{t}\!/_{x_i}\right], \ldots, t_k\left[{}^{t}\!/_{x_i}\right]\right) = f_M\left(\{v\}\,t_1\left[{}^{t}\!/_{x_i}\right], \ldots, \{v\}\,t_k\left[{}^{t}\!/_{x_i}\right]\right)$$

e per ipotesi induttiva quest'ultimo equivale a

$$f_M\left(\left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}t_1, \ldots, \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}t_k\right) = \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}f(t_1, \ldots, t_k) \quad \left(\left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}s\right)$$

Da questo fatto segue che l'equazione (2.2) equivale a dire che

$$\left\{v\left[{}^{\{v\}\,t}\!/_{x_k}\right]\right\}t_1 = \left\{v\left[{}^{\{v\}\,t}\!/_{x_k}\right]\right\}t_2$$

da cui sempre per la semantica di Tarski si ottiene la tesi. Il ragionamento è analogo per l'ultimo passo base $\varphi \doteq r(t_1, \ldots, t_k)$ infatti $M \vDash \{v\}\,r(t_1, \ldots, t_k)\left[{}^{t}\!/_{x_i}\right]$ se e solo se

$$\left(\{v\}\,t_1\left[{}^{t}\!/_{x_i}\right], \ldots, \{v\}\,t_k\left[{}^{t}\!/_{x_i}\right]\right) \in r_M$$

e questo per quanto dimostrato per i termini equivale a dire che

$$\left(\left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}t_1, \ldots, \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}t_k\right) \in r_M \tag{2.3}$$

che per definizione della valutazione sulle formule atomiche vale se e solo se

$$M \vDash \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}r(t_1, \ldots, t_k) \tag{2.4}$$

Per il passo induttivo separiamo diversi casi:

- Se $\varphi \doteq \neg\psi$ allora $M \vDash \{v\}\,\varphi\left[{}^{t}\!/_{x_i}\right]$ per la semantica di Tarski (e per definizione di sostituzione) se e solo se $M \nvDash \{v\}\,\psi\left[{}^{t}\!/_{x_i}\right]$ e per ipotesi induttiva questo vale se e solo se

$$M \nvDash \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}\psi$$

da cui segue per la semantica di tarski che la tesi vale anche per φ.

- Analogamente al caso precedente se $\varphi \doteq \psi \vee \sigma$ allora $M \vDash \{v\}\,\varphi\left[{}^{t}\!/_{x_i}\right]$ per la semantica di Tarski (e per definizione di sostituzione) se e solo se $M \vDash \{v\}\,\psi\left[{}^{t}\!/_{x_i}\right]$ oppure $M \vDash \{v\}\,\sigma\left[{}^{t}\!/_{x_i}\right]$ e per ipotesi induttiva questo vale se e solo se

$$M \vDash \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}\psi \quad \vee \quad M \vDash \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}\sigma$$

da cui segue per la semantica di tarski che la tesi vale anche per φ.

- I casi della congiunzione e dell'implicazione sono uguali al precedente sostituendo le disgiunzioni con l'opportuna relazione.

- Se $\varphi \doteq \forall\, x_j.\psi$ distinguiamo due sottocasi:

  - se $i = j$ allora $\varphi \equiv \varphi\left[{}^{t}\!/_{x_i}\right]$ ed $x_i \notin \mathrm{vl}(\varphi)$ quindi per la proposizione 2.1.3 vale

$$M \vDash \{v\}\,\varphi\left[{}^{t}\!/_{x_i}\right] \quad \Longleftrightarrow \quad M \vDash \left\{\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}\varphi$$

  - altrimenti $i \neq j$ quindi per definizione di sostituzione $\varphi\left[{}^{t}\!/_{x_i}\right] \equiv \forall\, x_j.\left(\psi\left[{}^{t}\!/_{x_i}\right)\right)$ ovvero per la semantica di Tarski $M \vDash \{v\}\,\varphi\left[{}^{t}\!/_{x_i}\right]$ se e solo se per ogni elemento della struttura $a \in M$ vale

$$M \vDash \left\{v\left[{}^{a}\!/_{x_j}\right]\right\}\psi\left[{}^{t}\!/_{x_i}\right]$$

  e per ipotesi induttiva questo vale se e solo se per ogni $a \in M$

$$M \vDash \left\{v\left[{}^{a}\!/_{x_j}, {}^{\left\{v\left[{}^{a}\!/_{x_j}\right]\right\}\,t}\!/_{x_i}\right]\right\}\psi$$

  ovvero per la semantica di Tarski vale se e solo se per ogni $a \in M$

$$M \vDash \left\{v\left[{}^{\left\{v\left[{}^{a}\!/_{x_j}\right]\right\}\,t}\!/_{x_i}\right]\right\}\varphi$$

  per concludere basta separare ancora due sottocasi:

  - ⋆ se $x_i \notin \mathrm{vl}(\varphi)$ allora per la proposizione 2.1.3 possiamo sostituire ad x_i 'quello che vogliamo', in particolare quindi questo vale se e solo se

$$M \vDash \left\{v\left[{}^{\{v\}\,t}\!/_{x_i}\right]\right\}\varphi$$

  - ⋆ altrimenti $x_i \in \mathrm{vl}(\varphi)$ ed allora per sostituibilità di t per x_i in φ deve necessariamente valere che $x_j \notin \mathrm{var}(t)$ allora sempre per la proposizione 2.1.3 per qualunque $a \in M$ vale

$$\{v\}\,t \equiv \left\{v\left[{}^{a}\!/_{x_j}\right]\right\}t$$

    ovvero anche in questo caso vale la tesi per φ.

- Rimane solo il caso di $\varphi \doteq \exists\, x_j.\psi$ che è esattamente analogo al caso precedente sostitutendo tutti i quantificatori universali con quantificatori esistenziali.

□

2.3 Teorie

In generale è interessante parlare di teorie matematiche, queste non sono altro che insiemi di formule, assiomi, che supponiamo essere vere, ad esempio la teoria dell'aritmetica di Peano o la teoria dei campi completi algebricamente chiusi di caratteristica zero.

Definizione 2.3.1: *L-teoria*

Dato un linguaggio L diciamo *L-teoria* un insieme di L-formule.

Definizione 2.3.2: *Modello di una teoria*

Data una L-teoria T ed una L-struttura M diciamo che $M \vDash T$, ovvero che M *è un modello di* T, se per ogni $\varphi \in T$ vale $M \vDash \varphi$.

Definizione 2.3.3: *Conseguenza logica*

Data una L-teoria T ed una L-formula φ diciamo che $T \vDash \varphi$, ovvero che φ *è conzeguenza logica di* T (o che T soddisfa φ), se per ogni L-struttura M se M è un modello di T allora $M \vDash \varphi$.

Nota 2.3.1 Anche l'insieme di formule vuoto è una teoria, quindi è legittimo usare il simbolismo $\vDash \varphi$ per dire che $\varnothing \vDash \varphi$ ovvero che φ è logicamente valida (2.1.6).

Definizione 2.3.4: *Teoria coerente*

Una teoria si dice *coerente* se ha almeno un modello.

Definizione 2.3.5: *Teoria completa*

Una teoria si dice *completa* se per ogni formula chiusa φ vale esattamente una tra $T \vDash \varphi$ e $T \vDash \neg\varphi$.

Osservazione 2.3.2 Una teoria T è coerente se e solo se $T \nvDash \bot$ infatti se T ammette almeno un modello M allora $M \nvDash \bot$ e se T non ammette alcun modello è vero a vuoto che $T \vDash \bot$.
Inoltre se T è completa allora è necessariamente anche coerente.

È facile costruire una teoria non coerente ma non sempre è immediato mostrare che una data teoria è incoerente, in generale una strategia per mostrare che T è incoerente è di mostrare che $T \vDash \bot$ mentre per mostrare che è coerente basta esibirne un modello, ad esempio per la teoria dei gruppi basta esibire un gruppo e verificare che soddisfa le formule che descrivono la teoria; come esempio adesso descriviamo esplicitamente la teoria dei gruppi.

Esempio 2.3.3: *teoria dei gruppi* Come linguaggio prendiamo $L = \{e, \_^{-1}, \_ \cdot \_\}$; possiamo definire la teoria dei gruppi come T_{grp}:

$$\begin{aligned} T_{grp} = \{&\forall x.\forall y.\forall z.\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \\ &\forall x.\ x \cdot e = x \wedge e \cdot x = x \\ &\forall x.\ x \cdot x^{-1} = e \wedge x^{-1} \cdot x = e\} \end{aligned}$$

i suoi modelli sono esattamente i gruppi, quindi questa teoria è coerente; però è altrettanto ovvio che non è completa, ad esempio la formula

$$\exists x.\neg(x = e) \wedge x \cdot x = e$$

ovvero *esiste un elemento di grado esattamente due* è vera nel gruppo finito $\mathbb{Z}/2\mathbb{Z}$ ma è falsa nel modello del gruppo banale.
Invece potremmo costruire la teoria dei campi algebricamente chiusi di caratteristica zero e questa risulterà essere completa, anche se dimostrare questo non è banale e forse lo faremo più avanti.

Definizione 2.3.6: *Teoria completa di un modello*

Dato un modello M si dice *Teoria completa di* M la teoria $\mathrm{Th}(M)$ formata da tutte le formule φ tali che $M \vDash \varphi$.

Osservazione 2.3.4 Fissato un linguaggio $L = (R, F, ar)$ e dato un qualunque modello M la teoria $\mathrm{Th}(M)$ è effettivamente una teoria completa, si potrebbe pensare che anche nell'altra direzione una qualunque teoria completa T caratterizzi un modello a meno di una nozione di isomorfismo, in realtà in generale questo non è vero, ma è vero se ci restringiamo al caso in cui T ammette un modello con dominio finito.

Definizione 2.3.7: *Morfismi di strutture*

Date due strutture $M = (D, i)$ ed $M' = (D', i')$ diciamo *morfismo di strutture* $\varphi : M \to M'$ una funzione $\varphi : D \to D'$ tale che:

- per ogni simbolo di relazione $r \in R$ e per ogni $(ar(r))$-upla $(x_1, \dots, x_{ar(r)}) \in D^{ar(r)}$ vale
$$(x_1, \dots, x_{ar(r)}) \in r_M \quad \Longrightarrow \quad (\varphi(x_1), \dots, \varphi(x_{ar(r)})) \in r_{M'}$$
- per ogni simbolo di funzione $f \in F$ e per ogni $(ar(r))$-upla $(x_1, \dots, x_{ar(r)}) \in D^{ar(r)}$ vale
$$\varphi \circ f_M(x_1, \dots, x_{ar(r)}) \quad = \quad f_{M'}(\varphi(x_1), \dots, \varphi(x_{ar(r)}))$$

Osservazione 2.3.5 Una funzione $f : D \to D'$ è un morfismo di strutture se e solo se preserva le formule atomiche, ovvero se e solo se data una qualunque formula atomica $\varphi(x_1, \dots, x_k)$ (dove $\mathrm{vl}(\varphi) \subseteq \{x_1, \dots, x_k\}$) e data una qualunque k-upla $(a_1, \dots, a_k) \in D^k$ vale
$$M \vDash \varphi(a_1, \dots, a_k) \quad \Longrightarrow \quad N \vDash \varphi(f(a_1, \dots, a_k))$$
Infatti se f è un morfismo allora iniziamo con una induzione strutturale sui termini per mostrare che dato un qualunque L-termine $t(x_1, \dots, x_k)$ dove $\mathrm{var}(t) \subseteq \{x_1, \dots, x_k\}$ per ogni k-upla $(a_1, \dots, a_k) \in D^k$ vale
$$f(t(a_1, \dots, a_k)) = t(f(a_1), \dots, f(a_k)) \tag{2.5}$$
- se $t \doteq c$ è una costrante allora la (2.5) è verificata in quanto per definizione $f(t) = c_N$;
- se $t \doteq x_i$ è una variabile allora per ipotesi $i \in \{1, \dots, k\}$ e la (2.5) diventa la tautologia $f(a_i) = f(a_i)$;
- se $t \doteq F(t_1, \dots, t_h)$ dove F è un simbolo di funzione h-ario supponiamo come ipotesi induttiva che la tesi valga per $t_1, \dots, t_h$; fissando per ogni $i \in \{1, \dots, h\}$
$$b_i \doteq t_1(a_1, \dots, a_k)$$
per definizione di morfismo e per l'ipotesi indutiva vale
$$f(t(a_1, \dots, a_k)) = f(F_M(b_1, \dots, b_h)) = F_N(f(b_1), \dots, f(b_h)) = t(f(a_1), \dots, f(a_k))$$

Vediamo adesso i casi delle varie formule atomiche:

- se $\varphi \doteq \top$ oppure $\varphi \doteq \bot$ non c'è niente da dimostrare;
- se $\varphi \doteq t_1 = t_2$ e allora data una qualunque k-upla $(a_1, \dots, a_k) \in D$ per quanto dimostrato sui termini se
$$M \vDash t_1(a_1, \dots, a_k) = t_2(a_1, \dots, a_k)$$
allora
$$t_1(f(a_1), \dots, f(a_k)) = f(t_1(a_1, \dots, a_k)) = f(t_2(a_1, \dots, a_k)) = t_2(f(a_1), \dots, f(a_k))$$
ovvero
$$N \vDash t_1(f(a_1), \dots, f(a_k)) = t_2(f(a_1), \dots, f(a_k))$$

- se $\varphi \doteq r(t_1, \ldots, t_h)$ allora per definizione di morfismo data una k-upla $(a_1, \ldots, a_k) \in D$ vale

$$M \vDash r\,(t_1(a_1, \ldots, a_k), \ldots, t_2(a_1, \ldots, a_k)) \implies N \vDash r\,(f(t_1(a_1, \ldots, a_k)), \ldots, f(t_2(a_1, \ldots, a_k)))$$

Se invece f preserva le formule atomiche allora è un morfismo infatti:

- se F è un simbolo di funzione k-ario allora la funzione f preserva la formula atomica $\varphi \doteq F(x_1, \ldots, x_k) = x_0$, quindi data una qualunque k-upla $(a_1, \ldots, a_k) \in D^k$ se $a \doteq F_M(a_1, \ldots, a_k)$ vale
$$N \vDash F(f(a_1), \ldots, f(a_k)) = f(a)$$
ovvero
$$f(F_M(a_1, \ldots, a_k)) \doteq f(a) = F_N(f(a_1), \ldots, f(a_k))$$
- se R è un simbolo di relazione k-ario allora f preserva la formula atomica $\varphi \doteq r(x_1, \ldots, x_k)$, quindi data una qualunque k-upla $(a_1, \ldots, a_k) \in D^k$ vale

$$(a_1, \ldots, a_k) \in r_M \iff M \vDash r(a_1, \ldots, a_k) \implies$$
$$\implies N \vDash r(f(a_1), \ldots, f(a_k)) \iff (f(a_1), \ldots, f(a_k)) \in r_N$$

Definizione 2.3.8: *Immersioni ed isomorfismi di stutture*

Un morfismo di strutture $f : M \to M'$ si dice *immersione di strutture* se, intesa come funzione dal dominio D nel dominio D', f è iniettiva.
Una immersione di strutture $f : M \to M'$ si dice *isomorfismo* se, ancora intesa come funzione dal dominio D nel dominio D', f è surgettiva e se la sua inversa insiemistica $f^{-1} : D' \to D$ è a sua volta un morfismo di strutture $f : M' \to M$.

Esercizio 2.3 Dimostra che se T è completa ed M è un modello di T con dominio finito allora tutti i modelli di T sono isomorfi ad M.

L'osservazione 6.5.1 è una soluzione di questo esercizio.

Nota 2.3.6 Vedremo più avanti che se T ammette un modello infinito allora ammette un modello per ogni cardinalità maggiore o uguale a $|L|$ e questo preclude quindi che una teoria al primo ordine con modelli infiniti possa caratterizzare univocamente un modello.
Il meglio che possiamo sperare come caratterizzazione è dunque di esibire teorie complete, non caratterizzando una struttura ma almeno tutti gli enunciati che sono veri e falsi nella struttura.

Esempio 2.3.7 Descriviamo ora la teoria degli ordini lineari densi senza estremi, quindi $L = \{\_ < \_\}$ e

$$\begin{aligned} T_{DLO} = \{&\forall x.\forall y.\forall z.\ (x < y \wedge y < z) \to x < z \\ &\forall x.\ \neg(x < x) \\ &\forall x.\forall y.\ x < y \wedge y < x \wedge y = x \\ &\forall x.\forall y.x < y \to (\exists z.x < z \wedge z < y) \\ &\forall x.(\exists y.x < y) \wedge (\exists y.y < x)\} \end{aligned}$$

anche questa è coerente infatti $\mathbb{Q}$ è un suo modello, vedremo in seguito che si può dimostrare la sua completezza dal fatto che è $\aleph_0$-categorica, cioè che ha un solo modello di cardinalità $\aleph_0$, ma adesso possiamo passare da una altra proprietà di questa teoria per dimostrarne la completezza.

Definizione 2.3.9: *Formule equivalenti (semanticamente[5])*

Due L-formule φ e ψ si dicono *logicamente equivalenti* se ciascuna è conseguenza logica dell'altra, ovvero se

$$\varphi \vDash \psi \quad \wedge \quad \psi \vDash \varphi$$

invece data una L-teoria T queste si dicono *equivalenti in* T se

$$T, \varphi \vDash \psi \quad \wedge \quad T, \psi \vDash \varphi$$

Osservazione 2.3.8 Date due formule φ e ψ queste sono logicamente equivalenti se e solo se $\vDash \varphi \longleftrightarrow \psi$.
Analogamente invece sono equivalenti in T se e solo se $T \vDash \varphi \longleftrightarrow \psi$.

Definizione 2.3.10: *Proprietà dell'eliminazione dei quantificatori*

Data una L-teoria T diciamo che questa *ha l'eliminazione dei quantificatori* se data una qualunque L-formula φ esiste una L-formula ψ senza quantificatori (cioè che non usa *per ogni* ed *esiste*) equivalente a φ in T.

Esercizio 2.4: *Forma normale disgiuntiva* Ogni formula senza quantificatori φ può essere scritta in forma normale disgiuntiva cioè è equivalente ad una formula

$$\bigvee_{i=1}^{n} \left(\bigwedge_{j=1}^{m_n} A_{i,j} \right)$$

dove le $A_{i,j}$ sono tutte formule atomiche o negazione di formule atomiche.

Svolgimento. Procediamo per induzione strutturale su φ.

Se φ è atomica o negazione di una formula atomica allora è in forma normale disgiuntiva.

Se φ è una disgiunzione di formule che si possono scrivere in forma normale disgiuntiva allora ovviamente anche φ si può scrivere in forma normale disgiuntiva.

Per vedere i casi di $\wedge$ e $\neg$ vediamo prima alcuni casi particolari.

Se φ è composta solo da congiunzioni o solo da disgiunzioni di formule atomiche e negazioni di formule atomiche allora è in forma normale disgiuntiva.

Se φ è una formula composta da con congiunzioni o disgiunzioni di formule atomiche e negazioni di formule atomiche possiamo utilizzare le leggi di De Morgan ($A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$) per portarla in forma normale disgiuntiva, infatti procediamo per induzione sul numero di disgiunzioni:

- al passo base con nessuna disgiunzione si è in forma normale disgiuntiva
- al passo induttivo se supponiamo che per ogni $m < n$ con al più m disgionzioni ed un qualunque numero finito di congiunzioni di atomiche e negazioni di atomiche ci si può ricondurre ad una forma normale disgiuntiva sia φ una formula scritta come congiunzione o disgiunzione di $k \geq n \geq 1$ formule atomiche e negazioni di atomiche dove n di queste sono disgiunzioni, se esistono φ_1 e φ_2 formule non vuote tali che

  $$\varphi = \varphi_1 \vee \varphi_2$$

  allora per l'ipotesi induttiva φ può essere scritta in forma normale disgiuntiva, altrimenti $k > n$ e devono esistere φ_1 e φ_2 formule non vuote tali che

  $$\varphi = \varphi_1 \wedge \varphi_2$$

  e senza perdita di generalità possiamo supporre che φ_2 contenga almeno una disgiunzione; dato che la congiunzione è associativa ($A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$) a meno di ripetere al più $k - n$

[5] Specificheremo che questa equivalenza tra formule è 'semantica' più avanti per distinguerla da una equivalenza 'sintattica' basata sulle dimostrazioni anche se in realtà grazie ai teoremi di completezza e correttezza vedremo che le due equivalenze sono isomorfe

volte l'applicazione della proprietà associativa possiamo quindi supporre che φ_2 sia della forma come $\psi_1 \vee \psi_2$ con ψ_1 e ψ_2 entrambe che contengono al più $n-1$ disgiunzioni, quindi applicando De Morgan

$$\varphi \equiv (\varphi_1 \wedge \psi_1) \vee (\varphi_1 \wedge \psi_2)$$

ed entrambe le due componenti possono essere ricondotte in forma normale disgiuntiva per ipotesi induttiva.

Se $\varphi \doteq \neg\psi$ con ψ che può essere scritta in forma normale disgintiva $\psi \equiv \bigvee_{i=1}^{n} \left(\bigwedge_{j=1}^{m_n} A_{i,j} \right)$ allora possiamo scrivere φ come

$$\bigwedge_{i=1}^{n} \left(\bigvee_{j=1}^{m_n} \neg A_{i,j} \right)$$

dove se $A_{i,j}$ era una negazione di atomica possiamo interpretare $\neg A_{i,j}$ come una formula atomica, quindi φ può essere scritta combinazione di congiunzioni e disgiunzioni di formule atomiche o negazione di atomiche.

Se $\varphi \doteq \psi \wedge \theta$ con ψ e θ che possono essere scritte in forma normale disgiuntiva allora φ equivale ad una formula costruita da congiunzioni o disgiunzioni di formule atomiche e negazioni di atomiche quindi può essere scritta in forma normale disgiuntiva.

Se $\varphi \doteq \psi \to \theta$ con ψ e θ che possono essere scritte in forma normale disgiuntiva allora

$$\varphi \equiv \theta \vee (\neg\psi)$$

con entrambe le componenti che possono essere scritte in forma normale disgiuntiva. □

Esercizio 2.5 Mostrare che la teoria T_{DLO} ha l'eliminazione dei quantificatori.
(Suggerimento: procedere per induzione)

Svolgimento. Data una formula φ vogliamo mostrare che esiste una formula senza quantificatori ψ che in ogni modello di T_{DLO} ha lo stesso valore di verità di φ, per brevità diremo che φ e ψ sono equivalenti e procediamo per induzione sulla complessità della formula.

Chiaramente per il passo base se φ è una formula atomica allora è senza quantificatori, quindi rispetta la tesi. Per il passo induttivo se $\varphi \doteq \neg\varphi_1$ ed esiste ψ_1 senza quantificatori equivalente a φ_1 allora $\neg\psi_1$ è senza quantificatori ed equivalente a φ.

Analogamente il passo induttivo si verifica anche con

$$\varphi \doteq \varphi_1 \wedge \varphi_2 \qquad \varphi \doteq \varphi_1 \vee \varphi_2 \qquad \varphi \doteq \varphi_1 \to \varphi_2$$

mentre è non banale il caso di $\varphi \doteq \exists x_i.\varphi_1$. Per l'ipotesi induttiva possiamo supporre senza perdita di generalità che φ_1 sia senza quantificatori.

Per l'esercizio precedente φ_1 può essere scritta in forma normale disgiuntiva come

$$\bigvee_{i=1}^{n} \left(\bigwedge_{j=1}^{m_n} A_{i,j} \right)$$

e vale l'equivalenza

$$\exists x_l. \bigvee_{i=1}^{n} \left(\bigwedge_{j=1}^{m_n} A_{i,j} \right) \equiv \bigvee_{i=1}^{n} \left(\exists x_l. \bigwedge_{j=1}^{m_n} A_{i,j} \right)$$

quindi ci siamo ricondotti a cercare di vedere che una qualunque formula della forma

$$\exists x_l. \bigwedge_{i=1}^{n} A_i \tag{2.6}$$

dove A_i è una delle seguenti:

$$x_{k_i} < x_{h_i} \qquad x_{k_i} = x_{h_i} \qquad x_{h_i} \leq x_{k_i} \qquad x_{k_i} \neq x_{h_i}$$

dove $a \leq b$ e $a \neq b$ non sono propriamente parte del linguaggio della teoria ma con queste vogliamo rispettivamente dire $\neg(b < a)$ e $\neg(a = b)$.

Inoltre se $x_l \neq x_{k_j}$ e $x_l \neq x_{h_j}$ allora vale anche l'equivalenza

$$\exists x_l. \bigwedge_{i=1}^{n} A_i \equiv A_j \wedge \exists x_l. \bigwedge_{\substack{i=1 \\ i \neq j}}^{n} A_i$$

quindi senza perdita di generalità possiamo supppore che per ogni i uno tra k_i ed h_i sia esattamente l. Inoltre se esiste una formula A_j del tipo $x_l = x_l$ questa può essere rimossa in quanto è sempre vera, se c'è una formula A_j del tipo $x_l = x_i$ con $i \neq l$ questa può essere rimossa sostituendo tutte le occorrenze di x_l con x_i e poi portare tutti i termini al di fuori dell'*esiste*, trasformando la formula in una senza quantificatori.

Se invece esiste una formula A_j del tipo $x_l \neq x_l$ allora questa è sempre falsa, quindi $\exists x_l.A_j \equiv \bot$ che è senza quantificatori, se invece esiste una formula A_j del tipo $x_l \neq x_i$ possiamo sostituirla con $x_l < x_i \vee x_l > x_i$ ovvero possiamo ricondurci a due *esiste* in cui abbiamo rimosso la disugualianza ponendo

$$\exists x_l.A_j \wedge A \equiv \exists x_l.(x_l < x_i \wedge A) \vee (x_l > x_i \wedge A) \equiv (\exists x_l.x_l < x_i \wedge A) \wedge (\exists x_l.x_l > x_i \wedge A)$$

con questi accorgimenti possiamo quindi considerare il caso in cui le formule A_i possono essere soltanto dei tipi

$$x_{k_i} < x_{h_i} \qquad \text{o} \qquad x_{h_i} \leq x_{k_i} \tag{2.7}$$

Per vedere che queste formule possono essere ricondotte in T_{DLO} a formule senza quantificatori procediamo per induzione sul numero n di formule atomiche in (2.6).

per il passo base con $n = 1$ la formula è $\exists x_l.A_1$ e tutte ed due le possibilità per A_1 ottenute da (2.7) sono sempre vere in quanto ogni modello di T_{DLO} è senza estremi.

Per il passo induttivo vediamo che la formula $\exists x_l.A_1 \wedge A_2 \wedge A$ dove A è composto da $n-2$ formule come quelle in (2.7), ed eventualmente zero formule cioè $A = \top$, può essere ricondotta a $\exists x_l.B \wedge A$ dove anche B o è sempre vera o è sempre falsa o è una formula come in (2.7), infatti:

- se $A_1 \doteq x_l < x_i$ ed $A_2 \doteq x_l < x_j$ con $i \neq l$ e $j \neq l$ allora $\exists x_l.A_1 \wedge A_2$ è sempre vera per ipotesi, quindi possiamo porre $B \doteq \top$ altrimenti se $i = l$ o $j = l$ la formula è sempre falsa, quindi possiamo porre $B \doteq \bot$;
- il ragionamento precedente è valido anche in tutti gli altri casi in cui x_l 'è dallo stesso lato' $A_1 \doteq x_i < x_l$ ed $A_2 \doteq x_j < x_l$, con $A_1 \doteq x_l \leq x_i$ ed $A_2 \doteq x_l \leq x_j$, con $A_1 \doteq x_i \leq x_l$ ed $A_2 \doteq x_j \leq x_l$, con $A_1 \doteq x_l \leq x_i$ ed $A_2 \doteq x_l < x_j$ e con $A_1 \doteq x_l < x_i$ ed $A_2 \doteq x_l \geq x_j$ con l'accortezza che se la disuguaglianza è con l'uguale è vera anche nel caso dove entrambi i termini della disuguaglianza hanno lo stesso indice
- se $A_1 \doteq x_l < x_i$ ed $A_2 \doteq x_j < x_l$ la formula $\exists x_l.A_1 \wedge A_2$ è vera per densità se e solo se $x_j < x_i$, quindi possiamo sostituire le due con $B \doteq x_j < x_i$, analogamente scambiando A_1 ed A_2 ed analogamente mettendo il *minore o uguale* invece del *minore* in B se entrambe le disuguaglianze sono larghe, con questi ultimi abbiamo quindi esaurito tutti i casi rimanenti.

Infine se $\varphi \doteq \forall x_i.\varphi_1$ allora questa è equivalente a $\neg\exists x_i.\neg\varphi_1$, che ricade nei casi precedenti. □

Osservazione 2.3.9 Se il linguaggio non ha costanti le uniche formule chiuse senza quantificatori possono essere solo la formula sempre vera e quella sempre falsa, quindi se una teoria in un linguaggio senza costanti ha l'eliminazione dei quantificatori questa è necessariamente completa. Se invece la teoria ha l'eliminazione dei quantificatori per farne seguire la completezza bisogna anche mostrare che per gli assiomi della teoria tutte le formule atomiche sono *decise* sulle costanti.

Esempio 2.3.10: *Teorie dell'aritmetica* Fissiamo il linguaggio $L = \{0, s, +, \cdot\}$ dove l'arietà è quella ovvia considerando 0 lo zero, s il successore, $+$ la somma e $\cdot$ il prodotto.
E mostriamo due teorie dell'aritmetica diverse, entrambe sottoinsiemi della teoria completa $\mathrm{Th}(\mathbb{N}, 0, s, +, \cdot)$ basata sul modello standard $\mathbb{N}$ dei numeri naturali.

Con questo linguaggio si dice aritmetica di Peano la teoria

$$\begin{aligned} T_{\mathrm{PA}} = \{ & \neg\exists\, x.s(x) = 0 \\ & s(x) = s(y) \to x = y \\ & x + 0 = x \\ & x + s(y) = s(x + y) \\ & x \cdot 0 = 0 \\ & x \cdot s(y) = (x \cdot y) + x \\ & \left(\forall\, x.\varphi \to \varphi\left[{}^{s(x)}\!/_{x}\right]\right) \wedge \varphi\left[{}^{0}\!/_{x}\right] \to \forall\, x.\varphi\} \end{aligned}$$

dove quello in rosso non è un solo assioma della teoria, è uno *schema di assioma* cioè un modo metateorico che usiamo per rappresentare il fatto che la teoria ha infiniti assiomi: uno per ogni L-formula φ corrispondente a sostituire φ nello schema.
Sarà utile anche un'altra caratterizzazione dell'aritmetica, detta teoria Q di Robinson:

$$\begin{aligned} Q = \{ & \neg\exists\, x.s(x) = 0 \\ & s(x) = s(y) \to x = y \\ & x + 0 = x \\ & x + s(y) = s(x + y) \\ & x \cdot 0 = 0 \\ & x \cdot s(y) = (x \cdot y) + x \\ & x \neq 0 \to \exists\, y.x = s(y)\} \end{aligned}$$

È banale che l'ultimo assioma di Q è dimostrabile per induzione nella teoria di Peano, ed in realtà effettivamente Q risulta essere strettamente più debole di T_{PA}, cioè non si possono dedurre tutti gli assiomi dell'induzione nella teoria di Peano a partire dalla teoria Q.

Esercizio 2.6 Dimostrare che l''assioma' di induzione non è conseguenza logica della teoria Q di Robinson.
(Suggerimento: cercare un modello di Q che non è modello di Peano)

Svolgimento. Consideriamo la struttura M che estende $\mathbb{N}$ con un punto 'all'infinito', cioè la struttura nel linguaggio dell'aritmetica che ha come dominio $D = \mathbb{N} \sqcup \{i\}$ e dove estendiamo le interpretazioni di $s, +, \cdot$ dicendo che: il successore di i è esattamente i, per la somma per ogni $x \in D$ poniamo

$$x + i = i + x = x \cdot i = i \cdot x = i$$

mentre per la moltiplicazione dato un qualunque x

$$\begin{aligned} i \cdot 0 &= 0 \\ i \cdot i &= i \\ s(x) \cdot i = i \cdot s(x) &= (i \cdot x) + x \end{aligned}$$

Questa struttura è ben definita infatti abbiamo definito univocamente il successore di ogni elemento, e la somma e moltiplicazione per ogni coppia di elementi.

Questo è un modello della Q di Robinson infatti:

- Non esiste un elemento di M il cui successore è zero;
- il successore è iniettivo;
- $x + 0 = x$ per ogni $x \in M$;
- $x + s(y) = s(x + y)$ infatti basta verificare due casi: se $x = i$ allora $x + s(y) = i = s(x + y)$ e se $y = i$ allora $x + s(y) = i = s(x + y)$;

- $x \cdot 0 = 0$ per ogni x per costruzione;
- $x \cdot s(y) = (x \cdot y) + x$ per costruzione;
- per costruzione se $x \neq 0$ allora esiste y tale che $x = s(y)$

Per concludere vediamo che questa struttura non è un modello dell'aritmetica di Peano infatti: se indichiamo $\varphi \doteq s(x) \neq x$ allora $M \not\models \forall x.\varphi$ però $M \models \forall x.\varphi \to \varphi\left[{}^{s(x)}/_{x}\right]$ e $M \models \varphi\left[{}^{0}/_{x}\right]$, e per la semantica di Tarski (2.1.2) questo contraddice l'assioma di induzione su φ. □

Dal fatto che Q è strettamente più debole di T_{PA} segue che Q non è completa, in realtà però neanche T_{PA} è completa: questo fatto è il primo teorema di incompletezza di Gödel, che vedremo più avanti.

Capitolo 3

Ultrafiltri ed ultraprodotti

Vediamo una tecnica per costruire un nuovo modello a partire da altri modelli che gia conosciamo, così da ottenere un modello dell'aritmetica di Peano che non sono i numeri naturali standard.

L'idea è di prendere infinite copie di $\mathbb{N}$ e farle 'votare a maggioranza' sulla verità di una formula; per fare questo dovremmo decidere come funziona la votazione, ad esempio la maniera più semplice è di scegliere una copia di $\mathbb{N}$ 'privilegiata' e porre che una formula è vera nel nuovo modello se è vera in quella copia di $\mathbb{N}$ ignorando le altre, ma questo produrrà un modello ovviamente non interessante in quanto isomorfo a quella singola componente, per ottenere una tipologia più interessante di 'votazione' introduciamo i filtri.

Definizione 3.0.1: *Filtro di insiemi*

Fissato un insieme I si dice *filtro su* $\mathscr{P}(I)$ un sottoinsieme $F \subset \mathscr{P}(I)$ tale che:

- $\varnothing \notin F \wedge I \in F$
- $A \in F \wedge A \subset B \to B \in F$
- $A \in F \wedge B \in F \to A \cap B \in F$

Rimanendo sull'interpretazione come 'maggioranza' in una votazione questa definizione ha diversi fattori positivi, chiaramente tutto è una maggioranza mentre il vuoto non è una maggioranza, poi qualcosa che estende una maggioranza resta una maggioranza, inoltre l'ultima proprietà è utile perché ci dice che se una maggioranza dice φ ed un'altra maggioranza dice ψ allora c'è una maggioranza che dice $\varphi \wedge \psi$, inoltre se una maggioranza dice φ allora nessuna maggioranza dice $\neg\varphi$ (altrimenti $\varnothing \in F$), il problema però è che in questo caso è possibile che non esista una maggioranza per alcuna delle due possibilità.

Definizione 3.0.2: *Ultrafiltro*

Fissato un insieme I si dice *ultrafiltro* un filtro $F \subset \mathscr{P}(I)$ che soddisfa

$$A \notin F \to I \setminus A \in F$$

Esempio 3.0.1: *Filtro principale* Fissiamo $I = \mathbb{N}$ e consideriamo l'insieme

$$F = \{A \in \mathscr{P}(\mathbb{N}) \mid 42 \in A\}$$

questo è un ultrafiltro, infatti contiene $\mathbb{N}$, non contiene il vuoto, se $42 \in A$ e $A \subset B$ allora $42 \in B$, se $A, B \in F$ allora $42 \in A \cap B$ e se $A \notin F$ allora $42 \notin A$, quindi $42 \in \mathbb{N} \setminus A$.
In particolare gli ultrafiltri costruiti in questo modo vengono detti *filtri principali*(o anche *ultrafiltri principali*).
Tornando all'interpretazione predecente come 'maggioranza' questo ultrafiltro corrisponde a fissare un componente e dire che quello è la maggioranza.

Esempio 3.0.2 Fissiamo $I = \mathbb{N}$ (volendo funziona anche con qualunque insieme infinito) e consideriamo l'insieme delle parti cofinite di I:

$$F = \{A \in \mathscr{P}(\mathbb{N}) \mid |\mathbb{N} \setminus A| < \aleph_0\}$$

questo è un filtro, infatti:

- contiene $\mathbb{N}$ e non contiene il vuoto;
- se A è cofinito e $A \subset B$ allora il complementare di B è contenuto nel complementare di A;
- se A e B sono cofiniti allora il complementare della loro intersezione ha cardinalità al più la somma delle cardinalità dei due complementari, quindi anche l'intersezione è cofinita.

Questo però non è un ultrafiltro in quanto esistono insiemi infiniti non cofiniti, ad esempio né l'insieme dei pari né quello dei dispari sono elementi di F.

Non è facile procurarsi un ultrafiltro non principale mentre è relativamente immediato procurarsi dei filtri; con la prossima proposizione vediamo che dato un filtro possiamo almeno dire che esiste un ultrafiltro che lo estende.

Proposizione 3.0.3

Dato un insieme I ed un filtro $F \subset \mathscr{P}(I)$ esiste un ultrafiltro U tale che $F \subset U$.

Dimostrazione. Se F non è un ultrafiltro allora esiste un insieme $A \subset I$ tale che $A \notin F$ ed anche il complementare $I \setminus A \notin F$.

Ma se $I \setminus A \notin F$ allora esiste un filtro $F' \supset F$ tale che $A \in F'$, infatti se costruiamo F' come

$$F' = \{C \in \mathscr{P}(I) \mid \exists\, B \in F . C \cap A = B \cap A\}$$

allora chiaramente $F \subset F'$ in quanto $B \cap A = B \cap A$; vediamo che F' è un filtro infatti:

- ovviamente $I \in F'$ in quanto $I \in F$ e se per assurdo $\varnothing \in F'$ allora esiste $B \in F$ tale che $B \cap A = \varnothing$ quindi $B \subseteq I \setminus A$ ma questo è assurdo perché F è un filtro ed $I \setminus A \notin F$ per ipotesi;
- se $C_1 \in F'$ e $C_2 \supset C_1$ allora $C_2 \cap A \supset C_1 \cap A$ ed esiste $B_1 \in F$ tale che $C_1 \cap A = B_1 \cap A$ allora

  $$B_1 \cup (C_2 \cap A \setminus C_1 \cap A)$$

  è un soprainsieme di B_1 che intersecato con A è uguale a $C_2 \cap A$, quindi $C_2 \in F'$ in quanto F è un filtro;
- se $C_1, C_2 \in F'$ allora esistono $B_1, B_2 \in F$ tali che $A \cap B_1 = A \cap C_1$ e $A \cap B_2 = A \cap C_2$, quindi

  $$(C_1 \cap C_2) \cap A = (C_1 \cap A) \cap (C_2 \cap A) = (B_1 \cap A) \cap (B_2 \cap A) = (B_1 \cap B_2) \cap A$$

  ovvero $C_1 \cap C_2 \in F'$ in quanto F è un filtro.

Per il lemma di Zorn[1] l'insieme dei filtri su $\mathscr{P}(I)$ ammette elementi massimali per l'inclusione, quindi esiste un tale elemento massimale U che contiene F, ma per la costruzione precedente questo deve essere un ultrafiltro, altrimenti per la costruzione precedente potremmo ottenere un filtro che lo contiene propriamente. □

Chiaramente avendo usato il lemma di Zorn questo risultato richiede qualche forma di scelta, in realtà è più debole dell'assioma della scelta ma non segue da ZF senza l'assioma della scelta e non è possibile costruire direttamente un ultrafiltro non principale.

[1] in realtà dovremmo dimostrare che valgono le ipotesi del lemma di Zorn sull'insieme dei filtri su $\mathscr{P}(I)$ rispetto all'inclusione, ma questo è facile vedendo che l'unione arbitraria di filtri inscatolati è anch'essa un filtro

Osservazione 3.0.3: *Insiemi infiniti ammettono ultrafiltri non principali* Esiste un ultrafiltro non principale su $\mathscr{P}(\mathbb{N})$ infatti partendo dal filtro $F = \mathscr{P}^{cof}(\mathbb{N})$ esiste per la proposizione precedente (3.0.3) un ultrafiltro U su $\mathscr{P}(\mathbb{N})$ tale che $F \subset U$, ma se U fosse principale allora esisterebbe $n \in \mathbb{N}$ tale che $\{n\} \in U$, ma questo non è possibile perché il singoletto è finito, quindi il suo complementare è un elemento di F.
Chiaramente lo stesso ragionamento funziona per mostrare l'esistenza di un ultrafiltro non principale per un qualunque insieme infinito.
Notiamo inoltre che ogni ultrafiltro non principale deve contenere i cofiniti in quanto contiene i complementari dei singoletti e tutte le loro intersezioni finite.

Definizione 3.0.4: *Ultraprodotto*

Fissato un linguaggio $L = (r_j, f_k)_{\substack{j\in J\\ k\in K}}$ ed una famiglia di L-strutture $M_i = (S_i, \mathfrak{i}_i)$ con $i \in I$ e fissato un ultrafiltro U su $\mathscr{P}(I)$, definiamo *ultraprodotto degli* M_i *modulo* U la L-struttura

$$\prod_{i\in I} M_i \big/ U = \left(\left(\prod_{i\in I} {}^{3} S_i \right) \Big/ \sim_U, r_J \big/ U, f_K \big/ U \right)$$

dove per definire il quoziente creiamo la relazione di equivalenza dove dati $a, b \in \prod_{i\in I} S_i$ diciamo che $a \sim_U b$ se e solo se

$$\{i \in I \mid a_i = b_i\} \in U$$

e dove poniamo che data una relazione n-aria r_j allora $r_j \big/ U([a_1]_U, \dots, [a_n]_U)$ se e solo se

$$\{i \in I \mid r_{j,i}(a_{1,i}, \dots, a_{n,i})\} \in U$$

e data una funzione m-aria f_k allora

$$f_k \big/ U([a_1]_U, \dots, [a_m]_U) \doteq \left[(f_{k,i}(a_{1,i}, \dots, a_{m,i}))_{i\in I} \right]_U$$

Esercizio 3.1 Verificare che l'ultraprodotto è ben definito, cioè che le definizioni per le relazioni e le funzioni passano al quoziente.

Svolgimento. Per iniziare la relazione $\sim_U$ è una relazione di equivalenza in quanto dato che $I \in U$ è riflessiva ed è sia simmetrica che transitiva perché U è chiuso per intersezione.

Sia f un simbolo di funzione h-ario e siano $x_1, \dots, x_h, y_1, \dots, y_h \in \prod_{i\in I} D_i$ tali che per ogni $a \in \{1, \dots, h\}$ vale $x_a \sim_U y_a$.

Per ogni $a \in \{1, \dots, h\}$ se definiamo

$$A_a \doteq \{i \in I \mid x_{a,i} = y_{a,i}\}$$

per costruzione vale $A_a \in U$, quindi essendo $h \in \mathbb{N}$ vale $\spadesuit \doteq \bigcap_{a=1}^{h} A_a \in U$; inoltre per costruzione di $\spadesuit$ se $i \in \spadesuit$ allora

$$f_a(x_{1,a}, \dots, x_{h,a}) = f_a(y_{1,a}, \dots, y_{h,a})$$

ovvero $\spadesuit$ è un sottoinsieme di

$$\{i \in I \mid f_i(x_{1,i}, \dots, x_{h,i}) = f_i(y_{1,i}, \dots, y_{h,i})\}$$

ed U è chiuso per soprainsiemi quindi

$$(f_i(x_{1,i}, \dots, x_{h,i}))_{i\in I} \sim_U (f_i(y_{1,i}, \dots, y_{h,i}))_{i\in I}$$

ovvero $f \big/ U$ è ben definita.

[9] con il prodotto $\prod S_i$ indichiamo come nel corso di ETI l'insieme delle funzioni che ad ogni $i \in I$ associano un elemento di S_i

Sia invece r un simbolo di relazione h-ario e come prima siano siano $x_1, \dots, x_h, y_1, \dots, y_h \in \prod_{i \in I} D_i$ tali che per ogni $a \in \{1, \dots, h\}$ vale $x_a \sim_U y_a$.

Se

$$\clubsuit \doteq \{i \in I \mid r_i(x_{1,i}, \dots, x_{h,i})\} \in U$$

allora anche $\spadesuit \cap \clubsuit \in U$ e per ogni $i \in \spadesuit \cap \clubsuit$ valgono per costruzione sia $r_i(x_{1,i}, \dots, x_{h,i})$ che

$$(x_{1,i}, \dots, x_{h,i}) = (y_{1,i}, \dots, y_{h,i})$$

ovvero $\spadesuit \cap \clubsuit$ è un sottoinsieme di

$$\{i \in I \mid r_i(y_{1,i}, \dots, y_{h,i})\}$$

ed U è chiuso per soprainsiemi quindi è ben definita anche $r_{/U}$. □

3.1 Teorema di Łoś

Vediamo adesso il Teorema di Łoś, una proprietà importante degli ultraprodotti, per poi vedere alcune sue conseguenze, in particolare una prima versione del teorema di compattezza (3.1.4).

Teorema 3.1.1: *di Łoś*

Data una famiglia di L-strutture $M_i(S_i, \mathfrak{i}_i)$ con $i \in I$, fissato un ultrafiltro U su $\mathscr{P}(I)$ e data una L-formula $\varphi(x_1, \dots, x_k)$ vale:

$$\prod_{i \in I} M_i /_U \vDash \varphi([a_1], \dots, [a_k]) \iff \{i \in I \mid M_i \vDash \varphi(a_{1,i}, \dots, a_{k,i})\} \in U$$

Dimostrazione. Procediamo per induzione strutturale su φ.

Per il passo base se φ è una formula atomica allora segue dalla definizione dell'ultraprodotto che la tesi è vera per φ.

> **Esercizio 3.2** Mostrare approfonditamente che effettivamente per le formule atomiche vale la tesi.

Svolgimento. Se φ è la formula sempre vera allora vale la tesi in quanto $I \in U$, analogamente se φ è la formula sempre falsa vale la tesi in quanto $\varnothing \notin U$.

Se $\varphi \doteq r(t_1, \dots, t_h)$ dove r è un simbolo di relazione h-ario allora per definizione

$$\prod_{i \in I} M_i /_U \vDash \varphi([a_1], \dots, [a_k]) \iff (t_1([a_1], \dots, [a_k]), \dots, t_h([a_1], \dots, [a_k])) \in r_{/U}$$

e per definizione di ultraprodotto questo è vero se e solo se

$$\{i \in I \mid (t_1(a_{1,i}, \dots, a_{k,i}), \dots, t_h(a_{1,i}, \dots, a_{k,i})) \in r_i\} \in U$$

cioè la tesi è vera per $r(t_1, \dots, t_h)$.

Se $\varphi \doteq t_1 = t_2$ allora indicando $M \doteq \prod_{i \in I} M_i /_U$ per la semantica di Tarski (2.1.2)

$$\prod_{i \in I} M_i /_U \vDash \varphi([a_1], \dots, [a_k]) \iff [t_1([a_1], \dots, [a_k])]_U =_M [t_2([a_1], \dots, [a_k])]_U$$

dove $M = \frac{\prod_{i \in I} M_i}{U}$, e per definizione della relazione di equivalenza $\sim_U$ questo vale se e solo se

$$\{i \in I \mid t_1(a_{1,i}, \dots, a_{k,i}) =_{M_i} t_2(a_{1,i}, \dots, a_{k,i})\} \in U$$

cioè per la semantica di Tarski la tesi è vera per $t_1 = t_2$. □

Come al solito nelle dimostrazioni per induzione strutturale bisogna separare diversi casi nel passo induttivo.

Partiamo da $\varphi(x_1,\dots,x_k) \doteq \neg\psi(x_1,\dots,x_k)$ dove come ipotesi induttiva la tesi vale per $\psi(x_1,\dots,x_k)$. Per la semantica di Tarski (2.1.2) vale $\prod_{i\in I} M_i/U \vDash \neg\psi([a_1],\dots,[a_k])$ se e solo se

$$\neg \prod_{i\in I} M_i/U \vDash \psi([a_1],\dots,[a_k])$$

e per ipotesi induttiva questo equivale a dire che

$$\{i \in I \mid M_i \vDash \psi([a_1],\dots,[a_k])\} \notin U$$

ma U è un ultrafiltro, quindi questo equivale a dire che il complementare dell'insieme appartiene ad U ovvero che

$$\{i \in I \mid \neg M_i \vDash \psi(a_{1,i},\dots,a_{k,i})\} \in U$$

che sempre per la semantica di Tarski equivale a dire che

$$\{i \in I \mid M_i \vDash \neg\psi(a_{1,i},\dots,a_{k,i})\} \in U$$

ovvero la tesi è vera per φ.

Ora consideriamo $\varphi(x_1,\dots,x_k) \doteq \varphi_1(x_1,\dots,x_k) \wedge \varphi_2(x_1,\dots,x_k)$ dove le due componenti φ_1 e φ_2 soddisfano l'ipotesi induttiva; il ragionamento è del tutto analogo al caso precedente infatti per la semantica di Tarski vale $\prod_{i\in I} M_i/U \vDash \varphi_1([a_1],\dots,[a_k]) \wedge \varphi_2([a_1],\dots,[a_k])$ se e solo se

$$\prod_{i\in I} M_i/U \vDash \varphi_1([a_1],\dots,[a_k]) \quad \wedge \quad \prod_{i\in I} M_i/U \vDash \varphi_1([a_1],\dots,[a_k])$$

e per ipotesi induttiva questo equivale a dire che

$$\{i \in I \mid M_i \vDash \varphi_1(a_{1,i},\dots,a_{k,i})\} \in U \quad \wedge \quad \{i \in I \mid M_i \vDash \varphi_2(a_{1,i},\dots,a_{k,i})\} \in U$$

ma U è un ultrafiltro, quindi questo equivale a dire che l'intersezione dei due insiemi appartiene ad U ovvero che

$$\{i \in I \mid M_i \vDash \varphi_1(a_{1,i},\dots,a_{k,i}) \wedge M_i \vDash \varphi_2(a_{1,i},\dots,a_{k,i})\} \in U$$

che sempre per la semantica di Tarski equivale a dire che

$$\{i \in I \mid M_i \vDash \varphi_1(a_{1,i},\dots,a_{k,i}) \wedge \varphi_2(a_{1,i},\dots,a_{k,i})\} \in U$$

ovvero la tesi è vera per φ.

Osservazione 3.1.1 I connetivi logici $\neg$ ed $\wedge$ costituiscono uno dei tanti insiemi completi di connettivi logici, cioè da combinazioni di questi due possiamo ricavare anche gli altri connettivi $\vee$ ed $\rightarrow$[10], quindi quando facciamo una dimostrazione per induzione sulle formule basta vedere per i passi induttivi ad esempio quelli con $\neg, \wedge$ ed $\exists$, infatti dalla semantica di Tarski seguono

$$\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$$
$$\varphi \rightarrow \psi \equiv \neg(\varphi \wedge \neg\psi)$$
$$\forall x.\varphi \equiv \neg\exists x.\neg\varphi$$

Per concludere la dimostrazione basta verificare il caso di $\varphi(x_1,\dots,x_k) \doteq \exists y.\psi(x_1,\dots,x_k,y)$ con ψ che soddisfa l'ipotesi induttiva.

Ancora una volta per la semantica di Tarski vale $\prod_{i\in I} M_i/U \vDash \exists x.\psi([a_1],\dots,[a_k],y)$ se e solo se

$$\exists\, b \in \prod S_i.\ \prod_{i\in I} M_i/U \vDash \psi([a_1],\dots,[a_k],[b])$$

[10] In realtà l'essere un insieme completo di connettivi vuol dire qualcosa di più, cioè che dato un qualunque connettivo logico k-ario, cioè una funzione booleana k-aria che risulta vera o falsa a seconda se gli argomenti siano veri o falsi, possiamo costruirne uno equivalente come combinazione di elementi dell'insieme, ma è altrettanto evidente che $\{\neg, \wedge\}$ ricade in questo caso più generale ed i connettivi logici che ci interessano per le formule sono soltanto i quattro connettivi standard

per l'ipotesi induttiva questo equivale a dire che

$$\exists b \in \prod S_i. \{i \in I \mid M_i \vDash \psi(a_{1,i}, \dots, a_{k,i}, b_i)\} \in U \tag{3.1}$$

e questo è equivalente a dire che

$$\{i \in I \mid \exists b_i \in D_i. M_i \vDash \psi(a_{1,i}, \dots, a_{k,i}, b_i)\} \in U \tag{3.2}$$

infatti:

- l'implicazione da 3.1 a 3.2 segue dal fatto che l'insieme in 3.2 è un soprainsieme di quello in 3.1
- l'implicazione da 3.2 a 3.1 segue costruendo b con l'assioma della scelta scegliendo b_i per ogni $i \in I$ ed un elemento qualunque di D_i per gli altri indici.

e per concludere grazie alla semantica di Tarski la 3.2 è equivalente a

$$\{i \in I \mid M_i \vDash \exists y. \psi(a_{1,i}, \dots, a_{k,i}, y)\} \in U$$

□

Corollario 3.1.1.1

Data una famiglia di L-strutture $M_i(S_i, \mathfrak{i}_i)$ con $i \in I$, fissato un ultrafiltro U su $\mathscr{P}(I)$ e data una L-formula φ se per ogni $i \in I$ vale $M_i \vDash \varphi$ allora anche per l'ultraprodotto vale $\prod_{i \in I} M_i /_U \vDash \varphi$.

Da questo corollario al teorema di Łoś segue ovviamente che se tutti gli M_i sono modelli di una stessa teoria T allora anche l'ultraprodotto è un modello di T, questo risultato può essere usato per mostrare che ci sono modelli di Peano che non sono i numeri naturali standard.

Esempio 3.1.2: $\mathbb{N}^\star$ Consideriamo un ultrafiltro non principale U su $\mathscr{P}(\mathbb{N})$, per l'osservazione 3.0.3 questo deve esistere, e consideriamo la struttura

$$\mathbb{N}^\star \doteq \prod_{i \in \mathbb{N}} \mathbb{N} /_U$$

dove gli elementi del prodotto sono gli $\mathbb{N}$ intesi come strutture modello standard di Peano.
Un elemento del dominio di $\mathbb{N}^\star$ è quindi classe di equivalenza $[\sigma]$ dove una funzione $\sigma : \mathbb{N} \to \mathbb{N}$ tale che

$$[\sigma] = \{t : \mathbb{N} \to \mathbb{N} \mid \{i \mid \sigma_i = t_i\} \in U\}$$

Questo è un modello dell'aritmetica T_{PA} di Peano.
Se supponiamo per assurdo che esista un isomorfismo $f : \mathbb{N} \to \mathbb{N}^\star$, si vede per induzione che per ogni $n \in \mathbb{N}$

$$f(n) = [(n, n, n, \dots)]$$

infatti

$$f(0) = [(0, 0, 0, \dots)] \qquad \text{e} \qquad f(s(m)) = [(s(m), s(m), s(m), \dots)]$$

ma allora per ogni $i \in \mathbb{N}$ vale l'assurdo

$$f(i) \neq [(0, 1, 2, \dots)]$$

infatti vale l'uguaglianza

$$[(0, 1, 2, \dots)] = [(i, i, i, \dots)]$$

per definizione se e solo se

$$\{i \in \mathbb{N} \mid \{n = i\}\} \in U$$

ma fissato un qualunque $i \in \mathbb{N}$ questo insieme è un singoletto, che quindi non appartiene ad U, altrimenti U sarebbe principale.
Notiamo che su $\mathbb{N}$ possiamo definire l'ordine ponendo

$$x < y \doteq \exists z. x + s(z) = y$$

e verificare per induzione che questo è un ordine totale, cioè che su $\mathbb{N}$ vale

$$\forall x.\forall y.x = y \vee \exists z.x + s(z) = y \vee y + s(z) = x$$

ed essendo $\mathbb{N}^\star$ costruito da copie di $\mathbb{N}$ per il teorema di Łoś (3.1.1) anche $\mathbb{N}^\star$ è totalmente ordinato in questo modo, si potrebbe vedere che $\mathbb{N}^\star$ è ordinato come $\mathbb{N} \sqcup \mathbb{Z} \sqcup \cdots \sqcup \mathbb{Z}$ con l'ordine che pone gli elementi di $\mathbb{N}$ all'inizio e poi le copie di $\mathbb{Z}$ una dopo l'altra, queste copie di $\mathbb{Z}$ sono dense e sono esattamente $2^{\aleph_0}$.

Teorema 3.1.2: *di Tennenbaum*

Non esiste un modello computabile non-standard dell'aritmetica di Peano.

Questo risultato giustifica un po' l'affermazione fatta in precedenza sull'impossibilità di costruire un ultrafiltro non principale, infatti se potessimo ottenere costruttivamente tale ultrafiltro su $\mathbb{N}$ potremmo costruire in $\mathbb{N}^\star$ invalidando il teorema. Non dimostreremo il teorema di Tennenbaum e non abbiamo ancora neanche detto cosa sia precisamente una la calcolabilità; approfondiremo questo più avanti. L'idea della dimostrazione di questo teorema è di prendere un insieme non computabile ma definibile dentro a T_{PA} come ad esempio l'insieme della fermata, troncare questo insieme ad un numero infinito non-standard e prendere il codice di questo insieme troncato manipolandolo con operazioni aritmetiche per esibire un algoritmo che risolve il problema della fermata.

Esempio 3.1.3: $\mathbb{R}^\star$ La stessa costruzione di $\mathbb{N}^\star$ è quella partendo dai numeri reali per ottenere $\mathbb{R}^\star = \prod \mathbb{R}/U$, ad esempio se consideriamo $(\mathbb{R}, <, 0, 1, +, \cdot)$ come campo reale chiuso (campo ordinato dove ogni polinomio di grado dispari ha una radice), otterremo che anche $\mathbb{R}^\star$ è un campo reale chiuso non archimedeo, ovvero che ammette dei numeri infiniti (cioè irraggiungibili sommando 1 a se stesso finite volte) ed infinitesimi (cioè che sommati a se stessi finite volte non arrivano mai ad 1), questa è una costruzione che può essere utile in analisi non-standard.

Mostriamo adesso un risultato di interesse al di fuori della logica che può essere dimostrato utilizzando gli ultraprodotti.

Teorema 3.1.3: *Ax-Groethendieck*

Sia $f : \mathbb{C}^n \to \mathbb{C}^n$ una funzione polinomiale, se f è iniettiva allora è biunivoca.

Nota 3.1.4 Per dimostrare questo teorema abbiamo bisogno di due fatti ausiliari:

1. due campi algebricamente chiusi di caratteristica zero sono isomorfi se hanno basi di trascendenza equipotenti[11], da questo segue che ogni campo algebricamente chiuso di caratteristica zero e cardinalità $2^{\aleph_0}$ è isomorfo a $\mathbb{C}$.
2. fissato un campo finito $\mathbb{F}_p$ la sua chiusura algebrica è

$$\overline{\mathbb{F}_p} = \bigcup_{k\in\mathbb{N}} \mathbb{F}_p^k = \bigcup_{k\in\mathbb{N}} \mathbb{F}_p^{k!} \tag{3.3}$$

Dimostrazione del teorema 3.1.3. Consideriamo ancora una volta un ultrafiltro non principale U su $\mathscr{P}(\mathbb{N})$ e cerchiamo di mostrare che nel linguaggio dei campi

$$F \doteq \prod_{i\in\mathbb{N}} \overline{\mathbb{F}_{p_i}}/U \cong \mathbb{C}$$

dove p_i è l'i-esimo numero primo e $\cong$ è l'isomorfismo di campi.

- F è un campo per il teorema di Łoś (3.1.1) in quanto teoria dei campi è assiomatizzata al primo ordine e tutti i fattori del prodotto sono campi.

[11] della stessa cardinalità

- si può scrivere al primo ordine che un campo è algebricamente chiuso mediante numerabili formule; chiaramente per farlo non possiamo usare una formula per ogni polinomio in quanto i coefficienti del polinomio dipendono dal campo, però possiamo usare una formula per ogni grado: ad esempio per il grado 4 la formula
$$\forall a,b,c,d,e.\exists x.ax^4+bx^3+cx^2+dx+e=0$$
è quella così ottenuta è una lista numerabile di formule nella teoria dei campi che sono tutte vere se e solo se il campo è algebricamente chiuso, quindi per definizione sono tutte vere in ogni fattore del prodotto che definisce F e quindi, sempre per il teorema di Łoś, le formule sono tutte vere anche in F ovvero anche F è algebricamente chiuso.
- supponiamo per assurdo che F non abbia caratteristica 0, ovvero che esista un primo p_j tale che sommando 1 a se stesso p_j volte si ottiene 0; essendo F costruito tramite un ultrafiltro non principale vale $\mathbb{N}\setminus\{j\}\in U$ e la formula $1+\cdots+1=0$ con p_j addendi in F è
$$[(1+\cdots+1,1+\cdots+1,1+\cdots+1,\dots)]\neq[(0,0,0,\dots)]$$
e $1+\cdots+1\neq 0$ con p_j addendi è vera in tutti i fattori diversi da $\overline{\mathbb{F}_{p_j}}$, quindi per definizione è vera anche nell'ultraprodotto.
- F ha la cardinalità del continuo, infatti chiaramente $|F|\leq\left|\prod_{i\in\mathbb{N}}\overline{\mathbb{F}_{p_i}}\right|=2^{\aleph_0}$ e possiamo costruire una mappa iniettiva dall'intervallo reale $[0,1]$ in F mandando ogni $x\in[0,1]$ nella classe di equivalenza della sequenza
$$\{\lfloor ix\rfloor\}_{i\in\mathbb{N}}$$
infatti dati due elementi diversi α e β di $[0,1]$ le due sequenze sono definitivamente diverse in quanto esiste $i_0>0$ tale che $\frac{1}{i_0}<|\beta-\alpha|$ e da questo segue che per ogni $i>i_0$ saranno diversi $\lfloor i\beta\rfloor$ e $\lfloor i\alpha\rfloor$; divergendo su un insieme cofinito le due sequenze appartengono a classi di equivalenza diverse nell'ultraprodotto.

Quindi se riusciamo a descrivere la tesi del teorema con numerabili formule che sono vere su ogni componente di F per Łoś deve essere valida anche in $\mathbb{C}$, usiamo la stessa idea di prima di usare una formula per ogni grado dei polinomi. Fissato un grado d possiamo effettivamente scrivere

$$\forall f:F^n\to F^n.f \text{ polinomiale di grado } d \text{ iniettiva} \to f \text{ surgettiva}$$

nel linguaggio della teoria dei campi senza usare parametri del campo come

$$\begin{aligned}
&\forall a_{1,0},\dots,a_{n,0},a_{1,1},\dots,a_{1,d},\dots,a_{n,1},\dots,a_{n,d}.\\
&\Big[\forall x_1,\dots,x_n,y_1,\dots,y_n.\Big(a_{1,0}+a_{1,1}x_1\cdots+a_{1,d}x_1^d=a_{1,0}+a_{1,1}y_1\cdots+a_{1,d}y^d\\
&\qquad\vdots\\
&\qquad a_{n,0}+a_{n,1}x_n\cdots+a_{n,d}x_n^d=a_{n,0}+a_{n,1}y_n\cdots+a_{n,d}y_n^d\Big)\\
&\qquad\to(x_1=y_1\wedge\cdots\wedge x_n=y_n)\Big]\to\\
&\forall x_1,\dots,x_n.\exists y_1,\dots y_n.\Big(a_{1,0}+a_{1,1}x_1\cdots+a_{1,d}x_1^d=y_1\\
&\qquad\vdots\\
&\qquad a_{n,0}+a_{n,1}x_n\cdots+a_{n,d}x_n^d=y_n\Big)
\end{aligned}$$

dove i colori sono di aiuto a decifrare il significato dei componenti nelle due equazioni.

Rimane solo da verificare che questo è vero in $\overline{\mathbb{F}_p}$ per ogni primo p, per fare questo sfruttiamo la seconda caratterizzazione di $\overline{\mathbb{F}_p}$ dell'equazione (3.3).

Se $f:\overline{\mathbb{F}_p}\to\overline{\mathbb{F}_p}$ è polinomiale di grado d iniettiva ha al più $d\in\mathbb{N}$ coefficienti, quindi esiste k_0 tale che tutti i coefficienti di f sono contenuti in $\mathbb{F}_{p^{k_0}}$ quindi con k multiplo di k_0 la restrizione $f|_{\mathbb{F}_{p^k}}$ manda $\mathbb{F}_{p^k}^n$ in se stesso ed è iniettiva, ma $\mathbb{F}_{p^k}^n$ è finito quindi $f|_{\mathbb{F}_{p^k}}$ è surgettiva.

A partire da questo vediamo che dato $x \in \overline{\mathbb{F}_p}$ esiste k_1 multiplo di k_0 tale che $x \in \mathbb{F}_{p^{k_1}}$, quindi esiste un elemento $y \in \mathbb{F}_{p^{k_1}}$ tale che

$$f|_{\mathbb{F}_{p^{k_1}}}(y) = f(y) = x$$

ovvero ogni $f : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ polinomiale di grado d iniettiva è surgettiva, quindi il risultato vale anche su $F \cong \mathbb{C}$. □

Prima di proseguire al prossimo argomento vediamo una ulteriore conseguenza del teorema di Łoś che sarà interessante per la parte di teoria di modelli.

Teorema 3.1.4: *di Compattezza (semantica*[12]*)*

Data una L-teoria T ed una L-formula φ se $T \vDash \varphi$ allora esiste una sottoteoria finita $T' \subseteq T$ (tale che $|T'| < \aleph_0$) tale che $T' \vDash \varphi$.

Dimostrazione. Il caso di T finito è banalmente vero, partiamo quindi dal caso in cui T è numerabile.

Se T è numerabile allora lo posso scrivere come $T = \{\varphi_i\}_{i\in\mathbb{N}}$ e definisco $T_i = \{\varphi_j \mid j \in \mathbb{N} \wedge j < i\}$, se per assurdo la tesi del teorema fosse falsa allora per ogni $i \in \mathbb{N}$ vale $T_i \nvDash \varphi$, quindi per ogni $i \in \mathbb{N}$ esiste un modello M_i di T_i tale che

$$M_i \vDash T_i \qquad \text{e} \qquad M_i \vDash \neg\varphi$$

Però se consideriamo l'ultraprodotto $P = \prod_{i\in\mathbb{N}} M_i/U$ con U ultrafiltro non principale questo è un modello di T in quanto per ogni $i \in \mathbb{N}$ vale

$$|\{j \in \mathbb{N} \mid M_j \vDash \neg\varphi_i\}| = i$$

quindi il suo complementare è un elemento di U in quanto cofinito, ovvero per ogni $i \in \mathbb{N}$ vale $P \vDash \varphi_i$, ma per il teorema di Łoś (3.1.1) vale anche che $P \vDash \neg\varphi$ ma questo è assurdo perché $T \vDash \varphi$.

Per il caso di cardinalità generica consideriamo un filtro F su $\mathscr{P}\left(\mathscr{P}^{\text{fin}}(T)\right)$ definito ponendo $X \in F$ se e solo se

$$\exists\, A \in \mathscr{P}^{\text{fin}}(T).\, \left\{B \in \mathscr{P}^{\text{fin}}(T) \;\middle|\; A \subseteq B\right\} \subseteq X$$

questo è un filtro in quanto:

- chiaramente $\varnothing \notin F$ e $\mathscr{P}\left(\mathscr{P}^{\text{fin}}(T)\right) \in F$;
- se $X \in F$ ed $Y \supset X$ allora per costruzione chiaramente anche Y è un elemento di F;
- se X ed Y sono elementi di F allora esistono due insiemi $A_X, A_Y \in \mathscr{P}^{\text{fin}}(T)$ tali che

$$\left\{B \in \mathscr{P}^{\text{fin}}(T) \;\middle|\; A_X \subseteq B\right\} \subseteq X$$
$$\left\{B \in \mathscr{P}^{\text{fin}}(T) \;\middle|\; A_Y \subseteq B\right\} \subseteq Y$$

  e se consideriamo l'insieme $A = A_X \cup A_Y$ questo è un soprainsieme sia di A_X che di A_Y, quindi è contenuto in $X \cap Y$ ed un qualunque soprainsieme B di A è anch'esso un soprainsieme sia di A_X che di A_Y ovvero $X \cap Y \in F$.

Fissiamo un ultrafiltro U che estende F e supponiamo per assurdo che il teorema di compattezza sia falso su T, ovvero che esista una formula φ tale che $T \vDash \varphi$ ma per ogni $T' \in \mathscr{P}^{\text{fin}}(T)$ esiste una struttura $M_{T'}$ tale che $M_{T'} \vDash T', \neg\varphi$, grazie all'assioma della scelta possiamo scegliere tale $M_{T'}$ per ogni T' e così costruire l'ultraprodotto

$$M \doteq \prod_{T'\in\mathscr{P}^{\text{fin}}(T)} M_{T'}/U$$

allora per il corollario al teorema di Łoś (3.1.1.1) vale $M \vDash \neg\varphi$; cerchiamo di dimostrare l'assurdo che $M \vDash T$.

Fissata $\psi \in T$ allora se $\{\psi\} \subseteq T'$ ovvero se $\psi \in T'$ allora per costruzione $M_{T'} \vDash \psi$, quindi vale il contenimento

$$\left\{T' \in \mathscr{P}^{\text{fin}}(T) \;\middle|\; M_{T'} \vDash \psi\right\} \supseteq \left\{T' \in \mathscr{P}^{\text{fin}}(T) \;\middle|\; \{\psi\} \subseteq T'\right\}$$

[12] Come per la definizione 2.3.9 distinguiamo questa formulazione del teorema di compattezza come 'semantica' a differenza di una formulazione 'sintattica' che useremo più avanti, per poi accorgerci che grazie ai teoremi di completezza e correttezza le due formulazioni sono equivalenti

ma essendo un singoletto $\{\psi\}$ ha cardinalità finita, quindi per costruzione il secondo di questi insiemi appartiene ad $F \subset U$, ovvero anche il primo è un elemento dell'ultrafiltro, quindi per il teorema di Łoś (3.1.1) per ogni $\psi \in T$ vale $M \vDash \psi$. □

Esercizio 3.3 Completare la dimostrazione del teorema di compattezza.

3.2 Conseguenze del teorema di compattezza

Proposizione 3.2.1

Data una L-teoria T se questa è finitamente coerente (ovvero se ogni sua sottoteoria finita è coerente) allora T è coerente.

Dimostrazione. La contronominale di questa proposizione segue immediatamente dal teorema di compattezza (3.1.4) infatti se T non è coerente allora $T \vDash \bot$ quindi per il teorema di compattezza esiste una sottoteoria $T' \subset T$ finita tale che $T' \vDash \bot$, quindi T' non è coerente da cui T non è finitamente coerente. □

Esempio 3.2.1 Abbiamo già visto che la teoria completa $Th(\mathbb{N}, 0, 1, +, \cdot, s)$ ammette modelli non-standard (con la costruzione tramite ultrafiltri non principali nell'esempio 3.1.2), mostriamo un'altra dimostrazione che sfrutta la conseguenza appena dimostrata del teorema di compattezza.
Sia $L_c = (0, 1, +, \cdot, s, c) = L_{ar} \cup \{c\}$ il linguaggio dell'aritmetica a cui aggiungiamo un simbolo di costante c e consideriamo la L_c-teoria

$$T = Th(\mathbb{N}, 0, 1, +, \cdot, s) \cup \{\begin{array}{l} \exists\, x.c = s(x) \\ \exists\, x.c = s(s(x)) \\ \exists\, x.c = s(s(s(x))) \\ \vdots \\ \} \end{array}$$

Questa teoria T è finitamente coerente, in quanto se $T' \subset T$ è finito allora chiaramente $\mathbb{N}$ sono un modello di T' in quanto T' contiene un numero finito di formule nell'insieme sulla destra, quindi per la proposizione precedente (3.2.1) T ammette un modello $M = (D, i)$, che è una L_c-struttura che per inclusione soddisfa $M \vDash \mathrm{Th}(\mathbb{N}, L_{ar})$.
Se definiamo il ridotto[13] di M al linguaggio dell'aritmetica L_{ar} come la L_{ar}-struttura

$$M|_{L_{ar}} \doteq (D, i|_{L_{ar}})$$

chiaramente vale ancora $M \vDash \mathrm{Th}(\mathbb{N}, L_{ar})$ ma M è necessariamente diverso dal modello standard $\mathbb{N}$ in quanto c è un elemento di M che ammette una catena infinita di predecessori.

Esempio 3.2.2 In maniera del tutto analoga all'esempio precedente si può mostrare che ci sono modelli non-archimedei di $\mathrm{Th}(\mathbb{R}, 0, 1, +, \cdot, <)$ aggiungendo invece a questa gli assiomi

$$1 < c, \quad 1 + 1 < c \quad 1 + 1 + 1 < c, \quad \dots$$

Definizione 3.2.2: *Classe assiomatizzabile di strutture*

Diciamo che una classe C di L-strutture è *assiomatizzabile* se esiste una L-teoria T tale che data una qualunque L-struttura M vale $M \in C$ se e solo se $M \vDash T$.
In particolare se esiste una tale T finita diciamo che la classe C è *finitamente assiomatizzabile*.

[13] Rivedremo meglio questa definizione nella prossima parte (5.2.2)

Esempio 3.2.3: *Classe non assiomatizzabile* La classe dei buoni ordini nel linguaggio $L = \{<\}$ non è assiomatizzabile.
Infatti supponiamo per assurdo che tale classe sia assiomatizzabile, ovvero che esiste una teoria T tale che data una qualunque L-struttura M vale $T \vDash M$ se e solo se M è un buon ordine, allora possiamo costruire la teoria T' come

$$T' = T \cup \{c_1 < c_2, c_3 < c_2, c_4 < c_3, \dots\}$$

che, sempre per la proposizione 3.2.1, è una teoria coerente nel linguaggio

$$L' = L \cup \{c_1, c_2, c_3, \dots\}$$

quindi esiste una L'-struttura M modello di T' e riducendo M ad L vale $M|_L \vDash T$, e questo è assurdo perché M è un modello di T', quindi anche $M|_L$ come M ammette una catena discendente infinita ottenuta dalle interpretazioni di $c_1, c_2, \dots$ in M.

Esercizio 3.4 Le seguenti classi non sono assiomatizzabili:

- gli insiemi finiti nel linguaggio vuoto;
- i grafi connessi nel linguaggio $\{\circlearrowleft(\cdot,\cdot)\}$ dove $\circlearrowleft(a,b)$ vuol dire 'esiste un arco da a a b';
- i gruppi abeliani divisibili, ovvero i gruppi abeliani tali che per ogni $n \in \mathbb{N}$

  $$\forall x \in G. \exists y \in G. x = \sum_{i=1}^{n} y$$

  dove $\sum_{i=1}^{n} y$ è un'abbreviazione per dire $y + y + y + \dots$ con esattamente n addendi;
- i gruppi liberi;
- i gruppi semplici (ovvero i gruppi senza sottogruppi normali non banali).

Esempio 3.2.4: *Classe assiomatizzabile non finitamente* Vediamo che la classe degli insiemi infiniti (nel linguaggio vuoto) è assiomatizzabile ma non finitamente.
Se indichiamo con φ_n la formula

$$\varphi_n \doteq \exists x_1, \dots, \exists x_n. \neg x_1 = x_2 \wedge \neg x_1 = x_3 \wedge \dots \wedge \neg x_{n-1} = x_n$$

chiaramente $T = \{\varphi_n\}_{n \in \mathbb{N}}$ ha come modello tutti e soli gli insiemi infiniti, ovvero la classe degli insiemi infiniti è assiomatizzabile.
Supponiamo adesso per assurdo che questa classe sia finitamente assiomatizzabile, quindi esiste una sua assiomatizzazione finita T', allora per il teorema di compattezza dato che $T \vDash T'$ esiste $n \in \mathbb{N}$ finito tale che

$$T'' = \{\varphi_1, \dots, \varphi_n\} \vDash T'$$

quindi anche T'' assiomatizza la classe degli insiemi infiniti, ma questo è falso in quanto un qualunque insieme di cardinalità n è un modello di T''.

Esercizio 3.5 Le seguenti classi sono assiomatizzabili ma non finitamente:

- i gruppi infiniti, gli anelli infiniti ed i campi infiniti;
- i campi di caratteristica zero;
- i campi algebricamente chiusi;
- i grafi 3-colorabili.

Adesso vediamo una applicazione del teorema di compattezza per ottenere un risultato sui grafi.

Definizione 3.2.3

Diciamo *litigiosa* una partizione $A \sqcup B = V$ di un grafo $G = (V, E)$ se per ogni vertice $v \in V$ il numero dei vertici adiacenti a v appartenenti alla stessa parte di v è minore o uguale al numero di vertici adiacenti a v appartenenti alla parte opposta, cioè indicando $N_C(v) = \{w \in C \mid (v, w) \in E \vee (w, v) \in E\}$ per ogni insieme $C \subseteq V$ la partizione si dice litigiosa se

$$v \in A \to |N_A(v)| \leq |N_B(v)| \quad \wedge v \in B \to |N_B(v)| \leq |N_A(v)|$$

Proposizione 3.2.4

Se un grafo è localmente finito (ovvero se ogni suo vertice ha un numero finito di vertici ad esso adiacenti) allora questo ammette una partizione litigiosa.

Dimostrazione. Se il grafo $G(V, E)$ è finito esiste almeno un taglio[14] che massimizza il numero di archi che attraversano il taglio; necessariamente questo taglio è una partizione litigiosa, infatti: se per assurdo esistesse un arco $v \in A$ tale che $|N_A(v)| > |N_B(v)|$ allora la partizione $(A \setminus \{v\}) \sqcup (B \cup \{v\})$ avrebbe un numero strettamente maggiore di archi che attraversano il taglio.

Per il caso generale invece sfruttiamo il teorema di compattezza. Consideriamo il linguaggio

$$L = \{p_i \mid i \in V\}$$

costituito soltanto da costanti proposizionali (una per ogni nodo del grafo) e consideriamo T la L-teoria

$$T = \left\{ (\varphi_i \doteq) \bigvee_{\substack{A \subseteq N(i) \\ |N(i)| \leq 2|A|}} \bigwedge_{j \in A} (p_i \longleftrightarrow \neg p_j) \;\middle|\; i \in V \right\}$$

ovvero per ogni $i \in V$ la formula φ_i ci dice che per il nodo i il numero delle costanti proposizionali con valore di verità diverso da quello di p_i è maggiore della metà dei vicini di i (quindi è anche maggiore o uguale al numero delle p_j con lo stesso valore di verità di p_i) chiaramente dare una L-struttura M che assegna un valore di verità a tutte le costanti proposizionali equivale a dare un taglio del grafo (ponendo A l'insieme dei nodi la cui corrispondente costante è vera e B quelle per cui la costante è falsa) da cui se T ammette un modello questo corrisponde ad una partizione litigiosa del grafo.

Supponiamo per assurdo T non sia finitamente coerente, cioè che esista $V' \subset V$ finito tale che $T' = \{\varphi_i \mid i \in V'\}$ non è coerente.

Consideriamo adesso il sottografo $G'' = (V'', E|_{V'' \times V''})$ dove

$$V'' \doteq V' \cup \bigcup_{i \in V'} N(i)$$

questo è un grafo finito per costruzione (essendo G localmente finito) e quindi abbiamo già dimostrato che ammette una partizione litigiosa $A \sqcup B = V''$; ma se adesso costruiamo una L-struttura M assegnando

$$(p_i)_M = \begin{cases} \top & \text{se } i \in A \\ \bot & \text{se } i \in B \\ \text{qualunque} & \text{se } i \notin V'' \end{cases}$$

abbiamo ottenuto un modello di T' (i nodi non in V'' non ci interessano perché non compaiono in alcun $N(i)$ per $i \in V'$, ovvero non compaiono in T') contraddicendo l'ipotesi assurda. Quindi T è coerente e per il teorema di compattezza (3.1.4) T è coerente per cui il grafo ammette una partizione litigiosa. □

[14] partizione dei nodi in esattamente due insiemi

Proposizione 3.2.5

Ogni gruppo abeliano senza torsione è ordinabile, ovvero ogni gruppo abeliano G che non ha elementi di ordine finito ammette un ordine $<$ tale che

$$\forall\, a, b, c \in G. a < b \longleftrightarrow ac < bc$$

Osservazione 3.2.5 Per dimostrare il teorema facciamo prima una osservazione. Se una teoria T è *universale* ovvero se tutte le $\varphi \in T$ sono della forma $\forall\, x_1 \dots \forall\, x_k.\psi$ con ψ senza quantificatori, dato un modello N di T ed una qualunque sua sottostruttura $M \subseteq N$ questa è anch'essa un modello di T.
Infatti segue dalla semantica di Tarski che le formule universali si preservano per sottostrutture e le formule esistenziali (analoghe a quelle universali ma solo con esiste) si preservano per estensioni mentre le formule senza quantificatori sono *assolute* ovvero valgono nella sottostruttura se e solo se valgono nell'estensione.

Esercizio 3.6 Dimostrare che effettivamente le formule senza quantificatori sono assolute.

Dimostrazione della proposizione 3.2.5. Indichiamo con T_{OAG} la teoria dei gruppi abeliani ordinati nel linguaggio $L = \{e, \cdot, ^{-1}, <\}$, che può essere assiomatizzata come:

$$T_{OAG} = T_{\text{gruppi abeliani}} \cup T_{\text{ordini totali}} \cup \{\forall\, a. \forall\, b, \forall\, c. a < b \longleftrightarrow a \cdot c < b \cdot c\}$$

Fissiamo un gruppo abeliano senza torsione G e mostriamo che $T_{OAG} \cup \mathrm{diag}(G)$ è coerente, infatti se questa teoria ammette un modello la sua sottostruttura G' ottenuta considerando soltanto l'interpretazione delle costanti c_G per ogni $g \in G$ è isomorfa come gruppo a G, e T_{OAG} è universale quindi $G' \vDash T_{OAG}$ da cui tramite l'isomorfismo si ottiene un ordine sul gruppo G.

Se per assurdo $T_{OAG} \cup \mathrm{diag}(G)$ non fosse coerente per il teorema di cmpattezza (3.1.4) esisterebbe un sottoinsieme finito $X \subset \mathrm{diag}(G)$ tale che $T_{OAG} \cup X \vDash \bot$.

L'insieme delle costanti che compaiono in X è necessariamente finito, quindi il sottogruppo H generato da tali costanti è per costruzione abeliano finitamente generato e senza torsione, ovvero esiste $n \in \mathbb{N}$ tale che $H \cong \mathbb{Z}^n$ come gruppi: quindi H è ordinabile, ad esempio con l'ordine lessicografico indotto dall'isomorfismo con $\mathbb{Z}^n$, ma allora H è un modello di $T_{OAG} \cup X$ il che è assurdo. □

Parte II

Teoria dei modelli

Capitolo 4

Le regole di inferenza

Vorremmo introdurre un concetto di deducibilità, cioè $T \vdash \varphi$ col significato che applicando una certa quantità finita di regole meccaniche (ovvero una dimostrazione) possiamo ricavare φ a partire dalle formule di T, con l'obbiettivo poi di mostrare che questo concetto è equivalente a dire che $T \vDash \varphi$.

In particolare arriveremo a dimostrare due teoremi: il teorema di correttezza ci dice che se $T \vdash \varphi$ allora $T \vDash \varphi$ ed il teorema di completezza corrisponde all'altra implicazione.

In questo modo otteniamo un metodo per verificare che una formula è conseguenza logica di una teora dal basso, infatti per ora sappiamo solo mostrare che una formula non è conseguenza logica di T esibendo un modello in cui è falsa, per mostrare che è sempre vera dovremmo invece considerare tutti i modelli di T.

> **Osservazione 4.0.1** Dimostrando che $T \vDash \varphi \iff T \vdash \varphi$ il teorema di compattezza (3.1.4) diventa una banalità in quanto una dimostrazione finita può avere al più un numero finito di premesse.

Ogni libro ed ogni corso da un sistema diverso di regole di inferenza, la cosa importante alla fine è che scegliendo un qualunque sistema del genere si riesca a dimostrare che $T \vDash \varphi \iff T \vdash \varphi$, a questa si aggiungono poi obbiettivi di tipo filosofico o didattico, che nel nostro caso sarà l'obbiettivo che il sistema sia uno di deduzione naturale, cioè che descriva effettivamente i processi intuitivi che riteniamo legittimi nelle dimostrazioni matematiche generiche.

In particolare esporremo due sistemi di deduzione naturale, uno completo, quindi che include tutti i comuni ragionamenti legittimi che vengono eseguiti nelle dimostrazioni informali ed uno ridotto, ovvero che molte meno regole ma comunque abbastanza regole da potere costruire con esse anche le regole mancanti.

La forma delle regole di deduzione che usiamo sarà:

$$\frac{\text{premesse}}{\text{conclusione}} \text{condizioni al margine}$$

dove in numero le premesse saranno zero o più e la conclusione sarà esattamente una, le condizioni al margine sono certe condizioni che devono essere vere perché l'implicazione sia valida; eventualmente per indicare meglio che regola usiamo metteremo a sinistra tra parentesi un nome che assegniamo alla regola.

Le regole connesse ai quantificatori logici saranno introdotte a coppie come regole di *introduzione* ed *eliminazione* in particolare:

$$(\text{In}_\wedge)\ \frac{T \vdash \varphi \quad T \vdash \psi}{T \vdash \varphi \wedge \psi} \qquad (\text{El}_{.\wedge})\ \frac{T \vdash \varphi \wedge \psi}{T \vdash \varphi} \qquad (\text{El}_{\wedge .})\ \frac{T \vdash \varphi \wedge \psi}{T \vdash \psi}$$

$$(\text{In}_{.\vee})\ \frac{T \vdash \varphi}{T \vdash \varphi \vee \psi} \qquad (\text{In}_{\vee .})\ \frac{T \vdash \psi}{T \vdash \varphi \vee \psi}$$

$$(\text{In}_\to)\ \frac{T, \varphi \vdash \psi}{T \vdash \varphi \to \psi} \qquad (\text{El}_\vee)\ \frac{T \vdash \varphi \vee \psi \quad T, \varphi \vdash \theta \quad T, \psi \vdash \theta}{T \vdash \theta}[1]$$

$$(\text{El}_\to)\ \frac{T \vdash \varphi \to \psi \quad T \vdash \varphi}{T \vdash \psi}[2]$$

[1] Questo corrisponde alla dimostrazione per casi
[2] Questo corrisponde al *modus ponens*

$$(\text{In}_\neg)\ \frac{T, \varphi \vdash \bot}{T \vdash \neg\varphi} \qquad (\text{El}_\neg)\ \frac{T \vdash \neg\varphi \quad T \vdash \varphi}{T \vdash \psi}$$

$$(\text{In}_\exists)\ \frac{T \vdash \varphi\left[t/x_k\right]}{T \vdash \exists x_k.\varphi} \qquad (\text{El}_\exists)\ \frac{T \vdash \exists x_k.\varphi \quad T, \varphi \vdash \psi}{T \vdash \psi}\ x_k \notin \text{vl}(T, \psi)$$

$$(\text{In}_\forall)\ \frac{T \vdash \varphi}{T \vdash \forall x_k.\varphi}\ x_k \notin \text{vl}(T) \qquad (\text{El}_\forall)\ \frac{T \vdash \forall x_k.\varphi}{T \vdash \varphi\left[t/x_k\right]}$$

$$(\text{In}_=)\ \frac{}{\vdash t = t} \qquad (\text{El}_=)\ \frac{T \vdash s = t \quad T \vdash \varphi\left[s/x_k\right]}{T \vdash \varphi\left[t/x_k\right]}$$

Invece il connettivo *vero* ($\top$) ha soltanto una regola di introduzione ed il connettivo *falso* ($\bot$) ha soltanto una regola di eliminazione:

$$(\text{In}_\top)\ \frac{}{\vdash \top} \qquad (\text{El}_\bot)\ \frac{T \vdash \bot}{T \vdash \varphi}$$

a questi aggiungiamo altre tre regole, la prima per gli assiomi che ci dice che da una formula φ segue se stessa, la seconda è la regola di indebolimento, cioè date due teorie T e T' se $T \subseteq T'$ e $T \vdash \varphi$ allora anche $T' \vdash \varphi$, l'ultima regola che aggiungiamo poi è quella della riduzione ad assurdo

$$(\text{Ax})\ \frac{}{\varphi \vdash \varphi} \qquad (\text{Wk})\ \frac{T \vdash \varphi}{T' \vdash \varphi}\ T \subseteq T' \qquad (\text{RaA})\ \frac{T, \neg\varphi \vdash \bot}{T \vdash \varphi}{}^{3}$$

Per il sistema ridotto invece rimuoviamo quasi tutte le regole eccetto le ultime tre descritte e quelle dei connettivi $\bot, \to, \exists, =$ ovvero le regole restanti composto dalle regole:

$$(\text{Ax})\ \frac{}{\varphi \vdash \varphi} \qquad (\text{Wk})\ \frac{T \vdash \varphi}{T' \vdash \varphi}\ T \subseteq T' \qquad (\text{RaA})\ \frac{T, \varphi \to \bot \vdash \bot}{T \vdash \varphi}$$

$$(\text{In}_\to)\ \frac{T, \varphi \vdash \psi}{T \vdash \varphi \to \psi} \qquad (\text{El}_\to)\ \frac{T \vdash \varphi \to \psi \quad T \vdash \varphi}{T \vdash \psi}$$

$$(\text{In}_\exists)\ \frac{T \vdash \varphi\left[t/x_k\right]}{T \vdash \exists x_k.\varphi} \qquad (\text{El}_\exists)\ \frac{T \vdash \exists x_k.\varphi \quad T, \varphi \vdash \psi}{T \vdash \psi}\ x_k \notin \text{vl}(T, \psi)$$

$$(\text{In}_=)\ \frac{}{\vdash t = t} \qquad (\text{El}_=)\ \frac{T \vdash s = t \quad T \vdash \varphi\left[s/x_k\right]}{T \vdash \varphi\left[t/x_k\right]}$$

con la regola della riduzione all'assurdo modificata per non usare $\neg$ (effettivamente stiamo rimpiazzando $\neg\varphi$ con $\varphi \to \bot$); da queste si possono ricavare anche le altre in quanto $\bot$ ed $\to$ formano un insieme completo di connettivi (3.1.1).

Notiamo che il simbolo $\bot$ è usato soltanto nella regola di riduzione all'assurdo; sarebbe intuitivo cercare di rimuoverlo ma risulta non essere possibile. Infatti pur essendo valido il risultato dell'esercizio seguente la legge di Peirce non è dimostrabile se si rimuove la regola della riduzione all'assurdo dai sistemi di assiomi presentati.

Probabilmente abbiamo una idea intuitiva di come funzionano le dimostrazioni con le regole di inferenza adesso cerchiamo di formalizzarlo e poi vedremo degli esempi.

Definizione 4.0.1: *Albero*

Un ordine parziale $(P, \leq)$ si dice *albero* se è:

diretto verso il basso ovvero se per ogni $p, p' \in P$ esiste $q \in P$ tale che $q \leq p$ e $q \leq p'$

semilineare inferiore se per ogni $p \in P$ la restrizione dell'ordine al sottoinsieme $\{q \in P \mid q \leq p\}$ (insieme dei predecessori di p) è un ordine lineare[4]

Inoltre un elemento massimale di un albero si dice *foglia*, un elemento minimale si rice *radice* e se p_0 e p_2 sono elementi di P tali che $p_0 < p_2$ e non esiste $p_1 \in P$ tale che $p_0 < p_1 < p_2$ allora diciamo

[3] Notiamo che questa è molto simile alla regola di introduzione del $\neg$, la potremmo ricavare dall'introduzione del $\neg$ se aggiungessimo invece anche la regola della doppia negazione

che p_0 è *predecessore immediato* di p_2 e che p_2 è *successore immediato* di p_0.

Osservazione 4.0.2 Ogni albero ha al più una radice e se un albero è finito non vuoto:

- ammette una radice;
- ogni elemento non-radice ammette esattamente un predecessore immediato;
- ogni non-foglia ammette almeno un successore immediato.

Definizione 4.0.2: *Dimostrazione in deduzione naturale*

Diciamo *dimostrazione nel sistema di deduzione naturale di φ a partire da T* una funzione P con dominio un albero finito $(Tree(P), \leq_P)$ e codominio l'insieme delle istanze di regole del sistema di deduzione naturale tale che:

- se $p \in Tree(P)$ è una foglia di P allora $P(p)$ non ha premesse (quindi è necessariamente un'istanza di (Ax), $\text{In}_\top$ o $\text{In}_=$);
- se $r \in Tree(P)$ è la radice allora $P(r)$ ha come conclusione $T \vdash \varphi$
- se $p \in Tree(P)$ ha come successori immediati tutti e soli $q_1, \ldots, q_k$ allora le premesse di $P(p)$ sono tutte e sole le conclusioni dei $P(q_1), \ldots, P(q_k)$

Se tale P esiste diciamo che φ è *dimostrabile* da T nel sistema di deduzione naturale (o che T dimostra φ) e lo indichiamo come $T \vdash_{ND} \varphi$ o anche $T \vdash \varphi$.

Esercizio 4.1: *Legge di Peirce* La legge di Peirce, ovvero $((\varphi \to \psi) \to \varphi) \to \varphi$ è dimostrabile nel sistema di deduzione naturale, cioè $\vdash ((\varphi \to \psi) \to \varphi) \to \varphi$.
(Suggerimento: bisogna per forza usare da qualche parte la riduzione ad assurdo)

Svolgimento. Costruiamo la dimostrazione nel sistema di deduzione naturale (per alleggerire la notazione omettiamo le etichette delle regole):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{(\varphi \to \psi) \to \varphi \vdash (\varphi \to \psi) \to \varphi}}{(\varphi \to \psi) \to \varphi, \neg\varphi \vdash (\varphi \to \psi) \to \varphi} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \vdash \varphi}}{\neg\varphi, \varphi \vdash \varphi} \quad \dfrac{}{\neg\varphi \vdash \neg\varphi}}{\neg\varphi, \varphi \vdash \neg\varphi}}{\neg\varphi, \varphi \vdash \psi}}{\neg\varphi \vdash \varphi \to \psi}}{(\varphi \to \psi) \to \varphi, \neg\varphi \vdash \varphi \to \psi} \quad \dfrac{}{\neg\varphi \vdash \neg\varphi}}{(\varphi \to \psi) \to \varphi, \neg\varphi \vdash \varphi} \quad \dfrac{}{(\varphi \to \psi) \to \varphi, \neg\varphi \vdash \neg\varphi}}{(\varphi \to \psi) \to \varphi, \neg\varphi \vdash \bot}}{(\varphi \to \psi) \to \varphi \vdash \varphi}}{\vdash ((\varphi \to \psi) \to \varphi) \to \varphi}$$

□

Esempio 4.0.3: *Commutatività della congiunzione e disgiunzione* Come esempio dell'utilizzo delle regole di inferenza cerchiamo di dimostrare la commutatività della congiunzione, cioè

$$\varphi \wedge \psi \vdash \psi \wedge \varphi$$

Una dimostrazione può essere scritta con le regole di inferenza come un albero con in fondo la conclusione e diramandosi in alto le premesse, se ad un certo punto (finito) le premesse restano

[4] sinonimo di ordine lineare

vuote abbiamo dimostrato la conclusione.

$$\dfrac{\dfrac{\dfrac{}{\varphi \wedge \psi \vdash \varphi \wedge \psi}\,(\mathsf{Ax})}{\varphi \wedge \psi \vdash \psi}\,(\mathsf{El}_{\wedge}.) \qquad \dfrac{\dfrac{}{\varphi \wedge \psi \vdash \varphi \wedge \psi}\,(\mathsf{Ax})}{\varphi \wedge \psi \vdash \varphi}\,(\mathsf{El}.{}_{\wedge})}{\varphi \wedge \psi \vdash \psi \wedge \varphi}\,(\mathsf{In}_{\wedge})$$

Cerchiamo adesso di ricavare anche la commutatività della disgiunzione. Non possiamo usare direttamente la regola di introduzione della disgiunzione in quanto chiaramente non possiamo sperare di riuscire a dimostrare che $\psi \vee \varphi \vdash \psi$, quindi proviamo a farlo per casi.

$$\dfrac{\dfrac{}{\varphi \vee \psi \vdash \varphi \vee \psi}\,(\mathsf{Ax}) \qquad \dfrac{\dfrac{\dfrac{}{\varphi \vdash \varphi}\,(\mathsf{Ax})}{\varphi \vee \psi, \varphi \vdash \varphi}\,(\mathsf{Wk}) \qquad \dfrac{\dfrac{}{\psi \vdash \psi}\,(\mathsf{Ax})}{\varphi \vee \psi, \psi \vdash \psi}\,(\mathsf{Wk})}{\varphi \vee \psi, \varphi \vdash \psi \vee \varphi}\,(\mathsf{In}_{\vee}.) \qquad \dfrac{\varphi \vee \psi, \psi \vdash \psi \vee \varphi}{\varphi \vee \psi, \psi \vdash \psi \vee \varphi}\,(\mathsf{In}.{}_{\vee})}{\varphi \vee \psi \vdash \psi \vee \varphi}\,(\mathsf{El}_{\vee})$$

Esempio 4.0.4: *Regola del terzo escluso* Adesso cerchiamo di dimostrare la regola del terzo escluso ovvero $\vdash \varphi \vee \neg\varphi$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg(\varphi \vee \neg\varphi) \vdash \neg(\varphi \vee \neg\varphi)}}{\neg(\varphi \vee \neg\varphi), \neg\varphi \vdash \neg(\varphi \vee \neg\varphi)}\,(\mathsf{Wk}) \qquad \dfrac{\dfrac{\dfrac{}{\neg\varphi \vdash \neg\varphi}\,(\mathsf{In}_{\vee}.)}{\neg\varphi \vdash \varphi \vee \neg\varphi}}{\neg(\varphi \vee \neg\varphi), \neg\varphi \vdash \varphi \vee \neg\varphi}\,(\mathsf{Wk})}{\neg(\varphi \vee \neg\varphi), \neg\varphi \vdash \bot}\,(\mathsf{RaA}) \qquad \dfrac{\dfrac{\star\star}{\neg(\varphi \vee \neg\varphi), \varphi \vdash \bot}\,(\mathsf{El}_{\neg})}{\neg(\varphi \vee \neg\varphi) \vdash \neg\varphi}\,(\mathsf{In}_{\neg})}{\neg(\varphi \vee \neg\varphi) \vdash \varphi}\,(\mathsf{El}_{\neg})}{\vdash \varphi \vee \neg\varphi}\,(\mathsf{RaA})$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg(\varphi \vee \neg\varphi) \vdash \neg(\varphi \vee \neg\varphi)}}{\neg(\varphi \vee \neg\varphi), \varphi \vdash \neg(\varphi \vee \neg\varphi)} \qquad \dfrac{\dfrac{\dfrac{}{\varphi \vdash \varphi}}{\varphi \vdash \varphi \vee \neg\varphi}}{\neg(\varphi \vee \neg\varphi), \varphi \vdash \varphi \vee \neg\varphi}}{\neg(\varphi \vee \neg\varphi), \varphi \vdash \bot}\,(\mathsf{El}_{\neg})}{\star\star}$$

In questo modo abbiamo dimostrato una nuova 'regola ammissibile' cioè potremmo aggiungere la regola del terzo escluso

$$\dfrac{}{\vdash \varphi \vee \neg\varphi}\,(\mathsf{TE})$$

al nostro sistema deduttivo senza modificarne le capacità espressive.

Esempio 4.0.5: *Doppia negazione* Vediamo che la doppia negazione di φ equivale a φ, cioè che $\neg\neg\varphi \leftrightarrow \varphi$. Per la prima implicazione

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\neg\varphi \vdash \neg\neg\varphi}}{\neg\neg\varphi, \neg\varphi \vdash \neg\neg\varphi} \qquad \dfrac{\dfrac{}{\neg\varphi \vdash \neg\varphi}}{\neg\neg\varphi, \neg\varphi \vdash \neg\varphi}}{\neg\neg\varphi, \neg\varphi \vdash \bot}}{\neg\neg\varphi \vdash \varphi}}{\vdash \neg\neg\varphi \to \varphi}$$

ed è analoga anche l'altra:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \vdash \varphi}}{\varphi, \neg\varphi \vdash \varphi} \quad \dfrac{\dfrac{}{\neg\varphi \vdash \neg\varphi}}{\varphi, \neg\varphi \vdash \neg\varphi}}{\varphi, \neg\varphi \vdash \bot}}{\varphi \vdash \neg\neg\varphi}}{\vdash \varphi \to \neg\neg\varphi}$$

Esempio 4.0.6: *Equivalenza delle due regole di riduzione ad assurdo* Vediamo che anche la formulazione senza $\neg$ è una regola valida, ovvero che effettivamente dal sistema completo si può ricavare che

$$\dfrac{T, \varphi \to \bot \vdash \bot}{T \vdash \varphi}$$

infatti possiamo ricavare

$$\dfrac{\dfrac{\dfrac{T, \varphi \to \bot \vdash \bot}{T \vdash \neg(\varphi \to \bot)}}{T, \neg\varphi \vdash \neg(\varphi \to \bot)} \quad \dfrac{\dfrac{\dfrac{}{\varphi \vdash \varphi}}{T, \neg\varphi, \varphi \vdash \varphi} \quad \dfrac{\dfrac{}{\neg\varphi \vdash \neg\varphi}}{T, \neg\varphi, \varphi \vdash \neg\varphi}}{T, \neg\varphi, \varphi \vdash \bot}}{T, \neg\varphi \vdash \varphi \to \bot}}{T \vdash \varphi}$$

dove l'unica ipotesi rimanente è effettivamente $T, \varphi \to \bot \vdash \bot$.
Invece nel sistema in cui usiamo la regola senza $\neg$ vediamo che si può ricavare la regola con $\neg$ infatti sfruttando la doppia negazione e l'introduzione della negazione

$$\dfrac{\dfrac{}{T \vdash \varphi \vee \neg\varphi} \quad \dfrac{\dfrac{T, \neg\varphi \vdash \bot}{T, \neg\varphi \vdash \varphi}}{T, \varphi \vdash \varphi}}{T \vdash \varphi}$$

questo funziona correggendo un dettaglio infatti abbiamo dimostrato la regola del terzo escluso nel sistema con la riduzione all'assurdo che usa la negazione, dobbiamo ancora dimostrarlo in questo sistema, ma è facile adattare la dimostrazione precedente (4.0.4) a questo caso:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \to \bot, \varphi \vdash \bot}}{\varphi \to \bot \vdash \neg\varphi}}{\varphi \to \bot \vdash \varphi \vee \neg\varphi}}{(\varphi \vee \neg\varphi) \to \bot, \varphi \to \bot \vdash \varphi \vee \neg\varphi} \quad \dfrac{\dfrac{\dfrac{}{\varphi \vdash \varphi}}{\varphi \vdash \varphi \vee \neg\varphi}}{(\varphi \vee \neg\varphi) \to \bot, \varphi \vdash \varphi \vee \neg\varphi}}{(\varphi \vee \neg\varphi) \to \bot, \varphi \to \bot \vdash \bot} \quad \dfrac{(\varphi \vee \neg\varphi) \to \bot, \varphi \vdash \bot}{(\varphi \vee \neg\varphi) \to \bot \vdash \neg\varphi}}{(\varphi \vee \neg\varphi) \to \bot \vdash \bot}}{\vdash \varphi \vee \neg\varphi}$$

Esercizio 4.2: *Dimostrazione per casi* Dimostrare che nel sistema di deduzione naturale vale la dimostrazione per casi, ovvero

$$\dfrac{T, \neg\varphi \vdash \psi \quad T, \varphi \vdash \psi}{T \vdash \psi}$$

Svoglimento. Basta sfruttare la regola del terzo escluso (4.0.4) insieme alla regola di eliminazione della

disgiunzione:

$$\dfrac{\dfrac{}{\vdash \neg\varphi \vee \varphi}}{T \vdash \neg\varphi \vee \varphi} \quad T, \neg\varphi \vdash \psi \quad T, \varphi \vdash \psi \over T \vdash \psi$$

□

Esercizio 4.3 Dimostrare che nel sistema di deduzione naturale

$$\dfrac{T, \varphi \to \psi \vdash \bot}{T, \varphi \vdash \neg\psi}$$

Svolgimento. Sfruttando la dimostrazione per casi (4.2) si ottiene che:

$$\dfrac{\dfrac{T, \varphi \to \psi \vdash \bot}{T, \varphi \to \psi \vdash \neg\psi}}{T, \varphi, \varphi \to \psi \vdash \neg\psi} \quad \dfrac{\dfrac{\dfrac{}{\neg(\varphi \to \psi) \vdash \neg(\varphi \to \psi)}}{T, \varphi, \neg(\varphi \to \psi), \psi \vdash \neg(\varphi \to \psi)} \quad \dfrac{\dfrac{\dfrac{}{\psi \vdash \psi}}{\psi, \varphi \vdash \psi}}{\psi \vdash \varphi \to \psi}}{T, \varphi, \neg(\varphi \to \psi), \psi \vdash \varphi \to \psi}}{\dfrac{T, \varphi, \neg(\varphi \to \psi), \psi \vdash \bot}{T, \varphi, \neg(\varphi \to \psi) \vdash \neg\psi}} \over T, \varphi \vdash \neg\psi$$

□

Esercizio 4.4 Dimostrare che nel sistema di deduzione naturale

$$\dfrac{T \vdash \exists x.\varphi \quad T \vdash \varphi \to \psi}{T \vdash \psi}\ x \notin \mathrm{vl}(T, \psi)$$

Svolgimento. Applicando la regola di introduzione dell'implicazione e poi l'eliminazione dell'esistenziale:

$$\dfrac{T \vdash \exists x.\varphi \quad \dfrac{\dfrac{T \vdash \varphi \to \psi}{T, \varphi \vdash \varphi \to \psi} \quad \dfrac{\dfrac{}{\varphi \vdash \varphi}}{T, \varphi \vdash \varphi}}{T, \varphi \vdash \psi}}{T \vdash \psi}\ x \notin \mathrm{vl}(T, \psi)$$

□

Esercizio 4.5 Dimostrare che nel sistema di deduzione naturale

$$\dfrac{T, \varphi \vdash \bot \quad T, \varphi \to \psi \vdash \bot}{T \vdash \bot}$$

Svolgimento. Applicando le regole di inferenza:

$$\begin{array}{l}(\mathsf{El}_\bot)\ \dfrac{T, \varphi \vdash \bot}{T, \varphi \vdash \psi} \\ (\mathsf{In}_\to)\ \dfrac{}{T \vdash \varphi \to \psi} \\ (\mathsf{El}_\to)\end{array} \quad (\mathsf{In}_\to)\ \dfrac{T, \varphi \to \psi \vdash \bot}{T \vdash (\varphi \to \psi) \to \bot} \over T \vdash \bot$$

□

Nella parte precedente abbiamo già visto il teorema di compattezza in una versione 'semantica' (3.1.4) valido per $\models$.

Grazie al teorema di completezza si potrà dedurre da questo anche una versione 'sintattica' della compattezza valida per $\vdash$ ma non avendo ancora dimostrato la completezza se vogliamo sfruttare la compattezza sintattica dobbiamo dimostrarla separatamente.

Teorema 4.0.3: *di Compattezza (sintattica)*

> Data una L-teoria T ed una L-formula φ se $T \vdash \varphi$ allora esiste una sottoteoria finita $T' \subseteq T$ tale che $T' \vdash \varphi$.

Dimostrazione. Se $T \vdash \varphi$ allora esiste una dimostrazione P di φ a partire da T, proseguiamo per induzione strutturale sugli alberi finiti (ovvero per induzione sull'altezza dell'albero $Tree(P)$).

Sia r la radice di $Tree(P)$ ed R la regola istanziata in $P(r)$, procediamo per casi a seconda di che regola sia R:

- Se R è Ax allora r è l'unico membro dell'albero ed in tutto l'albero c'è una sola formula a sinista di $\vdash$, quindi selezionando questa formula come T' abbiamo una dimostrazione di φ.
- Se R è una regola tra $\text{In}_\top$, $\text{El}_\bot$, $\text{In}_\wedge$, $\text{El}_{\wedge\cdot}$, $\text{El}_{\cdot\wedge}$, $\text{In}_{\cdot\vee}$, $\text{In}_{\vee\cdot}$, $\text{El}_\neg$, $\text{El}_\to$, $\text{In}_\exists$, $\text{In}_\forall$, $\text{El}_\forall$, $\text{In}_=$ ed $\text{El}_=$ sia nelle premesse che nella conclusione della regola c'è sempre una stessa teoria quindi per ogni premessa $T_i \vdash \varphi$ nella istanza $P(r)$ possiamo trovare per ipotesi induttiva una dimostrazione di $S_i \vdash \varphi$ con $S_i \subseteq T_i$ finito, quindi ponendo $T' \doteq \bigcup S_i$ ed utilizzando Wk su tutte le premesse di $P(r)$ per portarle a $T' \vdash \varphi_i$ si ottiene una dimostrazione di $T' \vdash \varphi$.
- Rimangono i casi di Wk, $\text{El}_\vee$, $\text{In}_\to$, $\text{In}_\neg$, $\text{El}_\exists$ e RaA: tutti questi hanno una conclusione della forma $T \vdash \varphi$ e le premesse sono tutte o della forma $T \vdash \varphi_i$ oppure $T, \psi_i \vdash \varphi_i$; su entrambe di queste si può applicare l'ipotesi induttiva per ottenere un sottoinsieme finito $S_i \subseteq T \cup \{\psi_i\}$ tale che $S_i \vdash \varphi_i$. Definendo $T' = \bigcup S_i$ a meno di usare un'altra volta Wk su tutte le premesse di $P(r)$ queste si possono portare rispettivamente nella forma $T' \vdash \varphi_i$ oppure $T', \psi_i \vdash \varphi_i$ a seconda di come richiesto per utilizzare la regola R, ottenendo così una dimostrazione di $T' \vdash \varphi$.

□

4.1 Il sistema ridotto

Come visto nella dimostrazione dell'ultimo teorema (4.0.3) effettuare una dimostrazione per induzione nel sistema di deduzione naturale può essere laborioso semplicemente per il fatto che ci sono molti casi, quindi effettivamente potrebbe essere utile il sistema ridotto.

Il sistema ridotto è minimale, cioè rimuovendo una qualunque regola dal sistema non varrebbe più il teorema di completezza, ma a noi questo non servirà per utilizzarlo; quindi ci limiteremo a mostrare che è equivalente al sistema di deduzione naturale completo, ovvero che il sistema ridotto può dimostrare tutte e sole le stesse formule del sistema completo a partire da una data teoria, senza dimostrarne la minimalità.

Per adesso usiamo la notazione $\vdash_R$ per indicare che una formula è dimostrabile usando soltanto le regole del sistema ridotto fino a quando mostreremo che questo equivale a $\vdash$.

Chiaramente il sistema completo è debolmente più forte di quello ridotto in quanto include tutte le regole che costituiscono il sistema ridotto, per mostrare l'equivalenza ci basta quindi mostrare che dal sistema ridotto si possono ricavare tutte le regole del sistema completo, da cui segue che anche il sistema ridotto è debolmente più forte di quello completo quindi sono equivalenti.

Se defininiamo $\neg, \top, \wedge, \vee, \forall$ a partire dai simboli nel sistema ridotto

$$\neg\varphi \doteq \varphi \to \bot \quad \top \doteq \neg\bot \quad \varphi \wedge \psi \doteq \neg(\varphi \to \neg\psi) \quad \varphi \vee \psi \doteq \neg\varphi \to \psi \quad \forall x_k.\varphi \doteq \neg\exists x_k.\neg\varphi \tag{4.1}$$

data una L-formula φ possiamo indicare $tr(\varphi)$ la 'traduzione' ottenuta sostituendo tutte le occorrenze dei simboli $\neg, \top, \wedge, \vee, \forall$ ricorsivamente fino ad ottenere una formula che usa soltanto $\bot, \to, \exists, =$ oltre ad i simboli in L.

In maniera analoga si possono definire la traduzione di una teoria e la traduzione di una istanza di una regola di inferenza.

Proposizione 4.1.1

Data una L-formula φ e la L-formula ψ ottenuta sostituendo una istanza delle abbreviazioni (4.1) ad una occorrenza di $\neg, \top, \wedge, \vee$ o $\forall$ in φ allora φ è sintatticamente equivalente a ψ, cioè valgono sia $\varphi \vdash \psi$ che $\psi \vdash \varphi$ o, equivalentemente, vale

$$\vdash (\varphi \to \psi) \wedge (\psi \to \varphi)$$

Dimostrazione. Chiaramente le due formulazioni dell'equivalenza sintattica sono equivalenti infatti:

$$\dfrac{\dfrac{\vdash (\varphi \to \psi) \wedge (\psi \to \varphi)}{\vdash \varphi \to \psi}}{\varphi \vdash \varphi \to \psi} \qquad \dfrac{}{\varphi \vdash \varphi}$$
$$\varphi \vdash \psi$$

ed in maniera simmetrica segue da $\vdash (\varphi \to \psi) \wedge (\psi \to \varphi)$ che $\psi \vdash \varphi$ mentre vale anche che

$$\dfrac{\dfrac{\varphi \vdash \psi}{\vdash \varphi \to \psi} \qquad \dfrac{\psi \vdash \varphi}{\vdash \psi \to \varphi}}{\vdash (\varphi \to \psi) \wedge (\psi \to \varphi)}$$

Vediamo che $\neg\varphi$ è equivalente a $\varphi \to \bot$ mostrando che $\neg\varphi \vdash \varphi \to \bot$ e che $\varphi \to \bot \vdash \neg\varphi$

$$\dfrac{\dfrac{\dfrac{}{\neg\varphi \vdash \neg\varphi}}{\neg\varphi, \varphi \vdash \neg\varphi} \qquad \dfrac{\dfrac{}{\varphi \vdash \varphi}}{\neg\varphi, \varphi \vdash \varphi}}{\dfrac{\neg\varphi, \varphi \vdash \bot}{\neg\varphi \vdash \varphi \to \bot}} \qquad \dfrac{\dfrac{\dfrac{}{\varphi \to \bot \vdash \varphi \to \bot}}{\varphi \to \bot, \varphi \vdash \varphi \to \bot} \qquad \dfrac{\dfrac{}{\varphi \vdash \varphi}}{\varphi \to \bot, \varphi \vdash \varphi}}{\dfrac{\varphi \to \bot, \varphi \vdash \bot}{\varphi \to \bot \vdash \neg\varphi}}$$

Invece per l'equivalenza di $\top$ con $\neg\bot$ possiamo usare l'altra formulazione dell'equivalenza semantica, infatti

$$\dfrac{\dfrac{\dfrac{}{\vdash \top}}{\neg\bot \vdash \top}}{\vdash \neg\bot \to \top} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\bot \vdash \bot}}{\top, \bot \vdash \bot}}{\top \vdash \neg\bot}}{\vdash \top \to \neg\bot}$$
$$\vdash (\neg\bot \to \top) \wedge \top \to \neg\bot$$

Per mostrare l'equivalenza di $\varphi \wedge \psi$ con $\neg(\varphi \to \neg\psi)$ vediamo che data una teoria T

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \wedge \psi \vdash \varphi \wedge \psi}}{\varphi \wedge \psi \vdash \psi}}{\varphi \wedge \psi, \varphi \to \neg\psi \vdash \psi} \qquad \dfrac{\dfrac{}{\varphi \to \neg\psi \vdash \varphi \to \neg\psi}}{\varphi \wedge \psi, \varphi \to \neg\psi \vdash \varphi \to \neg\psi} \qquad \dfrac{\dfrac{\dfrac{}{\varphi \wedge \psi \vdash \varphi \wedge \psi}}{\varphi \wedge \psi \vdash \varphi}}{\varphi \wedge \psi, \varphi \to \neg\psi \vdash \varphi}}{\varphi \wedge \psi, \varphi \to \neg\psi \vdash \neg\psi}$$
$$\dfrac{\varphi \wedge \psi, \varphi \to \neg\psi \vdash \bot}{\varphi \wedge \psi \vdash \neg(\varphi \to \neg\psi)}$$

e dall'altro lato dimostriamo che

$$\dfrac{\dfrac{\dfrac{\dots}{\neg(\varphi \to \neg\psi), \neg\varphi \vdash \bot}}{\neg(\varphi \to \neg\psi) \vdash \varphi} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\psi \vdash \neg\psi}}{\neg\psi, \varphi \vdash \neg\psi}}{\neg\psi \vdash \varphi \to \neg\psi}}{\neg(\varphi \to \neg\psi), \neg\psi \vdash \varphi \to \neg\psi} \qquad \dfrac{\dfrac{}{\neg(\varphi \to \neg\psi) \vdash \neg(\varphi \to \neg\psi)}}{\neg(\varphi \to \neg\psi), \neg\psi \vdash \neg(\varphi \to \neg\psi)}}{\neg(\varphi \to \neg\psi), \neg\psi \vdash \bot}}{\neg(\varphi \to \neg\psi) \vdash \psi}$$
$$\neg(\varphi \to \neg\psi) \vdash \varphi \wedge \psi$$

dove

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varphi \vdash \varphi}}{\neg\varphi, \varphi \vdash \varphi} \quad \dfrac{}{\neg\varphi, \varphi \vdash \neg\varphi}}{\neg\varphi, \varphi \vdash \bot}}{\neg\varphi, \varphi \vdash \neg\psi}}{\neg\varphi \vdash \varphi \to \neg\psi} \quad \dfrac{}{\neg(\varphi \to \neg\psi) \vdash \neg(\varphi \to \neg\psi)}}{\neg(\varphi \to \neg\psi), \neg\varphi \vdash \varphi \to \neg\psi} \quad \dfrac{}{\neg(\varphi \to \neg\psi), \neg\varphi \vdash \neg(\varphi \to \neg\psi)}}{\dfrac{\neg(\varphi \to \neg\psi), \neg\varphi \vdash \bot}{\cdots}}$$

Per la disgiunzione iniziamo mostrando che $\neg\varphi \to \psi \vdash \varphi \vee \psi$ omettendo dove sono ovvi dei passi di Wk per abbreviare la notazione

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\varphi \to \psi \vdash \neg\varphi \to \psi}}{\neg\varphi \to \psi, \neg(\varphi \vee \psi) \vdash \neg\varphi \to \psi} \quad \dfrac{\dfrac{\dfrac{}{\neg(\varphi \vee \psi) \vdash \neg(\varphi \vee \psi)} \quad \dfrac{}{\varphi \vdash \varphi \vee \psi}}{\neg(\varphi \vee \psi), \varphi \vdash \bot}}{\neg(\varphi \vee \psi) \vdash \neg\varphi}}{\neg\varphi \to \psi, \neg(\varphi \vee \psi) \vdash \psi} \quad \dfrac{\dfrac{\dfrac{}{\neg(\varphi \vee \psi) \vdash \neg(\varphi \vee \psi)} \quad \dfrac{}{\psi \vdash \varphi \vee \psi}}{\neg(\varphi \vee \psi), \psi \vdash \bot}}{\neg(\varphi \vee \psi) \vdash \neg\psi}}{\dfrac{\neg\varphi \to \psi, \neg(\varphi \vee \psi) \vdash \bot}{\neg\varphi \to \psi \vdash \varphi \vee \psi}}$$

mentre per mostrare che $\varphi \vee \psi \vdash \neg\varphi \to \psi$ omettiamo anche la dimostrazione ovvia (gia vista in altri casi precedenti) di $\neg\psi, \psi \vdash \bot$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\varphi \vdash \neg\varphi} \quad \dfrac{\dfrac{}{\varphi \vee \psi \vdash \varphi \vee \psi} \quad \dfrac{}{\neg\psi, \varphi \vdash \varphi}}{\varphi \vee \psi, \neg\psi \vdash \varphi} \quad \dfrac{\neg\psi, \psi \vdash \bot}{\neg\psi, \psi \vdash \varphi}}{\varphi \vee \psi, \neg\varphi, \neg\psi \vdash \bot}}{\varphi \vee \psi, \neg\varphi \vdash \psi}}{\varphi \vee \psi \vdash \neg\varphi \to \psi}$$

Per il quantificatore universale dato che $x_i \notin \mathrm{vl}(\exists\, x_i.\neg\varphi)$

$$\dfrac{\dfrac{\dfrac{}{\neg\exists\, x_i.\neg\varphi \vdash \neg\exists\, x_i.\neg\varphi} \quad \dfrac{\dfrac{\dfrac{}{\neg\varphi \vdash x_i = x_i} \quad \dfrac{}{\neg\varphi \vdash \neg\varphi}}{\neg\varphi \vdash \neg\varphi\left[x_i \diagup x_i\right]}}{\neg\varphi \vdash \exists\, x_i.\neg\varphi}}{\neg\exists\, x_i.\neg\varphi, \varphi \vdash \bot}}{\dfrac{\neg\exists\, x_i.\neg\varphi \vdash \varphi}{\neg\exists\, x_i.\neg\varphi \vdash \forall\, x_i.\varphi}}$$

e per concludere dato che $x_i \notin \mathrm{vl}\,\{\forall\, x_i.\varphi, \bot\}$

$$\dfrac{\dfrac{\dfrac{}{\exists\, x_i.\neg\varphi \vdash \exists\, x_i.\neg\varphi} \quad \dfrac{\dfrac{\dfrac{}{\forall\, x_i.\varphi \vdash \forall\, x_i.\varphi}}{\forall\, x_i.\varphi \vdash \varphi\left[x_i \diagup x_i\right]} \quad \dfrac{\dfrac{}{\neg\varphi \vdash x_i = x_i} \quad \dfrac{}{\neg\varphi \vdash \neg\varphi}}{\neg\varphi \vdash \neg\varphi\left[x_i \diagup x_i\right]}}{\forall\, x_i.\varphi, \neg\varphi \vdash \bot}}{\forall\, x_i.\varphi, \exists\, x_i.\neg\varphi \vdash \bot}}{\forall\, x_i.\varphi \vdash \neg\exists\, x_i.\neg\varphi}$$

□

Corollario 4.1.1.1

una qualunque formula φ è sintatticamente equivalente a $tr(\varphi)$.

Proposizione 4.1.2

Per ogni regola del sistema di deduzione naturale la sua traduzione nel sistema ridotto è una regola ammissibile nel sistema ridotto.

Esercizio 4.6 Dimostrare la proposizione precedente.

Svolgimento. Iniziamo con le regole di introduzione di $\top$ ed eliminazione di $\bot$:

$$\dfrac{\dfrac{}{\bot \vdash \bot}}{\vdash \bot \to \bot} \qquad \dfrac{\dfrac{T \vdash \bot}{T, \varphi \to \bot \vdash \bot}}{T \vdash \varphi}$$

Procediamo con le regole di introduzione ed eliminazione della negazione notando la prima è esattamente la regola di introduzione dell'implicazione nel caso particolare di $\psi = \bot$ e dove per la seconda usiamo la regola già dimostrata dell'eliminazione di $\bot$

$$\dfrac{\dfrac{}{T, \varphi \vdash \bot}}{T \vdash \varphi \to \bot} \qquad \dfrac{T \vdash \varphi \to \bot \quad T \vdash \varphi}{\dfrac{T \vdash \bot}{T \vdash \psi}}$$

Per la regola di introduzione della congiunzione, dove $tr(\varphi \wedge \psi) = (\varphi \to (\psi \to \bot)) \to \bot$ usando la regola già verificata di eliminazione della negazione

$$\dfrac{\dfrac{\dfrac{T \vdash \psi}{T\varphi \to (\psi \to \bot) \vdash \psi} \quad \dfrac{\dfrac{}{\varphi \to (\psi \to \bot) \vdash \varphi \to (\psi \to \bot)} \quad T \vdash \varphi}{T, \varphi \to (\psi \to \bot) \vdash \psi \to \bot}}{T\varphi \to (\psi \to \bot) \vdash \bot}}{T \vdash (\varphi \to (\psi \to \bot)) \to \bot}$$

e per le sue regole di eliminazione invece

$$\dfrac{T \vdash (\varphi \to (\psi \to \bot)) \to \bot \quad \dfrac{\dfrac{\dfrac{}{\varphi \vdash \varphi} \quad \dfrac{}{\varphi \to \bot \vdash \varphi \to \bot}}{\varphi \to \bot, \varphi \vdash \psi \to \bot}}{\varphi \to \bot \vdash \varphi \to (\psi \to \bot)}}{\dfrac{T, \varphi \to \bot \vdash \bot}{T \vdash \varphi}} \qquad \dfrac{T \vdash (\varphi \to (\psi \to \bot)) \to \bot \quad \dfrac{\dfrac{}{\psi \to \bot, \varphi \vdash \psi \to \bot}}{\psi \to \bot \vdash \varphi \to (\psi \to \bot)}}{\dfrac{T, \psi \to \bot \vdash \bot}{T \vdash \psi}}$$

Per le regole di introduzione della disgiunzione ($tr(\varphi \vee \psi) = (\varphi \to \bot) \to \psi$)

$$\dfrac{\dfrac{\dfrac{}{\varphi \to \bot \vdash \varphi \to \bot} \quad T \vdash \varphi}{T, \varphi \to \bot \vdash \psi}}{T \vdash (\varphi \to \bot) \to \psi} \qquad \dfrac{\dfrac{T \vdash \psi}{T, \varphi \to \bot \vdash \psi}}{T \vdash (\varphi \to \bot) \to \psi}$$

e per l'eliminazione della disgiunzione

$$\dfrac{T\vdash(\varphi\to\bot)\to\psi \qquad \dfrac{\dfrac{\dfrac{T,\psi\vdash\theta \quad \overline{\theta\to\bot\vdash\theta\to\bot}}{T,\theta\to\bot,\psi\vdash\bot}}{T,\theta\to\bot\vdash\psi\to\bot} \qquad \dfrac{\overline{(\varphi\to\bot)\to\psi\vdash(\varphi\to\bot)\to\psi} \qquad \dfrac{\dfrac{T,\varphi\vdash\theta \quad \overline{\theta\to\bot\vdash\theta\to\bot}}{T,\theta\to\bot,\varphi\vdash\bot}}{T,\theta\to\bot\vdash\varphi\to\bot}}{T,\theta\to\bot,(\varphi\to\bot)\to\psi\vdash\psi}}{T,\theta\to\bot,(\varphi\to\bot)\to\psi\vdash\bot}}{T,\theta\to\bot\vdash((\varphi\to\bot)\to\psi)\to\bot}}{T,\theta\to\bot\vdash\bot}}{T\vdash\theta}$$

Per l'introduzione del quantificatore universale ($tr(\forall\, x_k.\varphi)=(\exists\, x_k.\varphi\to\bot)\to\bot$) vediamo che

$$\dfrac{\dfrac{\dfrac{}{\exists\, x_k.\varphi\to\bot\vdash\exists\, x_k.\varphi\to\bot} \qquad \dfrac{T\vdash\varphi \quad \overline{\varphi\to\bot\vdash\varphi\to\bot}}{T,\varphi\to\bot\vdash\bot}\ x_i\notin \mathrm{vl}(T,\bot)=\mathrm{vl}(T)}{T,\exists\, x_k.\varphi\to\bot\vdash\bot}}{T\vdash(\exists\, x_k.\varphi\to\bot)\to\bot}$$

Per concludere rimane da verificare soltanto il caso dell'eliminazione del quantificatore universale e, dato che per definizione $\varphi\left[{}^{t}/_{x_i}\right]\to\bot=(\varphi\to\bot)\left[{}^{t}/_{x_i}\right]$, vediamo che

$$\dfrac{\dfrac{T\vdash(\exists\, x_k.\varphi\to\bot)\to\bot \qquad \dfrac{\overline{\varphi\left[{}^{t}/_{x_i}\right]\to\bot\vdash(\varphi\to\bot)\left[{}^{t}/_{x_i}\right]}}{\varphi\left[{}^{t}/_{x_i}\right]\to\bot\vdash\exists\, x_k.\varphi\to\bot}}{T,\varphi\left[{}^{t}/_{x_i}\right]\to\bot\vdash\bot}}{T\vdash\varphi\left[{}^{t}/_{x_i}\right]}$$

□

Corollario 4.1.2.1

Data una qualunque teoria T ed una qualunque formula φ vale $T\vdash\varphi$ se e solo se $tr(T)\vdash_R tr(\varphi)$.

Corollario 4.1.2.2

Una qualunque regola R è ammissibile nel sistema di deduzione naturale se e solo se la sua traduzione $tr(R)$ è ammissibile nel sistema ridotto.

Corollario 4.1.2.3

Il sistema ridotto è sintatticamente compatto, cioè se $T\vdash_R\varphi$ allora esiste un sottoinsieme finito $T'\subseteq T$ tale che $T'\vdash_R\varphi$.

Proposizione 4.1.3

Data una L-formula φ e la L-formula ψ ottenuta sostituendo una istanza delle abbreviazioni (4.1) ad una occorrenza di $\neg,\top,\wedge,\vee$ o $\forall$ in φ allora φ è semanticamente equivalente a ψ (2.3.9).

Esercizio 4.7 Dimostrare la tesi (apparentemente più forte della proposizione 4.1.3) che per ogni formula φ data una formula ψ ottenuta stituendo una istanza delle abbreviazioni (4.1) ad una

occorrenza di $\neg, \top, \wedge, \vee$ o $\forall$ in φ e dato una struttura M con una valutazione delle variabili v vale

$$M \vDash \{v\}\varphi \iff M \vDash \{v\}\psi$$

Svolgimento. Procediamo per casi:

- Se $\varphi = \top$ allora in tutti i modelli e con tutte le valutazioni vale $M \vDash \{v\}\neg\bot$ per la semantica di Tarski.
- Se $\varphi \doteq \neg\psi$ per la semantica di Tarski $M \vDash \{v\}\varphi$ se e solo se $M \nvDash \{v\}\psi$ ed essendo $\bot$ falsa in tutti i modelli per la semantica di Tarski questo equivale a dire che $M \vDash \{v\}\psi \to \bot$.
- Se $\varphi \doteq \psi \wedge \theta$ per la semantica di Tarski $M \vDash \{v\}\neg(\varphi \to \neg\psi)$ se e solo se $M \nvDash \{v\}\varphi \to \neg\psi$ e sempre per la semantica di Tarski questo vale se e solo se in M nel contesto v sono vere sia φ che ψ, ovvero se e solo se $M \vDash \{v\}\varphi$.
- Nel caso di $\varphi \doteq \psi \vee \theta$ si procede in maniera analoga al precedente.
- Se $\varphi \doteq \forall x_k.\psi$ allora per la semantica di Tarski $M \vDash \{v\}\varphi$ se e solo se dato un qualunque $a \in M$ vale $M \vDash \{v\}\psi\left[{}^{a}/_{x_k}\right]$, ovvero se e solo se dato un qualunque $a \in M$ vale $M \nvDash \{v\}\neg\psi\left[{}^{a}/_{x_k}\right]$ quindi per la semantica di Tarski vale $M \nvDash \{v\}\exists x_k.\psi$ ovvero $M \vDash \{v\}\neg\exists x_k.\psi$

□

4.2 Il teorema di correttezza

Teorema 4.2.1: *di Correttezza*

Per ogni L-teoria T ed ogni L-formula φ se $T \vdash \varphi$ allora $T \vDash \varphi$.

Dimostrazione. Per i risultati della sezione precedente $T \vdash \varphi$ se e solo se $T \vdash_R \varphi$, quindi possiamo limitarci a fare meno casi.

Se P è una dimostrazione di φ a partire da T (senza perdita di generalità nel sistema ridotto) mostriamo per induzione sull'altezza di P che $T \vDash \varphi$.

Per il passo base con $h(tree(P)) = 1$ allora $tree(P)$ è composto dalla sola radice r e necessariamente $P(r)$ è una istanza di Ax oppure In$_=$, nel caso di Ax necessariamente $T = \{\varphi\}$ ed è banalmente vero che $\varphi \vDash \varphi$; mentre nel caso di In$_=$ la teoria T è la teoria vuota e tautologicamente dato un qualunque terminte t, una qualunque struttura M ed una qualunque valutazione v vale $\{v\}t = \{v\}t$, cioè per la semantica di Tarski (2.1.2) data una qualunque L-struttura M vale $M \vDash t = t$, ovvero $\varnothing \vDash t = t$.

Per il passo induttivo supponiamo che $h(tree(P)) = k > 1$ e che per ogni formula dimostrabile da una qualunque teoria tramite un albero di altezza minore di k la tesi sia vera, separiamo in casi a seconda di che regola $P(r)$ è una istanza (basta considerare le regole nel sistema ridotto eccetto Ax in quanto $k > 1$):

$P(r)$ **istanzia Wk** con $P(r) = \dfrac{T_1 \vdash \varphi}{T \vdash \varphi}$ $T_1 \subseteq T$ allora per ipotesi induttiva $T_1 \vDash \varphi$ ma ogni modello di T è anche un modello di $T_1 \subseteq T$, quindi per ogni modello M di T vale $M \vDash \varphi$, quindi $T \vDash \varphi$.

$P(r)$ **istanzia RaA** con $P(r) = \dfrac{T, \varphi \to \bot \vdash \bot}{T \vdash \varphi}$ allora per ipotesi induttiva $T, \varphi \to \bot \vDash \bot$, quindi possiamo distinguere due sottocasi:

- se $T \vDash \bot$ allora $T \vDash \varphi$;
- altrimenti esiste un modello di T, dato un qualunque modello M di T necessariamente deve valere $M \vDash \neg(\varphi \to \bot)$ (altrimenti $M \vDash \bot$) quindi per la semantica di Tarski $M \nvDash \varphi \to \bot$ ma se per assurdo $M \vDash \neg\varphi$ allora l'ipotesi dell'implicazione è falsa in M ma dalla semantica di Tarski questo implica l'assurdo $M \vDash \varphi \to \bot$, ovvero per ogni modello M di T vale $M \vDash \varphi$, cioè per definizione $T \vDash \varphi$.

$P(r)$ **istanzia In$_\to$** con $P(r) = \dfrac{T, \varphi \vdash \psi}{T \vdash \varphi \to \psi}$ allora per ipotesi induttiva $T, \varphi \vdash \psi$ ovvero ogni modello di T e φ è anche un modello di ψ, quindi per ogni modello di T in cui vale φ allora vale anche ψ (per la semantica di Tarski) ed in ogni modello di T in cui non vale φ l'implicazione $\varphi \to \psi$ è valida per la semantica di Tarski, cioè ogni modello M di T verifica $M \vDash \varphi$, ovvero $T \vDash \varphi$.

$P(r)$ **istanzia El$_\to$** con $P(r) = \dfrac{T \vdash \varphi \to \psi \qquad T \vdash \varphi}{T \vdash \psi}$ allora per ipotesi induttiva $T \vDash \varphi \to \psi$ e $T \vDash \varphi$ quindi per la semantica di Tarski $T \vDash \psi$.

$P(r)$ **istanzia El$_=$** con $P(r) = \dfrac{T \vdash t = s \qquad T \vdash \varphi\left[{}^{s}\!/_{x_k}\right]}{T \vdash \varphi\left[{}^{t}\!/_{x_k}\right]}$ allora per ipotesi induttiva $T \vDash t = s$ e $T \vDash \varphi\left[{}^{s}\!/_{x_k}\right]$ quindi dato un qualunque modello M di T ed una qualunque valutazione v vale $\{v\}\, t = \{v\}\, s$ da cui per il lemma 2.2.3

$$M \vDash \{v\}\, \varphi\left[{}^{s}\!/_{x_k}\right] \iff M \vDash \left\{v\left[{}^{\{v\}\, t}\!/_{x_k}\right]\right\} \varphi \iff M \vDash \left\{v\left[{}^{\{v\}\, s}\!/_{x_k}\right]\right\} \varphi \iff M \vDash \{v\}\, \varphi\left[{}^{t}\!/_{x_k}\right]$$

ovvero $T \vDash \varphi\left[{}^{t}\!/_{x_k}\right]$

$P(r)$ **istanzia In$_\exists$** con $P(r) = \dfrac{T \vdash \varphi\left[{}^{t}\!/_{x_k}\right]}{T \vdash \exists\, x_k.\varphi}$ allora per ipotesi induttiva $T \vDash \varphi\left[{}^{t}\!/_{x_k}\right]$ quindi per ogni modello M di T e per ogni valutazione delle variabili v esiste un elemento a del dominio di M tale che l'interpretazione di t nel modello M con valutazione v è $\{v\}\, t = a$ e per ipotesi induttiva $M \vDash \varphi\left[{}^{a}\!/_{x_k}\right]$, quindi per la semantica di Tarski ogni modello M di T con una qualunque valutazione delle variabili v soddisfa $M \vDash \{v\}\, \exists\, x_k.\varphi$ ovvero $T \vDash \exists\, x_k.\varphi$.

$P(r)$ **istanzia El$_\exists$** con $P(r) = \dfrac{T \vdash \exists\, x_k.\varphi \qquad T, \varphi \vdash \psi}{T \vdash \psi}$ $x_k \notin \mathrm{vl}(T, \psi)$ allora per ipotesi induttiva $T \vDash \exists\, x_k.\varphi$ e $T, \varphi \vDash \psi$, quindi fissati un qualunque modello M di T ed una qualunque valutazione v esiste un elemento a nel dominio di M tale che $M \vDash \left\{v\left[{}^{a}\!/_{x_k}\right]\right\} \varphi$ e per ipotesi $x_k \notin \mathrm{vl}(T)$, quindi per la proposizione 2.1.3

$$M \vDash \{v\}\, T \qquad \iff \qquad M \vDash \left\{v\left[{}^{a}\!/_{x_k}\right]\right\} T$$

da cui per costruzione segue che $M \vDash \left\{v\left[{}^{a}\!/_{x_k}\right]\right\} T, \varphi$ ovvero per ipotesi induttiva vale che $M \vDash \left\{v\left[{}^{a}\!/_{x_k}\right]\right\} \psi$, e sempre per la proposizione 2.1.3 dato che $x_k \notin \mathrm{vl}(\psi)$ allora $M \vDash \left\{v\left[{}^{a}\!/_{x_k}\right]\right\} \psi$ è equivalente a $M \vDash \{v\}\, \psi$, cioè effettivamente $T \vDash \psi$.

□

Corollario 4.2.1.1

Se $T \vdash \bot$ allora T non ammette alcun modello.

Capitolo 5

Il teorema di completezza

Per dimostrare il teorema di completezza inizieremo con una parentesi su dei lemmi importanti (5.1.1) che ci serviranno più avanti. Poi dimostreremo che se una teoria T non dimostra $\bot$ allora T è coerente (l'implicazione inversa del corollario 4.2.1.1, o più precisamente l'implicazione inversa alla sua contronominale).

Per dimostrare questo passeremo per la *costruzione di Henkin*, che possiamo interpretare come una generalizzazione della presentazione di un gruppo con generatori e relazioni.

Per esempio, nella teoria dei gruppi possiamo presentare un gruppo come ad esempio $\langle S|R\rangle$ dove $S = \{a, b\}$ ed $R = \{a\,b\,a^{-1}\,b^{-1}\}$, quindi vorremmo poterlo descrivere come modello della teoria $T_{grp} \cup \{r = e \mid r \in R\}$; al livello di teoria dei gruppi questo funziona: prendiamo il gruppo libero generato da due elementi e lo quozientiamo per il sottogruppo normale generato dalle relazioni.

Ma come facciamo a generalizzare questa costruzione?

Continuando con un altro esempio se cerchiamo di rappresentare un modello di ZFC, avremo sicuramente bisogno di aggiungere qualcosa perché il linguaggio di ZFC non ha costanti, anzi vedremo che per ogni formula tale che $T_{ZFC} \vdash \exists\, x.\varphi(x)$ avremo bisogno di un simbolo di costante per indicare nel modello quale elemento soddisfa φ; in questo modo espanderemo il linguaggio L e la teoria T a teorie dette *di Henkin* su cui sarà più facile ottenere la completezza.

Quindi riassumiamo il procedimento che useremo per dimostrare che se $T \nvdash \bot$ allora T è coerente in un elenco numerato:

1. partiamo da una teoria T tale che $T \nvdash \bot$;
2. espandiamo T a T' nel linguaggio $L' \supset L$ in modo che $T' \nvdash \bot$ e che contiene un simbolo di costante per ogni formula esistenziale dimostrata da T, ovvero tale che se $T \vdash \exists\, x_k.\varphi(x_k)$ allora esiste $c \in L'$ tale che $T \vdash \varphi(c)$;
3. espandiamo T' a T'', stavolta senza bisogno di aggiungere simboli al linguaggio, in modo che ancora $T'' \nvdash \bot$ e che T'' sia 'più grande possibile';
4. costruiamo un modello M con dominio il quoziente

   $$\{L'\text{-termini chiusi}\}\big/_{T \vdash t = t'}$$

   cioè quozientando gli L'-termini chiusi in modo da rendere uguali tutti i termini che devono essere uguali per T;
5. controlliamo che $M \vDash T$.

5.1 Lemmi delle costanti

Più avanti vorremo poter lavorare soltanto con enunciati (2.1.4) invece che qualunque tipo di formula (così da non doverci preoccupare di valutazioni delle variabili quando ci chiediamo se $M \vDash \varphi$) quindi vorremmo poter dire che restringendoci a formule senza variabili libere non si perde valore espressivo.

Lemma 5.1.1: *delle costanti*

Date una L-teoria T, una L-formula φ ed una variabile x_k sia c un simbolo di costante tale che $c \notin L$ allora:

- c è sostituibile ad x_k (cioè $\varphi\left[{}^{c}\!/_{x_k}\right]$ è ben definito);
- le seguenti sono equivalenti:

$$T \vdash \varphi\left[{}^{c}\!/_{x_k}\right] \quad , \quad T \vdash \forall x_k.\varphi \quad , \quad T, \exists x_k.\neg\varphi \vdash \bot$$

dove consideriamo la prima come dimostrabilità nel linguaggio $L \cup \{c\}$, che possiamo indicare come $L(c)$, mentre le altre due sono intese come dimostrabilità strettamente nel linguaggio L.

Esercizio 5.1 Dimostrare il lemma precedente.

Svolgimento. Essendo c un simbolo di costante $\mathrm{var}(c) = \varnothing$ quindi per definizione c è sostituibile ad ogni variabile in qualunque L-formula.

Se $T \vdash \varphi\left[{}^{c}\!/_{x_k}\right]$ allora per compattezza sintattica (4.0.3) esiste $T_0 \subseteq T$ finito tale che esiste una dimostrazione P di $\varphi\left[{}^{c}\!/_{x_k}\right]$ a partire da T_0.

Essendo sia T_0 che P finiti esiste una variabile x_l che non compare né in T_0 né nella dimostrazione P, quindi sostituendo passo passo tutte le istanze di c con x_l otteniamo una dimostrazione valida di $\varphi\left[{}^{x_l}\!/_{x_k}\right]$ a partire da $T_0\left[{}^{c}\!/_{x_k}\right] \equiv T_0$, questa dimostrazione non menziona mai c quindi ci siamo ristretti dal linguaggio $L(c)$ nel linguaggio L.

Vediamo che da questo segue che $T \vdash \forall x_k.\varphi$ infatti

$$\dfrac{\dfrac{T_0 \vdash \varphi\left[{}^{x_l}\!/_{x_k}\right]}{T_0 \vdash \forall x_l.\varphi\left[{}^{x_l}\!/_{x_k}\right]}\; x_l \notin \mathrm{vl}(T_0) \qquad \dfrac{\dfrac{}{\forall x_l.\varphi\left[{}^{x_l}\!/_{x_k}\right] \vdash \forall x_l.\varphi\left[{}^{x_l}\!/_{x_k}\right]}}{\forall x_l.\varphi\left[{}^{x_l}\!/_{x_k}\right] \vdash \varphi\left[{}^{x_k}\!/_{x_k}\right] (\equiv \varphi)}}{\forall x_l.\varphi\left[{}^{x_l}\!/_{x_k}\right] \vdash \forall x_k.\varphi}\; x_k \notin \mathrm{vl}\left(\forall x_l.\varphi\left[{}^{x_l}\!/_{x_k}\right]\right)}{\dfrac{T_0 \vdash \forall x_k.\varphi}{T \vdash \forall x_k.\varphi}}$$

dove abbiamo usato la regola

$$\dfrac{T \vdash \varphi \qquad \varphi \vdash \psi}{T \vdash \psi}$$

che è valida nel sistema di deduzione naturale, infatti la possiamo costruire come abbreviazione di

$$\dfrac{T \vdash \varphi \qquad \dfrac{\dfrac{\varphi \vdash \psi}{\vdash \varphi \to \psi}}{T \vdash \varphi \to \psi}}{T \vdash \psi}$$

Notiamo che siamo comunque rimasti nel linguaggio L in quanto non abbiamo mai usato c in questa dimostrazione.

Se invece $T \vdash \forall x_k.\varphi$ allora con una applicazione della regola di eliminazione del quantificatore universale si ottiene che $T \vdash \varphi\left[{}^{c}\!/_{x_k}\right]$ nel linguaggio L, e la stessa dimostrazione è quindi valida anche nel linguaggio più grande $L(c)$.

Per concludere notiamo che grazie alla regola definita sopra $T \vdash \forall x_i.\varphi$ se e solo se $T \vdash \neg\exists x_i.\neg\varphi$ in quanto abbiamo già dimostrato (4.1.1) che

$$\forall x_i.\varphi \vdash \neg\exists x_i.\neg\varphi \qquad \text{e} \qquad \neg\exists x_i.\neg\varphi \vdash \forall x_i.\varphi$$

ed è ovvio grazie alle regole di riduzione ad essurdo e di introduzione della negazione che $T \vdash \neg\exists x_i.\neg\varphi$ se e solo se $T, \exists x_i.\neg\varphi \vdash \bot$. □

Lemma 5.1.2

Date una L-teoria T, una L-formula φ ed una variabile libera $x_k \in \mathrm{vl}(\varphi)$ sia c un simbolo di costante tale che $c \notin L$. Se $x_k \notin \mathrm{vl}(T)$ allora $T \vdash \varphi$ se e solo se $T \vdash \varphi\left[{}^{c}\!/_{x_k}\right]$[1].

Esercizio 5.2 Dimostrare il lemma precedente.

Svolgimento. Dato che $x_k \notin \mathrm{vl}(T)$ possiamo dimostrare che

$$\frac{T \vdash \varphi}{T \vdash \forall x_k.\varphi}\ x_k \notin \mathrm{vl}(T)$$

e viceversa dato che $\varphi\left[{}^{x_k}\!/_{x_k}\right] = \varphi$ vale

$$\frac{T \vdash \forall x_k.\varphi}{T \vdash \varphi}$$

quindi per concludere basta notare che per il lemma delle costanti (5.1.1)$T \vdash \forall x_k.\varphi$ se e solo se $T \vdash \varphi\left[{}^{c}\!/_{x_k}\right]$ □

In realtà questo risultato si può estendere anche al caso di variabili che appartengono a $\mathrm{vl}(T)$ infatti data una qualunque L-struttura M con una valutazione v possiamo considerare la L_c-struttura M' che pone $c_{M'} = \{v\}\, x_k$ con la valutazione v' definita restringendo v sulle variabili eccetto x_k, in questo modo dove nel modello M possiamo sostituire un termine t alla variabile x_k nel modello M' possiamo invece cambiare l'interpretazione di c a $\{v\}\, t$; controllando i dettagli risulterebbe che effettivamente la sostituzione è legale se e soltanto se nell'interpretazione in M' non stiamo quantificando su c (non si può quantificare su una costante).

5.2 Teorie deduttivamente coerenti e complete

Definizione 5.2.1: *Espansione e riduzione di linguaggi*

Dati due linguaggi L ed L' se $L \subseteq L'$ diciamo che L' è un'*espansione di* L e che L è un *ridotto di* L'.

Definizione 5.2.2: *Espansione e riduzione di strutture*

Dati due linguaggi L ed L' ed una L'-struttura M diciamo *ridotto di* M la L-struttura $M \restriction L$ con lo stesso dominio di M e dove per ogni simbolo di L l'interpretazione in $M \restriction L$ è la stessa che in M. Analogamente ai linguaggi possiamo dire che M è un'*espansione di* $M \restriction L$.

Esempio 5.2.1 Se scegliamo un anello, ad esempio $(\mathbb{Z}, +, \cdot, 0, 1)$, il gruppo abeliano 'sottostante' è il ridotto di $(\mathbb{Z}, +, \cdot, 0, 1)$ al linguaggio dei gruppi abeliani.

Adesso che abbiamo introdotto questi concetti dimostriamo una proposizione, che effettivamente può essere vista come un corollario al teorema di compattezza sintattica (4.0.3), la quale sarà utile per mostrare che le nuove teorie non sono incoerenti nei passi 2. e 3. dell'elenco di prima.

Proposizione 5.2.3: *Corollario al teorema di compattezza sintattica*

Sia T un L-teoria, φ una L-formula e C un insieme di simboli di costante tale che $C \cap L = \varnothing$. Indicando $L(C) = L \cup C$ vale che $T \vdash \varphi$ in L se e solo se $T \vdash \varphi$ in $L(C)$.

Dimostrazione. È ovvio che se $T \vdash \varphi$ in L allora $T \vdash \varphi$ in $L(C)$ in quanto una dimostrazione in L è valida anche in $L(C)$, quindi rimane da mostrare solo l'implicazione inversa.

[1] come prima notiamo che $T \vdash \varphi$ è nel linguaggio L mentre $T \vdash \varphi\left[{}^{c}\!/_{x_k}\right]$ è nel linguaggio $L(c)$

Sia quindi φ una L-formula tale che $T \vdash \varphi$ in $L(C)$, per compattezza sintattica esiste una sottoteoria finita T' tale che $T' \vdash \varphi$ in $L(C)$.

Inoltre una qualunque dimostrazione in $L(C)$ per finitezza può menzionare solo un numero finito di costanti.

Sia P una dimostrazione di $T' \vdash \varphi$ in $L(C)$ e $c_1, \dots, c_n$ le costanti in C menzionate nella dimostrazione, ovvero $T' \vdash \varphi$ in $L(c_1, \dots, c_n)$; procediamo per induzione su n:

- per il passo base se $n = 0$ allora $T' \vdash \varphi$ in L;
- per il passo induttivo se ogni L-formula dimostrabile da T' nel linguaggio $L(c_1, \dots, c_n)$ è dimostrabile da T' in L sia φ tale che $T' \vdash \varphi$ nel linguaggio $L(c_1, \dots, c_{n+1})$, per finitezza di T' esiste x_k tale che $x_k \notin \mathrm{vl}(T', \varphi)$ e scegliendo tale x_k vale $\varphi\left[c_{n+1}/x_k\right] \equiv \varphi$ ovvero $T_0 \vdash \left[c_{n+1}/x_k\right]$ nel linguaggio $L(c_1, \dots, c_{n+1})$, quindi per il lemma delle costanti (5.1.1) vale $T_0 \vdash \forall x_k.\varphi$ nel linguaggio $L(c_1, \dots, c_n)$, quindi per ipotesi induttiva $T_0 \vdash \forall x_k.\varphi$ nel linguaggio L ovvero per la regola di eliminazione del quantificatore universale $T_0 \vdash \varphi$ nel linguaggio L.

□

Corollario 5.2.3.1

Nel caso della proposizione precedente vale che $T \nvdash \bot$ in L se e solo se $T \nvdash \bot$ in $L(C)$.

Definizione 5.2.4: *Chiusura deduttiva di una teoria*

Data una L-teoria T definiamo la sua *chiusura deduttiva* come la L-teoria $\{\varphi \mid T \vdash \varphi\}$.[2]

Definizione 5.2.5: *Teoria deduttivamente coerente*

Diciamo che una teoria T è *deduttivamente*[3]*coerente* se $T \nvdash \bot$.

Definizione 5.2.6: *Teoria deduttivamente completa*

Diciamo che una L-teoria deduttivamente coerente T è *deduttivamente*[3] *completa* se per ogni L-formula φ vale $T \vdash \varphi$ oppure $T \vdash \neg\varphi$.

Lemma 5.2.7

Se T è deduttivamente coerente allora almeno[4]una tra $T \cup \{\varphi\}$ e $T \cup \{\neg\varphi\}$ è deduttivamente coerente.

Dimostrazione. Se per assurdo sia $T \cup \{\varphi\}$ che $T \cup \{\neg\varphi\}$ non fossero deduttivamente coerenti allora $T, \varphi \vdash \bot$ e $T, \neg\varphi \vdash \bot$ ma $\vdash \varphi \vee \neg\varphi$, quindi per la regola di eliminazione della disgiunzione seguirebbe che $T \vdash \bot$ che è assurdo perché per ipotesi T è deduttivamente coerente. □

Lemma 5.2.8: *Caratterizzazione delle teorie deduttivamente complete*

Data una L-teoria[5]T deduttivamente coerente le seguenti sono equivalenti:

1. la chiusura deduttiva di T è massimale per inclusione fra le chiusure deduttive di L-teorie deduttivamente coerenti.
2. date due qualunque L-formule φ e ψ se $T \vdash \varphi \vee \psi$ allora $T \vdash \varphi$ o $T \vdash \psi$.
3. T è deduttivamente completa.

[2] Spesso in questo capitolo considereremo una teoria come un insieme di enunciati invece che di formule generiche, in tale caso per mantenere questa proprietà considereremo la sua chiusura come l'insieme di tutti gli enunciati dimostrati da essa invece che di tutte le formule anche non chiuse.

[3] Nella lezione ha detto solo teoria coerente e completa, ma noi avevamo già definito una teoria coerente (2.3.4) ed una teoria completa (2.3.5) in precedenza, quindi riprendendolo dalle note dell'anno dopo ci ho aggiunto 'deduttivamente'

[4] Possono essere entrambe coerenti, ad esempio nella teoria dei gruppi con $\varphi \doteq$ 'esiste un elemento di ordine esattamente 2' entrambe sono coerenti in quanto $\mathbb{Z}/2\mathbb{Z}$ è un modello di $T \cup \{\varphi\}$ e $\mathbb{Z}/3\mathbb{Z}$ è un modello di $T \cup \{\neg\varphi\}$

Esercizio 5.3 Dimostrare il lemma precedente.

Svolgimento. Senza perdita di generalità supponiamo che T sia deduttivamente chiusa.

1.→3. Se T è massimale per inclusione fra le teorie deduttivamente coerenti supponiamo per assurdo che esista una L-formula φ tale che $T \nvdash \varphi$ e $T \nvdash \neg\varphi$, per il lemma precedente (5.2.7) almeno una fra $T \cup \{\varphi\}$ e $T \cup \{\neg\varphi\}$ è deduttivamente coerente, ma questo contraddirrebbe l'ipotesi perché costituirebbe una teoria strettamente più grande di T.

3.→1. Se T è deduttivamente completa supponiamo per assurdo che esista una teoria coerente T' tale che $T \subsetneq T'$, quindi esisterebbe una L-formula $\varphi \in T' \setminus T$ e per completezza $T \vdash \varphi$ oppure $T \vdash \neg\varphi$, chiaramente $T \nvdash \varphi$ in quanto abbiamo supposto che sia deduttivamente chiusa e che $\varphi \notin T$ ma questo è assurdo perché segue che $T' \vdash \neg\varphi \wedge \varphi$ cioè $T' \vdash \bot$ e per costruzione T' doveva essere deduttivamente coerente.

3.→ 2. Se T è deduttivamente completa supponiamo per assurdo che esistano due L-formule φ e ψ tali che $T \vdash \varphi \vee \psi$, $T \nvdash \varphi$ e $T \nvdash \psi$, allora per completezza $T \vdash \neg\varphi$ e $T \vdash \neg\psi$ ma da questo si deduce che $T \vdash \neg(\varphi \vee \psi)$ infatti

$$\dfrac{\dfrac{}{\varphi \vee \psi \vdash \varphi \vee \psi} \qquad \dfrac{\dfrac{T \vdash \neg\varphi \quad \dfrac{}{\varphi \vdash \varphi}}{T, \varphi \vdash \bot} \qquad \dfrac{T \vdash \neg\psi \quad \dfrac{}{\psi \vdash \psi}}{T, \psi \vdash \bot}}{T, \varphi \vee \psi \vdash \bot}}{T \vdash \neg(\varphi \vee \psi)}$$

ovvero $T \vdash \bot$ contraddicendo l'ipotesi di coerenza deduttiva di T.

2.→3. Se date due qualunque L-formule φ e ψ se $T \vdash \varphi \vee \psi$ allora $T \vdash \varphi$ o $T \vdash \psi$ allora in particolare data una qualunque L-formula φ (dato che $\vdash \varphi \vee \neg\varphi$) per indebolimento $T \vdash \varphi \vee \neg\varphi$, ovvero per ogni L-formula φ per costruzione $T \vdash \varphi$ oppure $T \vdash \neg\varphi$ cioè per definizione T è deduttivamente completa.

□

Esempio 5.2.2 Se M è una L-struttura la teoria completa di M (2.3.6) è deduttivamente completa, infatti in una L-struttura una qualunque L-formula o è vera o è falsa, quindi necessariamente data una qualunque L-formula vale $\mathrm{Th}(M) \vdash \varphi$ oppure $\mathrm{Th}(M) \vdash \neg\varphi$ inoltre essendo M modello di $\mathrm{Th}(M)$ vale $\mathrm{Th}(M) \nvdash \bot$ da cui per la contronominale del teorema di correttezza (4.2.1) $\mathrm{Th}(M) \nvdash \bot$ ovvero $\mathrm{Th}(M)$ è deduttivamente coerente.
Chiaramente questo esempio non è molto utile, in quanto la teoria completa di un modello è un oggetto abbastanza astratto, ma vedremo come semplice corollario del teorema di completezza che questo descrive tutte le teorie deduttivamente complete, cioè tutte le teorie deduttivamente complete possono essere descritte come teorie complete di un qualche modello.

Esempio 5.2.3 La teoria degli ordini lineari non è deduttivamente completa, in quanto non decide se esiste un minimo ($\exists x \forall y . x \leq y$).

Esempio 5.2.4 Fissata una caratteristica la teoria dei campi algebricamente chiusi di tale caratteristica è deduttivamente completa.

Esercizio 5.4 Sia $\mathbb{F}_{7^{12}}$-VS la teoria degli spazi vettoriali non banali su $\mathbb{F}_{7^{12}}$ in $L_{ab} \cup \{\cdot\}$ (con $\cdot$ moltiplicazione per scalare), questa non è deduttivamente completa completa.

[5] Il lemma vale anche se ci restringiamo a teorie composte solo di enunciati (e le rispettive chiusure deduttive)

Dimostrazione. Dato che sia $\mathbb{F}_{7^{12}}$ che $\mathbb{F}_{7^{12}}^2$ sono spazi vettoriali su $\mathbb{F}_{7^{12}}$ per il teorema di correttezza né la formula che dice che esistono $7^{12}+1$ elementi diversi né la sua negazione possono essere dimostrate dalla teoria. □

Lemma 5.2.9: *di Lindenbaum*

Data una L-teoria deduttivamente coerente T esiste una L-teoria deduttivamente completa T' tale che $T \subseteq T'$.

Dimostrazione. Dimostriamo che valgono le ipotesi del lemma di Zorn per le L-teorie coerenti contenenti T con l'inclusione.

Anzitutto l'insieme delle L-formule esiste per separazione nelle stringhe di simboli in L, quindi l'insieme delle L-teorie coerenti esiste per separazione nelle parti dell'insieme delle L-formule; questo insieme è non vuoto perché per ipotesi T è deduttivamente coerente ed parzialmente ordinato dall'inclusione, quindi rimane da vedere che ogni catena ammette un maggiorante, per fare questo vediamo che l'unione arbitraria di L-teorie coerenti inscatolate è a sua volta una L-teoria coerente.

Data una I-sequenza $(T_i)_{i\in I}$ di L-teorie coerenti inscatolate indichiamo $T = \bigcup_{i\in I} T_i$ se per assurdo questa non fosse coerente allora $T \vdash \bot$ e per compattezza sintattica (4.0.3) esisterebbe una sottoteoria $T' \subset T$ finita tale che $T' \vdash \bot$ ma essendo T' finita esiste $i \in I$ tale che $T' \subset T_i$ e questo è assurdo perché T_i è coerente.

In particolare le ipotesi del lemma di Zorn valgono anche nel sottoinsieme non vuoto delle L-teorie coerenti che contengono T, quindi anche questo ammette elementi massimali, ovvero esiste una L-teoria coerente $T' \supseteq T$ massimale per inclusione, quindi per il lemma (5.2.8) T' è deduttivamente completa. □

5.3 Teorie di Henkin

Nota 5.3.1 Al livello di notazione data una L-formula φ in questo capitolo indicheremo questa come $\varphi(x_1,\dots,x_k)$ soltanto se $\mathrm{vl}(\varphi) \subseteq \{x_1,\dots,x_k\}$, in maniera più restrittiva rispetto a quello indicato nella nota precedente 2.2.1.

Definizione 5.3.1: *Teoria di Henkin*

Una L-teoria T si dice *di Henkin* se per ogni L-formula chiusa della forma $\exists x.\varphi(x)$ esiste una costante $c \in L$ tale che

$$T \vdash (\exists x.\varphi(x)) \to \varphi\left[{}^{c}/_{x}\right]$$

Esempio 5.3.2 La teoria dei campi algebricamente chiusi di caratteristica zero(o non avendo dimostrato che è la teoria di $(\mathbb{C},+,\cdot,-,0,1)$ diciamo $\mathrm{Th}(\mathbb{C},+,\cdot,-,0,1)$) non è di Henkin, infatti se ad esempio prendiamo la formula

$$\varphi(x) \doteq x = 1+1$$

non abbiamo una costante per il numero 2.

Lemma 5.3.2

Date una L-teoria deduttivamente coerente T, una L-formula φ ed una costante $c \notin L$; la $L(C)$-teoria

$$T \cup \{(\exists x.\varphi(x)) \to \varphi(c)\}$$

è anch'essa deduttivamente coerente.

Dimostrazione. Se per assurdo questa nuova teoria non fosse deduttivamente coerente ovvero se in $L(C)$

$$T, (\exists x.\varphi(x)) \to \varphi(c) \to \bot$$

per l'esercizio 4.3 varrebbe

$$T, \exists x.\varphi(x) \vdash \neg\varphi(c)$$

quindi per introduzione dell'implicazione possiamo applicare l'esercizio 4.4 istanziato con $\psi = \bot$ insieme al lemma delle costanti (5.1.1) ottenendo che:

$$T, \exists\, x.\varphi(x) \vdash \bot$$

e grazie all'esercizio successivo (4.5) da questo si ricava che $T \vdash \bot$ come $L(C)$-teoria. Scriviamo più esplicitamente questa dimostrazione, dove non è ovvio indichiamo che esercizio o lemma stiamo usando:

$$\dfrac{T, (\exists\, x.\varphi(x)) \to \varphi(c) \vdash \bot \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\neg\varphi(c) \vdash \varphi(c) \to \bot} \qquad \dfrac{T, (\exists\, x.\varphi(x)) \to \varphi(c) \vdash \bot}{T, \exists\, x.\varphi(x) \vdash \neg\varphi(c)}\ (4.3)}{T, \exists\, x.\varphi(x) \vdash \varphi(c) \to \bot}}{T, \exists\, x.\varphi(x) \vdash \forall\, x.\varphi(x) \to \bot}\ (5.1.1)}{T, \exists\, x.\varphi(x) \vdash \varphi(x) \to \bot}\ (4.4)^{6} \qquad \dfrac{}{\exists\, x.\varphi(x) \vdash \exists\, x.\varphi(x)}}{T \vdash \bot}\ (4.5)$$

Da questo segue per il corollario 5.2.3.1 l'assurdo che T non è deduttivamente coerente anche come L-teoria.

□

Un'altra dimostrazione. Se per assurdo questa nuova teoria non fosse deduttivamente coerente ovvero se in $L(C)$

$$T, (\exists\, x.\varphi(x)) \to \varphi(c) \vdash \bot$$

per l'esercizio 4.3 varrebbe

$$T, \exists\, x.\varphi(x) \vdash \neg\varphi(c)$$

nel linguaggio $L(C)$ quindi per il lemma delle costanti

$$T, \exists\, x.\varphi(x) \vdash \neg\forall\, x.\neg\varphi(x)$$

in L, ma $\exists\, x.\varphi(x) \vdash \neg\forall\, x.\neg\varphi(x)$ quindi

$$T, \exists\, x.\varphi(x) \vdash \bot$$

in L, e quindi anche in $L(C)$, da cui per la regola di eliminazione di $\bot$ segue che

$$T, \exists\, x.\varphi(x) \vdash \varphi(c)$$

ovvero per l'introduzione dell'implicazione

$$T \vdash (\exists\, x.\varphi(x)) \to \varphi(c)$$

quindi $T \vdash \bot$ in $L(C)$ ovvero $T \vdash \bot$ in L (5.2.3.1), ma questo è assurdo perché avevamo supposto T deduttivamente coerente. □

Proposizione 5.3.3

Data una L-teoria deduttivamente coerente T esistono un linguaggio $L' \supseteq L$ ed una L'-teoria di Henkin deduttivamente completa T' tali che $T \subseteq T'$.

Dimostrazione. Indichiamo $L_0 = L$ e $T_0 = T$; per ogni L-formula $\varphi(x)$ fissiamo un nuovo simbolo di costante c_φ ed indichiamo l'insieme di questi nuovi simboli come L_1.

Adesso definiamo la teoria

$$T_1 = T \cup \{(\exists\, x.\varphi(x)) \to \varphi(c_\varphi) \mid \varphi(x) \text{ è una } L_0\text{-formula}\}$$

se per assurdo $T_1 \vdash \bot$ allora esiste una dimostrazione P di $\bot$ a partire da T_1, questa dimostrazione menzionerà un numero finito di costanti, quindi possiamo usare il lemma precedente (5.3.2) mostrando

[6] Non mi torna, questa regola funziona solo se $x \notin \mathrm{vl}(T, \exists\, x.\varphi(x) \vdash \bot)$ ma non abbiamo alcuna ipotesi per la quale $x \notin \mathrm{vl}(T)$

per induzione l'assurdo che aggiungendo un numero finito di costanti la teoria rimane deduttivamente coerente.

Avendo espanso il linguaggio L_0 ad $L_0 \cup L_1$ avremo aggiunto delle formule quindi T_1 potrebbe non essere di Henkin nel nuovo linguaggio; per procedere definiamo ricorsivamente T_{n+1} da T_n come T_1 era definita da T_0 ottenendo una sequenza $(T_i)_{i\in\mathbb{N}}$ di teorie deduttivamente coerenti inscatolate, indichiamo poi $L' = \bigcup_{i\in\mathbb{N}} L_i$ l'unione dei linguaggi e $T_\omega = \bigcup_{i\in\mathbb{N}} T_i$ l'unione delle teorie; T_ω è per costruzione una L'-teoria ed per compattezza sintattica è deduttivamente coerente.

Per finitezza delle stringhe per ogni L'-formula φ esiste $i \in \mathbb{N}$ tale che φ è una L_i-formula, quindi per costruzione T_ω è di Henkin.

Per il lemma di Lindenbaum (5.2.9) esiste una L'-teoria deduttivamente completa T' tale che $T_\omega \subseteq T'$, e non avendo aggiunto altri simboli al linguaggio dato che T_ω è di Henkin allora anche T' è di Henkin. □

Osservazione 5.3.3 In generale se T è una L-teoria di Henkin e T' è una L-teoria tale che $T \subset T'$ allora anche T' è di Henkin.

Osservazione 5.3.4 Per come abbiamo costruito il linguaggio L' nella dimostrazione predecente aggiungendo numerabili volte al più $|L| + \aleph_0$ costanti (tante quante le L_i-formule), quindi vale che $|L'| \leq |L| + \aleph_0$.
Al livello pratico quando si parla della cardinalità di un linguaggio di solito ci si riferisce alla cardinalità delle formule invece che al numero di simboli, essendo le prime almeno numerabili con tale interpretazione possiamo dire che con questo procedimento la cardinalità del linguaggio rimane invariata.

5.4 Il teorema di completezza

La dimostrazione del teorema di completezza si baserà sul dimostrare l'esistenza di modelli per teorie complete di Henkin, separiamo questo in una proposizione e aggiungiamo al risultato delle informazioni in più sulla cardinalità e su come è composto questo modello; queste non servono per dimostrare il teorema di completezza ma sono utili in teoria dei modelli.

Proposizione 5.4.1

Data una L-teoria T deduttivamente completa di Henkin esiste un modello M di T di cardinalità $|M| \leq |L| + \aleph_0$ tale che per ogni $a \in M$ esiste un L-termine chiuso t tale che valutando t in M[7]si ottiene a (cioè $t^M = a$).

Dimostrazione. Iniziamo costruendo il dominio della struttura come un quoziente a partire dall'insieme degli L-termini chiusi.

Indichiamo con X l'insieme degli L-termini chiusi, essendo T di Henkin l'insieme X è non vuoto; definiamo una relazione di equivalenza su X ponendo che $t_1 \sim_T t_2$ quando $T \vdash t_1 = t_2$ (chiaramente ben definita).

Definiamo quindi il dominio della struttura come il quoziente $M = {}^{X}\!/_{\sim_T}$.

Adesso definiamo le interpretazioni dei simboli di funzione nella struttura.

Dato un simbolo di funzione n-ario $f \in L$ definiamo la sua interpretazione $f^M : M^n \to M$ ponendo

$$f^M([t_0]_T, \ldots, [t_{n-1}]_T) = [f(t_0, \ldots, t_{n-1})]_T$$

ovvero scegliamo un rappresentante per ognuna delle classi di equivalenza ed assegnamo come immagine la classe di f applicata a quei rappresentanti.

Mostriamo che questa è una buona definizione: usando la regola di introduzione dell'uguaglianza si ottiene che

$$T \vdash f(t_0, \ldots, t_{n-1}) = f(t_0, \ldots, t_{n-1})$$

[7]essendo t chiuso non abbiamo bisogno di inserire valutazioni delle variabili

e consideriamo la formula

$$\varphi(y_0, \dots, y_{n-1}) \doteq f(y_0, \dots, y_{n-1}) = f(t_0, \dots, t_{n-1})$$

che ha come variabili libere esattamente $\{y_0, \dots, y_{n-1}\}$ in quanto $t_0, \dots, t_{n-1}$ sono termini chiusi, ed analogamente t_i è sostituibile ad y_i in φ per ogni i, quindi per definizione di sostituzione

$$T \vdash \varphi\left[t_0/y_0, \dots, t_{n-1}/y_{n-1}\right]$$

dati $t'_0, \dots, t'_{n-1}$ altri rappresentanti delle stesse classi di equivalenza allora per definizione $T \vdash t_i = t'_i$ per ogni i, quindi per la regola di eliminazione dell'uguaglianza

$$T \vdash \varphi\left[t'_0/y_0, \dots, t'_{n-1}/y_{n-1}\right] \equiv f(t'_0, \dots, t'_{n-1}) = f(t_0, \dots, t_{n-1})$$

ovvero $f(t'_0, \dots, t'_{n-1})$ e $f(t_0, \dots, t_{n-1})$ appartengono alla stessa classe di equivalenza cioè l'interpretazione di f è effettivamente ben definita.

Esercizio 5.5 Mostrare che per ogni L-termine chiuso t vale $t^M = [t]_T$ per induzione strutturale sui termini.

Svolgimento.

- se $t \equiv c()$ è una costante allora per costruzione $t^M = [c()]_T = [t]_T$;
- essendo t chiuso non può essere una variabile;
- altrimenti $t \equiv f(t_1, \dots, t_k)$ allora per costruzione

$$t^M = f^M([t_1]_T, \dots, [t_k]_T) = [f(t_1, \dots, t_k)]_T = [t]_T$$

□

Procediamo definendo le interpretazioni dei simboli di relazione nella struttura.
Dato un simbolo di relazione n-ario $R \in L$ definiamo la sua interpretazione nella struttura come

$$R^M = \{([t_0]_T, \dots, [t_{n-1}]_T) \mid T \vdash R(t_0, \dots, t_{n-1})\}$$

Esercizio 5.6 Mostrare che l'interpretazione delle relazioni è ben definita.

Svolgimento. Fissata una relazione n-aria R ed n elementi del dominio $[t_0]_T, \dots, [t_{n-1}]_T$ e per ognuno di essi due rappresentanti t_i, t'_i per introduzione dell'uguale

$$T \vdash R(t_0, \dots, t_{n-1}) = R(t_0, \dots, t_{n-1})$$

quindi come nel caso precedente possiamo definire la L-formula

$$\psi(y_0, \dots, y_{n-1}) \doteq R(y_0, \dots, y_{n-1}) = R(t_0, \dots, t_{n-1})$$

ricavando dalla regola di eliminazione dell'uguale che

$$T \vdash \psi(t'_0, \dots, t'_{n-1}) \equiv R(t'_0, \dots, t'_{n-1}) = R(t_0, \dots, t_{n-1})$$

ovvero per ogni simbolo di relazione $R \in L$ l'insieme R^M è ben definito. □

Adesso che abbiamo completato la costruzione della struttura notiamo che per costruzione ogni elemento $a \in M$ è della forma t^M ed i termini chiusi sono $|L| + \aleph_0$ quindi $|M| \leq |L| + \aleph_0$; rimane da verificare soltanto che $M \vDash T$ ovvero che per ogni $\varphi \in T$ vale $M \vDash \varphi$.

Verifichiamo che le formule vere in T e costruite con il sistema ridotto ($\bot, \to, \exists, =, \neg$[8]) sono vere in M.

[8] il sistema ridotto non ha la negazione ma sarà più semplice effettuare le verifiche degli altri punti includendo anche questa relazione

Dato che se $\varphi \in T$ allora $T \vdash \varphi$ ci basta mostrare che fissata un L-formula chiusa φ (che utilizza soltanto $\bot, \to, \exists, =, \neg$ come simboli logici) vale

$$T \vdash \varphi \qquad \iff [9] \qquad M \vDash \varphi \tag{5.1}$$

per induzione sul numero di simboli $\bot, \to, \exists, \neg$ che compaiono in φ[10].

Fissiamo una valutazione delle variabili v ma per semplificare la notazione omettiamo di scriverla (effettivamente la formula φ è chiusa ma se è della formula $\exists x.\psi(x)$ la sottoformula $\psi(x)$ potrebbe non essere chiusa, quando andremo a vedere quel caso ricominceremo a scrivere v nella notazione e sfrutteremo il fatto che è una teoria di Henkin per ricondurci al caso di $\psi(c_\varphi)$).

Iniziamo verificando 5.1 per φ atomica o negazione di atomica:

- con $\varphi \doteq \bot$ essendo T deduttivamente coerente sia $T \vdash \varphi$ che $M \vDash \varphi$ sono false.
- con $\varphi \doteq \neg\bot$ essendo T sia $T \vdash \varphi$ che $M \vDash \varphi$ sono vere.
- con $\varphi \doteq R(t_0, \dots, t_{n-1})$ per costruzione $T \vdash R(t_0, \dots, t_{n-1})$ se e solo se $([t_0]_T, \dots, [t_{n-1}]_T) \in R^M$ ovvero per la semantica di Tarski (2.1.2) se e solo se $M \vDash \varphi$.
- con $\varphi \doteq \neg R(t_0, \dots, t_{n-1})$ essendo T coerente necessariamente $T \nvdash \varphi$ e questo vale se e solo se $([t_0]_T, \dots, [t_{n-1}]_T) \notin R^M$ ovvero di nuovo per la semantica di Tarski se e solo se $M \vDash \neg\varphi$.
- con $\varphi \doteq t_1 = t_2$ se $T \vdash \varphi$ allora per costruzione $t_1 \sim_T t_2$, e quindi vale $M \vDash \varphi$, viceversa se $M \vDash \varphi$ sempre per costruzione $t_1 \sim_T t_2$ ovvero $T \vdash \varphi$.
- con $\varphi \doteq \neg t_1 = t_2$ se $T \vdash \varphi$ essendo $t_1 \nsim_T t_2$, e quindi vale $M \vDash \varphi$, viceversa se $M \vDash \varphi$ sempre per costruzione $t_1 \nsim_T t_2$ ovvero $T \vdash \varphi$.

Per iniziare il caso induttivo vediamo che la 5.1 è vera per

$$\varphi \doteq \psi_1 \to \psi_2$$

supponendo che sia vera per ψ_1 e ψ_2.

Fissando $\psi_2 \doteq \bot$ questo è il caso della negazione. Se $T \vdash \psi_1 \to \bot$ allora per l'eliminazione dell'implicazione deve valere $T \nvdash \psi_1$ perché T è deduttivamente coerente, quindi per ipotesi induttiva $M \nvDash \psi_1$ quindi per la semantica di Tarski è vale $M \vDash \psi_1 \to \bot$. Inversamente se in $M \vDash \psi_1 \to \bot$ allora necessariamente $M \nvDash \psi_1$ (altrimenti $M \vDash \bot$) quindi per ipotesi induttiva $T \nvdash \psi_1$ ed essendo T completa $T \vdash \neg\psi_1$ cioè $T \vdash \psi_1 \to \bot$. Quindi proseguendo possiamo considerare verificato il caso di $\varphi \doteq \neg\psi$.

Invece con ψ_2 arbitraria vale $M \vDash \psi_1 \to \psi_2$ per la semantica di Tarski se e solo se $(M \vDash \psi_1) \implies (M \vDash \psi_2)$ e per ipotesi induttiva questo è vero se e solo se $(T \vdash \psi_1) \implies (T \vdash \psi_2)$.

Se $T \vdash \psi_1 \to \psi_2$ allora se $T \vdash \psi_1$ applicando la regola di eliminazione dell'implicazione $T \vdash \psi_2$ ovvero vale $(T \vdash \psi_1) \implies (T \vdash \psi_2)$.

Mostriamo invece l'implicazione inversa ovvero che se $(T \vdash \psi_1) \implies (T \vdash \psi_2)$ allora $T \vdash \psi_1 \to \psi_2$ separando in due casi:

- se $T \nvdash \psi_1$ allora per completezza deduttiva $T \vdash \psi_1 \to \bot$ da cui

$$\dfrac{\dfrac{\dfrac{T \vdash \psi_1 \to \bot}{T, \psi_1 \vdash \psi_1 \to \bot} \quad \dfrac{}{\psi_1 \vdash \psi_1}}{T, \psi_1 \vdash \bot}}{\dfrac{T, \psi_1 \vdash \psi_2}{T \vdash \psi_1 \to \psi_2}}$$

[9] in realtà questo è equivalente alla sola implicazione $T \vdash \varphi \to M \vDash \varphi$ infatti se $M \vDash \varphi$ allora per la semantica di Tarski $M \nvDash \neg\varphi$ e da questo per la contronominale segue che $T \nvdash \neg\varphi$ e quindi per completezza deduttiva $T \vdash \varphi$; inoltre l'implicazione da sinistra a destra è effettivamente l'unica che ci serve per mostrare che $\varphi \in T \implies M \vDash \varphi$ però l'inversa sarà utile nei passi induttivi della dimostrazione

[10] non usiamo l'induzione sulla lunghezza di φ perché ad un certo punto vorremo rimpiazzare una parte di φ con una sottoformula diversa o potenzialmente più lunga, che però non contiene quei simboli

- altrimenti $T \vdash \psi_1$, quindi per ipotesi vale anche $T \vdash \psi_2$ se per assurdo $T \nvdash \psi_1 \to \psi_2$ allora per completezza deduttiva $T \vdash (\psi_1 \to \psi_2) \to \bot$ ovvero applicando la regola di eliminazione dell'implicazione $T, \psi_1 \to \psi_2 \vdash \bot$ quindi per l'esercizio (4.3) $T, \varphi \vdash \neg\psi$ ma questo è assurdo perché T è deduttivamente coerente e $T \vdash \varphi$, da cui anche T, φ deve essere deduttivamente coerente.

Rimane da verificare la 5.1 per formule della forma

$$\varphi \doteq \exists\, x.\psi(x)$$

dove essendo T di Henkin esiste una costante c tale che $T \vdash (\exists\, x.\psi(x)) \to \psi(c)$ e dove per ipotesi induttiva la 5.1 vale per $\psi(c)$.

Se $T \vdash \exists\, x.\psi(x)$ allora per la regola di eliminazione dell'implicazione $T \vdash \psi(c)$ e per ipotesi induttiva $M \vDash \{v\}\, \psi\, [{}^{c}\!/_{x}]$ quindi per il lemma 2.2.3

$$M \vDash \left\{ v \left[\{v\}_M \, {}^{c}\!/_{x} \right] \right\} \psi$$

ma allora per la semantica di Tarski $\vDash \{v\} \exists\, x.\psi(x)$.

Inversamente se $M \vDash \{v\} \exists\, x.\psi(x)$ allora per la semantica di Tarski esiste un elemento del dominio $a \in M$ tale che

$$M \vDash \{v\, [{}^{a}\!/_{x}]\}\, \psi$$

e per costruzione del modello esiste un L-termine chiuso t tale che $a = \{v\}_M\, t = [t]_T$, quindi per lo stesso lemma di prima (2.2.3)

$$M \vDash \{v\}\, \psi \left[{}^{t}\!/_{x} \right]$$

(essendo t chiuso è sostituibile per x, quindi effettivamente tale sostituzione è ben definita) quindi per ipotesi induttiva $T \vdash \psi(t)$ da cui si conclude con la regola di introduzione dell'esistenziale che $T \vdash \exists\, x.\psi(x)$. □

Teorema 5.4.2: *di completezza*

Ogni L-teoria T deduttivamente coerente ammette un modello M ovvero per ogni L-teoria T e per ogni L-formula φ

$$T \vDash \varphi \qquad \Longrightarrow \qquad T \vdash \varphi \tag{5.2}$$

inoltre il modello M si può scegliere con $|M| \leq |L| + \aleph_0$.

Dimostrazione. Iniziamo dal dimostrare che dire che per ogni L-teoria T vale $T \vDash \bot \implies T \vdash \bot$ è equivalente a dire che per ogni L-teoria T e per ogni L-formula φ vale $T \vDash \varphi \implies T \vdash \varphi$.

Chiaramente la formulazione con $\bot$ è un caso particolare dell'altra formulazione, quindi basta dimostrare che dalla prima segue la seconda.

Fissate T e φ per definizione $T \vDash \varphi$ se e solo se ogni modello di T è un modello di φ, e questo vale per la semantica di Tarski se e solo se $T, \neg\varphi$ non ha modelli, ovvero se e solo se $T, \neg\varphi \vDash \bot$.

Se supponiamo che per ogni L-teoria T vale $T \vDash \bot \implies T \vdash \bot$ allora in particolare $T, \neg\varphi \vDash \bot \implies T, \neg\varphi \vdash \bot$ e per la regola di riduzione all'assurdo se $T, \neg\varphi \vdash \bot$ allora $T \vdash \varphi$.

Quindi abbiamo dimostrato che per ogni L-teoria T e per ogni L-formula φ vale la tesi (5.2) se e solo se per ogni teoria T vale $T \nvdash \bot \implies T \nvDash \bot$ cioè se e solo se tutte le L-teorie deduttivamente coerenti ($T \nvdash \bot$) ammettono modelli ($T \nvDash \bot$); per concludere quindi rimane da costruire un modello di cardinalità minore o uguale ad $|L| + \aleph_0$ per ogni teoria deduttivamente coerente.

Se T è deduttivamente coerente per la proposizione 5.3.3 esiste un linguaggio L' di cardinalità $|L'| \leq |L| + \aleph_0$ ed esiste una L'-teoria T' deduttivamente completa di Henkin tali che $T \subseteq T'$, quindi per la proposizione 5.4.1 la teoria T' ammette un modello M di cardinalità

$$|M| \leq |L'| + \aleph_0 = |L| + \aleph_0$$

ed essendo $T \subseteq T'$ per definizione M è anche un modello di T come L'-teoria, quindi il ridotto di M ad L è un modello della L-teoria T, ovvero ogni teoria deduttivamente coerente ammette modelli. □

Corollario 5.4.2.1: *Teorema di Compattezza*

Una teoria ammette un modello se e solo se tutte le sue sottoteorie finite ammettono un modello.

Dimostrazione. Fissata la L-teoria T per compattezza sintattica (4.0.3) $T \vdash \bot$ se e solo se esiste una sottoteoria finita $T' \subseteq T$ tale che $T' \vdash \bot$ e per i teoremi di correttezza (4.2.1) e completezza questo vale se e solo se esiste una sottoteoria finita $T' \subseteq T$ tale che $T' \vDash \bot$, abbiamo quindi dimostrato la contronominale della tesi. □

Corollario 5.4.2.2

Data una L-teoria T questa è deduttivamente completa se e solo se esiste una L-struttura M tale che, a meno di chiusura deduttiva, vale $T = \mathrm{Th}(M)$.

Dimostrazione. Chiaramente se esiste una L-struttura M tale che $T = \mathrm{Th}(M)$ allora necessariamente T è deduttivamente completa in quanto avendo un modello è necessariamente deduttivamente coerente per il teorema di correttezza (4.2.1) e per ogni L-enunciato φ vale o $M \vDash \varphi$ o $M \vDash \neg\varphi$, quindi usando il teorema di completezza (5.4.2) $T \vdash \varphi$ o $T \vdash \neg\varphi$.

Invece se T è deduttivamente completa allora per definizione è deduttivamente coerente, quindi per la contronominale del teorema di completezza $T \nvdash \bot$ ovvero è coerente.

Fissato un qualunque modello M di T necessariamente vale $T \subseteq \mathrm{Th}(M)$ e data una qualunque L-formula φ la teoria T decide φ per completezza deduttiva, cioé $T \vDash \varphi$ o $T \vDash \neg\varphi$, quindi $\mathrm{Th}(M) \subseteq T$. □

5.5 Generalizzazioni

Abbiamo visto fino ad ora un teorema di completezza ed uno di correttezza, in particolare abbiamo visto questi risultati per la logica del primo ordine con un singolo sort[11] e con l'uguaglianza rispetto al sistema di deduzione naturale, alla classe delle strutture del primo ordine non vuote ed alla semantica di Tarski.

In generale si possono modificare queste specifiche per definire altri tipi di logiche, sia più restrittive (come abbiamo visto restringendo il sistema di deduzione naturale) che meno restrittive.

Esercizio 5.7 Costruire una variante del sistema di deduzione ridotto che usa solo $\wedge, \neg, \bot, \exists, =$ e verificare che è corretto e completo.
(Suggerimento:guardare cosa serve per fare completezza e correttezza e fare reverse engineering per capire quali regole servono)

Chiaramente è irragionevole aspettarsi che valgano sempre gli stessi risultati, però ci sono una grande quantità di risultati analoghi, di invarianti etc...

Una delle tante generalizzazioni della logica del primo ordine è quella *del secondo ordine* in cui le strutture sono le stesse che al primo ordine ma in più è possibile quantificare su sottoinsiemi delle potenze del dominio, ovvero di quantificare su relazioni.

Esempio 5.5.1 La logica del secondo ordine non è compatta, ad esempio consideriamo l'aritmetica di Peano al secondo ordine, quindi con il linguaggio $L = \{s, 0, +, \cdot\}$ e la teoria del secondo ordine PA_2, che invece di avere infiniti assiomi per l'induzione usa la classica formulazione che dice 'per ogni formula ...', che è una formulazione valida al secondo ordine(non lo è al primo ordine).
Se espandiamo il linguaggio ad $L(c)$ ed aggiungiamo alla teoria infinite formule per cui c è diversa da ogni naturale ($s^n(0) \neq c$) questa teoria più grande è finitamente soddifacibile, ovvero ogni suo sottoinsieme finito ha un modello, pur non essendo soddifacibile: infatti ogni modello di PA_2 è isomorfo al modello standard $\mathbb{N}$, che non è un modello della teoria espansa in quanto per costruzione una qualunque valutazione di c dovrebbe essere un elemento non-standard in $\mathbb{N}$.

[11] nel senso che l'universo è una collezione omogenea di oggetti, invece di avere cose di 'tipi' diversi

Esercizio 5.8 Data una L-struttura finita M con L finito mostrare che esiste un L-enunciato φ tale che $N \vDash \varphi$ se e solo se $N \cong M$.
E se L è infinito?

Capitolo 6

I teoremi di Löwenheim-Skolem

Per concludere questa parte introduciamo gli emdedding, le sottostrutture ed i diagrammi, per poi dimostrare i teoremi di Löwenheim-Skolem e vedere la relazione tra categoricità e completezza di teorie che segue da questi teoremi.

6.1 Equivalenza elementare

Definizione 6.1.1: *Equivalenza elementare*

Due L-strutture M ed N si dicono elementarmente equivalenti ($M \equiv N$) se hanno la stessa teoria completa ($\mathrm{Th}(M) = \mathrm{Th}(N)$).

In generale è difficile mostrare che due strutture sono elementarmente equivalenti, dovremmo dire che sono modelli di una stessa teoria e che tale teoria è completa; di solito è invece molto più facile mostrare che due strutture non sono elementarmente equivalenti, infatti basta esporre una formula che è vera in una struttura e falsa nell'altra.

Esercizio 6.1 Trovare un L_{AB}-enunciato che distingua ognuna a due a due le seguenti strutture non elementarmente equivalenti:

$$\mathbb{Q} \qquad \mathbb{Z} \qquad \mathbb{Z}^2 \qquad \mathbb{R}/\mathbb{Z} \qquad Z_{(3)} \left(= \left\{ \frac{m}{n} \;\middle|\; (m,n) = 1 \wedge 3 \nmid n \right\}\right)$$
$$\bigoplus_{i \in \mathbb{N}} \mathbb{Z}/3\mathbb{Z} \qquad \mathbb{Z}(3^\infty) \left(= \left\{ z \in \mathbb{C} \;\middle|\; \exists\, n \in \mathbb{N}. z^{3^n} = 1 \right\}\right)$$

Svolgimento. Vediamo che $\mathbb{Q}$ non è elementarmente equivalente a $\mathbb{Z}, \mathbb{Z}^2, \mathbb{Z}_{(3)}, \bigoplus_{i \in \mathbb{N}} \mathbb{Z}/3\mathbb{Z}$ perché è l'unico di questi che soddisfa la formula

$$\forall\, x. \exists\, y. y + y + y + y + y + y = x$$

Dato che $\mathbb{R}/\mathbb{Z}$ ha elementi di ordine 2 è distinto da $\mathbb{Q}, \mathbb{Z}, \mathbb{Z}^2, Z_{(3)}, \bigoplus_{i \in \mathbb{N}} \mathbb{Z}/3\mathbb{Z}$ e $\mathbb{Z}(3^\infty)$ dalla formula

$$\exists\, x. x + x = 0 \wedge \neg x = 0$$

Analogamente la formula che dichiara l'esistenza di un elemento di ordine 9 distingue il gruppo di Prüfer ($\mathbb{Z}(3^\infty)$) da tutti gli altri gruppi (eccetto $\mathbb{R}/\mathbb{Z}$ che però abbiamo già visto non essere elementarmente equivalente al gruppo di Prüfer).

Per distinguere $\mathbb{Z}$ da $\mathbb{Z}^2$ vediamo che in $\mathbb{Z}$ o un numero è pari oppure il numero successivo è pari, in particolare $\mathbb{Z}$ soddisfa:

$$\exists\, x. \forall\, y. \exists\, w. x + y = w + w \vee y = w + w$$

infatti ponendo $x = 1$ se y è pari allora esiste w tale che $y = w + w$ altrimenti y è dispari ed in tale caso $x + y$ è pari quindi esiste w tale che $x + y = w + w$.

Invece questa formula non vale in $\mathbb{Z}^2$ infatti se x è una coppia di due elementi pari, due elementi dispari, oppure è una coppia della forma $(\text{dispari}, \text{pari})$ allora non esiste tale w se poniamo $y = (0, 1)$; altrimenti x è una coppia della forma $(\text{pari}, \text{dispari})$ ed in tale caso non esiste w se poniamo $y = (1, 0)$.

Per distinguere $\bigoplus_{i\in\mathbb{N}} \mathbb{Z}/3\mathbb{Z}$ dai rimanenti basta dire che tutti gli elementi non banali hanno ordine 3.

Rimane da distinguere $\mathbb{Z}$ e $\mathbb{Z}^2$ da $Z_{(3)}$... □

6.2 Insiemi definibili

Definizione 6.2.1: *Insieme definibile*

Data una L-formula $\varphi(x_0, \dots, x_{n-1})$ ed una L-struttura M definiamo l'insieme

$$\varphi(M) = \{(a_0, \dots, a_{n-1}) \in M^n \mid M \vDash \varphi(a_0, \dots, a_{n-1})\}$$

e diciamo che un qualche sottoinsieme $X \subseteq M^n$ è *definibile* (più precisamente definibile *su* $\varnothing$ o definibile *senza parametri*) se esiste una L-formula ψ tale che $X = \psi(M)$.

Esempio 6.2.1 Nel linguaggio dei gruppi abeliani nella struttura del gruppo $(\mathbb{R}, +)$ la formula $\varphi(x_0, x_1, x_2) \doteq x_0 = x_1 + x_2$ definisce il grafico della funzione binaria $+$.

Osservazione 6.2.2 In $(\mathbb{R}, +, \leq)$ gruppo abeliano ordinato la formula $\varphi(x_0) \doteq x_0 = x_0$ definisce tutto il dominio $\mathbb{R}$, però "$x_0 = x_0$" può anche essere interpretata come una funzione in più variabili

$$\varphi(x_0, x_1) \doteq x_0 = x_0$$

e quindi definire anche l'insieme $\mathbb{R}^2$; nella definizione di insieme definibile abbiamo fatto un po' un abuso di notazione infatti l'insieme definibile in realtà non dipende solo da φ ma anche da quali e quante variabili stiamo mappando; anche per questo è utile la restrizione che abbiamo messo con la nota 5.3.1 per fare si che la formula nella definizione sia chiusa.

Osservazione 6.2.3 In $(\mathbb{R}, +, \leq)$ nel linguaggio dei gruppi abeliani ordinati non tutti gli insiemi saranno definiti, infatti il linguaggio è finito, quindi le L_{OAB}-formule sono numerabili ma i sottoinsiemi di $\mathbb{R}$ sono $2^{2^{\aleph_0}}$.

Definizione 6.2.2: *Insieme definibile con parametri*

Data una L-struttura M definiamo l'insieme ed un suo sottoinsieme $A \subseteq M$ definiamo il linguaggio

$$\mathfrak{L}(A) = L \cup \{c_a \mid a \in A\}$$

dove tutte le c_a sono simboli di costante e definiamo M_A la $\mathfrak{L}(A)$-struttura che ristretta ad L è esattamente M e tale che per ogni $a \in A$ la costante c_a si interpreta in M_A come $c_a^{M_A} = a$.
Detto questo un sottoinsieme $X \subseteq M^n$ si dice *A-definibile* (o definibile *a parametri in* A) se è definibile in M_A.

Osservazione 6.2.4 Dato A i sottoinsiemi A-definibili formano un'algebra di Boole, dove $\wedge$ è l'intersezione, $\vee$ è l'unione e $\neg$ è il complementare.

6.3 Sottostrutture ed embedding

Definizione 6.3.1: *Sottostruttura*

Date due L-strutture M ed N diciamo che M è *sottostruttura* di N (o che Nè un'*estensione* di M) se:

- il dominio di M è contenuto nel dominio di N
- per ogni simbolo di funzione $f \in L$ vale $f^N(M^{ar(f)}) = f^M(M^{ar(f)})$
- per ogni simbolo di relazione $r \in L$ vale $r^N \cap M^{ar(r)} = r^M$

e questo si indica con il contenimento $M \subseteq N$.

Osservazione 6.3.1 Data una L-struttura M ed un sottoinsieme A del dominio di M se A è chiuso per i simboli di funzione esiste un'unica L-struttura con dominio A che è sottostruttura di M, infatti l'interpretazione di ogni simbolo di funzione è univocamente determinata restringendo ad A l'interpretazione su M e l'interpretazione di ogni simbolo di relazione è univocamente determinata intersecando con A l'interpretazione su M.

Definizione 6.3.2: *Embedding di strutture*

Date due L-strutture M ed N e data una mappa $\iota : M \to N$ questa si dice *embedding* di M in N se per ogni L-formula atomica $\varphi(x_0, \dots, x_{n-1})$ e per ogni n-upla $(a_0, \dots, a_{n-1})$ di elementi del dominio di M

$$M \vDash \varphi(a_0, \dots, a_{n-1}) \qquad \iff \qquad N \vDash \varphi(\iota(a_0), \dots, \iota(a_{n-1}))$$

Dato un embedding $\iota : M \to N$ indichiamo come $\iota(M)$ la sottostruttura di N immagine di ι.

Nota 6.3.2 Un'altra maniera per definire un embedding può sembrare essere dicendo che l'immagine è una sottostruttura, pur essendo una conseguenza di essere un embedding questo non è la stessa cosa: la definizione che abbiamo fatto per gli embedding è strettamente più specifica in quanto descrive esattamente dove deve andare ogni elemento di M mentre non è il caso se richiediamo soltanto che l'immagine sia una qualche sottostruttura.

Esercizio 6.2 Ogni embedding di strutture è iniettivo.

Svolgimento. Dato che in ogni linguaggio del primo ordine esiste la formula atomica $\varphi(x_0, x_1) \doteq x_0 = x_1$, segue che $N \vDash \iota(a_0) = \iota(a_1)$ se e solo se $M \vDash a_0 = a_1$, ovvero ogni embedding di strutture è iniettivo. □

Esempio 6.3.3: *Morfismi di strutture* Nel linguaggio $L = \{\leq\}$ l'identità da $(\mathbb{N}^+, |)$ in $(\mathbb{N}^+, \leq)$ non è un embedding infatti se $n \mid m$ allora in particolare $n \leq m$ ma il contrario è falso; ma l'identità è un *morfismo* di strutture, come definito in precedenza (2.3.7), questo segue dall'osservazione (2.3.5) in quanto preserva tutte le formule atomiche.

Osservazione 6.3.4: *Isomorfismi ed embedding* Un morfismo bigettivo la cui inversa è un morfismo è per definizione un isomorfismo (2.3.8), in realtà possiamo definire un ismorfismo di strutture anche come *un embedding di strutture bigettivo* ottenendo esattamente gli stessi isomorfismi.
Infatti verifichiamo che tutti gli embedding bigettivi sono isomorfismi e tutti gli isomorfismi sono embedding.

- Per l'osservazione 2.3.5 tutti gli embedding sono morfismi in quanto per definizione presevano le formule atomiche (l'implicazione da sinistra a destra nella (6.3)), vediamo che l'inversa di un embedding bigettivo è anch'essa un embedding. Fissato $f : M \to N$ embedding bigettivo, data $\varphi(x_1, \dots, x_n)$ è una L-formula atomica e data la n-upla $(a_1, \dots, a_n) \in N^n$ per bigettività

esiste $(b_1, \dots, b_n) \in M^n$ tale che per ogni $i \in \{1, \dots, n\}$ vale $a_i = f(b_i)$, quindi $b_i = f^{-1}(a_i)$, allora per definizione di embedding:

$$N \vDash \varphi(a_1, \dots, a_n) \iff M \vDash \varphi(b_1, \dots, b_n) \equiv \varphi(f^{-1}(a_1), \dots, f^{-1}(a_n))$$

cioè $f^{-1} : N \to M$ è un embedding, quindi in particolare è un morfismo, ovvero f è un isomorfismo di strutture.

- Se $f : M \to N$ è un isomorfismo di strutture allora è un morfismo, quindi per l'osservazione 2.3.5 data $\varphi(x_1, \dots, x_n)$ una L-formula atomica e data la n-upla $(a_1, \dots, a_n) \in M^n$ vale

$$M \vDash \varphi(a_1, \dots, a_n) \to N \vDash \varphi(f(a_1), \dots, f(a_n))$$

ma essendo anche $f^{-1} : N \to M$ un morfismo di strutture applicando la composizione vale anche l'implicazione inversa

$$N \vDash \varphi(f(a_1), \dots, f(a_n)) \to M \vDash \varphi((f^{-1} \circ f)(a_1), \dots, (f^{-1} \circ f)(a_n)) \equiv \varphi(a_1, \dots, a_n)$$

ovvero f è un embedding.

Esercizio 6.3 Se $f : M \to N$ è un isomorfismo di L-strutture allora $f(\varphi(M)) = \varphi(f(M))$ ovvero data una L-formula $\varphi(x_1, \dots, x_n, y_1, y_m)$ e per ogni m-upla $(b_1, \dots, b_m) \in M^m$ vale che

$$f(\varphi(M, b_1, \dots, b_m)) = \varphi(N, f(b_1), \dots, f(b_m))$$[1]

Svolgimento. Procediamo per induzione strutturale sulle formule (considerando senza perdita di generalità le formule che usano solo i connettivi logici $\bot, \wedge, \neg, \exists$[2]) e per alleggerire la notazione indichiamo $\overline{a}$ una k-upla di $a_1, \dots, a_k$ di lunghezza adeguata dove serve.

Per il passo base se φ è una formula atomica allora per definizione di isomorfismo di strutture c'è una bigezione ovvia tale che

$$f(\varphi(M, \overline{b})) \doteq f\left(\left\{\overline{x} \in M^n \;\middle|\; M \vDash \varphi(\overline{x}, \overline{b})\right\}\right) = \left\{f(\overline{x}) \in N^n \;\middle|\; \overline{x} \in M^n, N \vDash \varphi(f(\overline{x}), f(\overline{b}))\right\} = \\ = \left\{\overline{x} \in N^n \;\middle|\; N \vDash \varphi(\overline{x}, f(\overline{b}))\right\} \doteq \varphi(N, f(\overline{b}))$$

Per il passo induttivo procediamo in maniera analoga:

- se $\varphi \doteq \neg\psi(\overline{x}, \overline{y})$ allora

$$f(\varphi(M, \overline{b})) \doteq f\left(\left\{\overline{x} \in M^n \;\middle|\; M \vDash \varphi(\overline{x}, \overline{b})\right\}\right) = \\ = f\left(\left\{\overline{x} \in M^n \;\middle|\; M \nvDash \varphi(\overline{x}, \overline{b})\right\}\right) = f\left(M^n \setminus \psi(M, \overline{b})\right)$$

quindi usando sia la bigettività di f che l'ipotesi induttiva su $\psi(M, \overline{b})$:

$$f(\varphi(M, \overline{b})) = f(M) \setminus f(\psi(M, \overline{b})) = N \setminus \psi(f(M), \overline{b}) = N \setminus \psi(N, \overline{b}) = \varphi(N, \overline{b})$$

- il procedimento è simile per $\varphi \doteq \psi \wedge \theta(\overline{x}, \overline{y})$ infatti

$$f(\varphi(M, \overline{b})) \doteq f\left(\left\{\overline{x} \in M^n \;\middle|\; M \vDash \psi \wedge \theta(\overline{x}, \overline{b})\right\}\right) = \\ = f\left(\left\{\overline{x} \in M^n \;\middle|\; M \vDash \psi(\overline{x}, \overline{b})\right\} \cap \left\{\overline{x} \in M^n \;\middle|\; M \vDash \psi(\overline{x}, \overline{b})\right\}\right) \doteq f(\psi(M, \overline{b}) \cap \theta(M, \overline{b}))$$

quindi di nuovo usando sia la bigettività di f che l'ipotesi induttiva su $\psi(M, \overline{b})$ e $\theta(M, \overline{b})$:

$$f(\varphi(M, \overline{b})) = f(\psi(M, \overline{b})) \cap f(\theta(M, \overline{b})) = \psi(N, \overline{b}) \cap \theta(N, \overline{b}) = \varphi(N, \overline{b})$$

[1] Ricordiamo che $\varphi(M, b_1, \dots, b_m)$ è il sottoinsieme di M^n definito dalla formula $\varphi(x_1, \dots, x_n, b_1, \dots, b_m)$ e applicarvi f vorrà dire applicarla elemento per elemento nelle n-uple che formano l'insieme

[2] non usiamo $\to$ perché in questo caso con $\wedge$ la dimostrazione diventa più facile

- per concludere se $\varphi \doteq (\exists z.\psi)(\overline{x},\overline{y})$ allora con lo stesso procedimento di prima

$$f(\varphi(M,\overline{b})) \doteq f\left(\left\{\overline{x}\in M^n \;\middle|\; M\vDash(\exists z.\psi)(\overline{x},\overline{b})\right\}\right) = f\left(\left\{\overline{x}\in M^n \;\middle|\; \exists a\in M.M\vDash\psi\left[{}^{a}\!/_{z}\right](\overline{x},\overline{b})\right\}\right) =$$
$$= f\left(\bigcup_{a\in M}\psi\left[{}^{a}\!/_{z}\right](M,\overline{b})\right) = \bigcap_{a\in M} f(\psi\left[{}^{a}\!/_{z}\right](M,\overline{b})) =$$
$$= \bigcap_{a\in M}\psi\left[{}^{f(a)}\!/_{z}\right](f(M),\overline{b}) = \bigcap_{a\in N}\psi\left[{}^{a}\!/_{z}\right](N,\overline{b}) = \varphi(N,\overline{b})$$

□

Esempio 6.3.5 Segue dall'esercizio precedente che un insieme definibile deve essere fissato (come insieme) da tutti gli automorfismi della struttura, dividere per 2 è un automorfismo della struttura $(\mathbb{R},+,0,-,\leq)$ e $\mathbb{Z}$ non è fissato da tale automorfismo, quindi $\mathbb{Z}$ non è un insieme definibile in $(\mathbb{R},+,0,-,\leq)$.

Definizione 6.3.3: *Embedding elementare*

Un embedding $\iota : M \to N$ di L-strutture si dice *elementare* se per ogni L-formula φ (non necessariamente atomica) vale

$$M\vDash\varphi(a_0,\dots,a_{n-1}) \qquad\Longleftrightarrow\qquad N\vDash\varphi(\iota(a_0),\dots,\iota(a_{n-1}))$$

Definizione 6.3.4: *Sottostruttura elementare*

Una sottostruttura M di N si dice *elementare* se l'inclusione di M in N è un embedding elementare (e quindi N si dice *estensione elementare* di M e si denota $M\preceq N$).

Esempio 6.3.6 Ad esempio $(\mathbb{Z},0,1,+,\cdot)$ è una sottostruttura di $(\mathbb{R},0,1,+,\cdot)$ ma non è una sottostruttura elementare, ad esempio in $\mathbb{R}$ è vera la formula

$$\exists x.\exists y.x\neq\pm1\wedge y\neq\pm1\wedge x\cdot y=3$$

ma questa è falsa in $\mathbb{Z}$ in quanto 3 è primo.
Invece $(\mathbb{N},0,1,+,-)$ non è una sottostruttura di $(\mathbb{R},0,1,+,-)$ in quanto il $-$ non è chiuso in $\mathbb{N}$, infatti ovviamente esiste $n\in\mathbb{N}$ tale che $i_{\mathbb{R}}(-)(n)=-n\notin\mathbb{N}$.
Nel linguaggio $L=\{\leq\}$ la struttura $(\mathbb{N},|)$ non è una sottostruttura di $(\mathbb{N},\leq)$ né viceversa, infatti nella prima 2 e 3 non sono confrontabili e nella seconda sì.

Esercizio 6.4 Date due L-strutture M ed N con $N\subseteq M$ le seguenti sono equivalenti:

1. $N\preceq M$
2. data una qualunque L-formula $\varphi(x_1,\dots,x_n)$ e data una qualunque n-upla $(a_1,\dots,a_n)\in N^n$ vale
$$N\vDash\varphi(a_1,\dots,a_n)\iff M\vDash\varphi(a_1,\dots,a_n)$$
3. $\mathrm{Th}(N)=\mathrm{Th}(M)$ se interpretate come $\mathfrak{L}(N)$-strutture
4. per ogni L-formula $\varphi(x_1,\dots,x_n)$ vale $\varphi(N)=\varphi(M)\cap N^n$.

In particolare se $M\preceq N$ allora $M\equiv N$.

Svolgimento. Chiaramente 1. $\iff$ 2. infatti indicando l'inclusione come $i:N\to M$ vale

$$\varphi(i(a_1),\dots,i(a_n))\equiv\varphi(a_1,\dots,a_n)$$

È anche ovvio che 3.$\to$1. infatti se $\mathrm{Th}(N)=\mathrm{Th}(M)$ come $\mathfrak{L}(N)$-strutture allora per definizione l'inclusione di N in M è un embedding elementare.

Dato che sia $\mathrm{Th}(N)$ che $\mathrm{Th}(M)$ sono deduttivamente complete e deduttivamente chiuse allora sono massimali per l'inclusione (5.2.8); quindi per ottenere che 1.→3. basta mostrare che $\mathrm{Th}(M) \subseteq \mathrm{Th}(N)$.

Data una qualunque $\mathfrak{L}(N)$-formula $\varphi(x_1, \dots, x_n)$ se $M \vDash \varphi(x_1, \dots, x_n)$ allora data una qualunque n-upla $(a_1, \dots, a_n) \in M^n$ vale $M \vDash \varphi(a_1, \dots, a_n)$ e per ipotesi $N^n \subseteq M^n$, quindi per ipotesi data una qualunque n-upla $(a_1, \dots, a_n) \in N^n$ vale $N \vDash \varphi(a_1, \dots, a_n)$ ovvero $N \vDash \varphi(x_1, \dots, x_n)$, quindi $\mathrm{Th}(M) \subseteq \mathrm{Th}(N)$.

rimane da verificare l'equivalenza del punto 4. ed il caso particolare in fondo... □

Esempio 6.3.7 Nell'esercizio precedente non vale l'altra implicazione per $N \equiv M$ perché le due strutture potrebbero essere isomorfe per qualche altro isomorfismo senza essere isomorfe per l'inclusione. Ad esempio se consideriamo $(2\mathbb{Z}, \leq)$ e $(\mathbb{Z}, \leq)$ come strutture nel linguaggio degli ordini lineari $2\mathbb{Z} \subseteq \mathbb{Z}$ (e sono anche isomorfe tramite $f : x \to 2x$), però

$$\exists\, x. 0 < x < 2$$

è una $\mathfrak{L}(2\mathbb{Z})$-formula falsa in $2\mathbb{Z}$ ma vera in $\mathbb{Z}$, quindi l'inclusione di $2\mathbb{Z}$ in $\mathbb{Z}$ è un embedding ma non è un embedding elementare, ovvero $2\mathbb{Z}$ non è una sottostruttura elementare di $\mathbb{Z}$.

Esempio 6.3.8 Se consideriamo una L-struttura M, un insieme di indici I ed un ultrafiltro U si $\mathscr{P}(I)$ allora

$$M \prec \prod_{i \in I} M/U$$

infatti se consideriamo la funzione che manda $a \in M$ in $[a, a, \dots]_U$ per il teorema di Łoś (3.1.1) è un embedding elementare.

6.3.1 Il criterio di Tarski-Vaught

Per mostrare che una sottostruttura è elementare è utile il criterio di Tarski-Vaught

Lemma 6.3.5: *Criterio di Taski-Vaught*

Data una L-struttura M ed un sottoinsieme N del suo dominio le seguenti sono equivalenti:

1. N è il dominio di una sottostruttura elementare di M
2. per ogni L-formula $\varphi(x, y_1, \dots, y_k)$ e per ogni k-upla $(b_1, \dots, b_k) \in N^k$ vale:

$$\exists\, a \in M. M \vDash \varphi(a, b_1, \dots, b_k) \implies \exists\, a \in N. M \vDash \varphi(a, b_1, \dots, b_k) \tag{6.1}$$

Dimostrazione. Se N è una sottostruttura elementare di M allora per la semantica di Tarski se esiste $a \in M$ tale che $M \vDash \varphi(a, b_1, \dots, b_k)$ allora $M \vDash \exists\, x. \varphi(x, b_1, \dots, b_k)$, quindi per definizione di embedding elementare $N \vDash \exists\, x. \varphi(x, b_1, \dots, b_k)$ ovvero esiste $a' \in N \subseteq M$ tale che $N \vDash \varphi(a', b_1, \dots, b_k)$, e di nuovo per definizione di embedding elementare $M \vDash \varphi(a', b_1, \dots, b_k)$.

Rimane da dimostrare l'implicazione inversa e partiamo mostrando che N è chiuso per i simboli di funzione.

Dato un qualunque simbolo di funzione k-ario $f \in L$ consideriamo la L-formula

$$\varphi(x, y_1, \dots, y_k) \doteq x = f(y_1, \dots, y_k)$$

per la semantica di Tarski fissata una qualunque k-upla $(b_1, \dots, b_k) \in N^k \subseteq M^k$ esiste un elemento $a \in M$ che soddisfa $\varphi(a, b_1, \dots, b_k)$, quindi per l'ipotesi 6.1 esiste $a' \in N$ che soddifa $\varphi(a', b_1, \dots, b_k)$ (ed in particolare per la definizione di struttura e per la semantica dell'uguale $M \vDash a = a'$ cioè $a \in N$) ovvero restringendo il dominio di f da M^k a N^k si ottiene una funzione da N^k in N, cioè N è chiuso per i simboli di funzione, quindi come osservato in precedenza (6.3.1) esiste un'unica sottostruttura di M con dominio N (da ora in avanti con N indichiamo tale struttura e non soltanto il suo dominio).

Per concludere grazie all'esercizio 6.4 basta dimostrare che l'inclusione di N in M è un embedding, ovvero che per ogni L-formula $\varphi(y_1, \dots, y_k)$ e per ogni $b_1, \dots, b_k \in N$ vale

$$N \vDash \varphi(b_1, \dots, b_k) \iff M \vDash \varphi(b_1, \dots, b_k)$$

per fare ciò procediamo per induzione strutturale su φ.

Il caso atomico è valido per definizione di sottostruttura ed i casi dei connettivi logici $\neg$ ed $\wedge$ (insieme completo di quantificatori) si riconduco immediatamente alle rispettive ipotesi induttive grazie alla semantica di Tarski quindi l'unico caso interessante è quello dell'*esiste*, ovvero il caso dove $\varphi(y_1, \dots, y_k) \doteq \exists\, x.\psi(x, y_1, \dots, y_k)$.

Fissati $b_1, \dots, b_k \in N$ per la semantica di Tarski vale $N \vDash \varphi(b_1, \dots, b_k)$ se e solo se

$$\exists\, a \in N. N \vDash \psi(a, b_1, \dots, b_k)$$

e grazie all'ipotesi induttiva questo è equivalente a

$$\exists\, a \in N. M \vDash \psi(a, b_1, \dots, b_k)$$

inoltre per l'ipotesi (6.1) questo è equivalente a

$$\exists\, a \in M. M \vDash \psi(a, b_1, \dots, b_k)$$

in quanto una delle due implicazioni è esplicitamente indicata in (6.1) mentre l'altra segue dalla definizione di sottostruttura, ed infine quest'ultimo è equivalente a

$$M \vDash \exists\, x.\psi(x, b_1, \dots, b_k)$$

per la semantica di Tarski. □

Esercizio 6.5 Se T ha la proprietà dell'eliminazione dei quantificatori allora date due L-strutture M ed N entrambe modello di T:

$$N \subseteq M \to N \preceq M$$

come strutture.

Svolgimento. Se N è una sottostruttura di M allora l'inclusione $i : N \to M$ è un embedding; vediamo che i è un embedding elementare mostrando che per ogni $\varphi(x_1, \dots, x_n)$ data una qualunque n-upla $(a_1, \dots, a_n) \in N^n$ vale

$$N \vDash \varphi(a_1, \dots, a_n) \iff M \vDash \varphi(a_1, \dots, a_n)$$

Vediamo che se φ è una formula senza quantificatori allora questo è vero per induzione strutturale, infatti:

- se φ è atomica allora la tesi è vera per ipotesi.
- se $\varphi(x_1, \dots, x_n) \doteq \neg\psi(x_1, \dots, x_n)$ e se la tesi è vera per ψ allora data una qualunque n-upla $(a_1, \dots, a_n) \in N^n$ per la semantica di Tarski vale

  $$N \vDash \varphi(a_1, \dots, a_n) \iff N \nvDash \psi(a_1, \dots, a_n)$$

  e per ipotesi induttiva questo è equivalente a $M \nvDash \psi(a_1, \dots, a_n)$ ovvero $M \vDash \varphi(a_1, \dots, a_n)$.
- se $\varphi(x_1, \dots, x_n) \doteq \psi(x_1, \dots, x_n) \wedge \theta(x_1, \dots, x_n)$ e se la tesi è vera per ψ e θ allora data una qualunque n-upla $(a_1, \dots, a_n) \in N^n$ per la semantica di Tarski vale

  $$N \vDash \varphi(a_1, \dots, a_n) \iff (N \vDash \psi(a_1, \dots, a_n) \wedge N \vDash \theta(a_1, \dots, a_n))$$

  e per ipotesi induttiva questo è equivalente a

  $$M \vDash \psi(a_1, \dots, a_n) \wedge M \vDash \theta(a_1, \dots, a_n)$$

  ovvero $M \vDash \varphi(a_1, \dots, a_n)$.

Essendo T senza quantificatori data una qualunque formula φ questa è equivalente in T ad una qualche formula ψ_φ senza quantificatori e sia N che M sono modelli di T, da cui segue che $N \vDash \varphi \iff N \vDash \psi_\varphi$ ed $M \vDash \varphi \iff M \vDash \psi_\varphi$ quindi data una qualunque formula $\varphi(x_1, \dots, x_n)$ e data una qualunque n-upla $(a_1, \dots, a_n) \in N^n$ per quanto appena dimostrato per le formule senza quantificatori vale

$$N \vDash \varphi(a_1, \dots, a_n) \iff N \vDash \psi_(a_1, \dots, a_n) \iff M \vDash \psi_\varphi(a_1, \dots, a_n) \iff M \vDash \varphi(a_1, \dots, a_n)$$

□

6.4 Diagramma elementare e diagramma atomico

Definizione 6.4.1: *Diagramma elementare e diagramma atomico*

Data una L-struttura M interpretandola come una $\mathfrak{L}(M)$-struttura dove $(c_j)_M = j$ per ogni $j \in M$ definiamo:

diagramma elementare di M la $\mathfrak{L}(M)$[3]-teoria completa $\mathrm{Th}(M)$, cioè l'insieme delle $\mathfrak{L}(M)$-formule valide in M, e lo indichiamo come $\mathrm{ED}(M)$.

diagramma atomico (o semplicemente *diagramma*) di M come l'insieme di $\mathfrak{L}(M)$-formule chiuse atomiche o negazione di atomiche valide in M, e lo indichiamo come $\mathrm{diag}(M)$

Proposizione 6.4.2

Date una L-struttura M ed una $\mathfrak{L}(M)$-struttura N fissando $\iota : M \to N$ la mappa che manda ogni elemento di M nell'interpretazione della rispettiva costante in N (cioè $\iota(j) = c_j^N$) allora:

1. ι è un embedding se e solo se $N \vDash \mathrm{diag}(M)$
2. ι è un embedding elementare se e solo se $N \vDash \mathrm{ED}(M)$.

Esercizio 6.6 Dimostrare la proposizione precedente.
(Suggerimento: è una facile verifica che segue dalle definizioni)

Svolgimento. Data $\varphi \in \mathrm{diag}(M)$ allora φ è una $\mathfrak{L}(M)$-formula atomica chiusa o negazione di una formula atomica chiusa tale che $M \vDash \varphi$; se ι è un embedding allora:

- se φ è atomica per definizione di embedding $N \vDash \varphi$;
- se φ è negazione della formula atomica ψ allora per la semantica di Tarski (2.1.2) $M \nvDash \psi$, quindi per definizione di embedding $N \nvDash \psi$ ovvero di nuovo per la semantica di Tarski $N \vDash \varphi$.

Se invece $N \vDash \mathrm{diag}(M)$ data un L-formula atomica $\varphi(x_1, \dots, x_k)$ e data una k-upla $(a_1, \dots, a_k) \in M^k$ se $M \vDash \varphi(a_1, \dots, a_k)$ allora $\varphi(a_1, \dots, a_k) \in \mathrm{diag}(M)$ ovvero $N \vDash \varphi(a_1, \dots, a_k)$ mentre se $M \nvDash \varphi(a_1, \dots, a_k)$ allora essendo questa formula chiusa il suo valore di verità non dipende dalle valutazioni delle variabili (2.1.4.1) quindi per la semantica di Tarski $M \vDash \neg\varphi(a_1, \dots, a_k)$ ovvero $N \vDash \neg\varphi(a_1, \dots, a_k)$ quindi per la semantica di Tarski $N \nvDash \varphi(a_1, \dots, a_k)$.

Data $\varphi \in \mathrm{ED}(M)$ allora $M \vDash \varphi$, quindi indicando $\{x_1, \dots, x_k\} = \mathrm{vl}(\varphi)$ vale

$$M \vDash \forall x_1, \dots, \forall x_k.\varphi$$

e se ι è un embedding elementare segue che

$$N \vDash \forall x_1, \dots, \forall x_k.\varphi$$

cioè per la semantica di Tarski $N \vDash \varphi$.

Se invece $N \vDash \mathrm{ED}(M)$ data una L-formula atomica $\varphi(x_1, \dots, x_k)$ e data una k-upla $(a_1, \dots, a_k) \in M^k$ per definizione $\varphi(c_{a_1}, \dots, c_{a_k})$ è una $\mathfrak{L}(M)$-formula tale che:

$$M \vDash \varphi(a_1, \dots, a_k) \iff N \vDash \varphi(c_{a_1}, \dots, c_{a_k})$$

e per costruzione di ι vale

$$N \vDash \varphi(c_{a_1}, \dots, c_{a_k}) = \varphi(\iota(a_1), \dots, \iota(a_k))$$

cioè ι è un embedding elementare. □

[3] definizione di $\mathfrak{L}(M)$ a 6.2.2

Esercizio 6.7 Nel linguaggio $L = \{s\}$ il cui unico simbolo è interpretato come il successore in $(\mathbb{N}, s)$.
Il grafico dell'addizione $+ : \mathbb{N}^2 \to \mathbb{N}$ non è definibile in $(\mathbb{N}, s)$ anche con parametri.
(Suggerimento: se l'addizione fosse definibile sarebbero definibili anche in numeri pari ($2\mathbb{N}$), ovvero esisterebbe una L-formula φ tale che $\mathbb{N} \vDash \varphi(a)$ se e solo se a è pari e quindi sarebbe verificato

$$N \vDash \forall x.\varphi(x) \longleftrightarrow \neg\varphi(s(x))$$

mostrando poi che esiste una estensione elementare propria N di $(\mathbb{N}, s)$ e che ogni tale estensione elementare ha un automorfismo che fissa punto per punto i naturali ma che non fissa l'insieme definito da φ)

6.5 I teoremi di Löwenheim-Skolem

Riprendiamo lo stesso argomento usato in un esempio precedente (3.2.1) per dimostrare adesso una prima versione di uno dei risultati che compongono il teorema di Löwenheim-Skolem.

Osservazione 6.5.1 Una L-struttura finita M non ha estensioni elementari proprie infatti, se M ha cardinalità n la $\mathfrak{L}(M)$-formula

$$\forall x.x = c_1 \vee x = c_2 \vee \cdots \vee x = c_n$$

è vera in M, quindi fa parte del diagramma elementare $\mathrm{ED}(M)$ ma se $|N| > n$ allora la formula è falsa quindi per ogni struttura N tale che $M \subseteq N$ necessariamente o $M = N$ oppure $N_M \nvDash \mathrm{ED}(M)$.

Teorema 6.5.1: *di Löwenheim-Skolem verso l'alto (versione debole)*

Data una L-teoria T se per ogni $n \in \mathbb{N}$ esiste un modello di T con cardinalità maggiore di n allora per ogni cardinalità κ allora esiste un modello di T con cardinalità maggiore di κ.
Una versione alternativa del teorema è: data una L-struttura infinita M per ogni cardinalità κ esiste una estensione elementare N di M tale che $|N| \geq \kappa$.

Dimostrazione. Per la prima delle due tesi se espandiamo il linguaggio L ad L_κ aggiungendo una costante c_i per ogni $i \in \kappa$ per ipotesi la teoria

$$T' = T \cup \{\neg c_i = c_j \mid i, j \in \kappa \wedge i \neq j\}$$

è finitamente coerente (per ogni $n \in \mathbb{N}$ esiste per ipotesi un modello di T con cardinalità maggiore di n, quindi aggiungendo un qualunque numero finito di quelle formule la teoria continua ad ammettere modelli) quindi per la proposizione 3.2.1 la L_κ-teoria T' ammette un modello M e questo per costruzione deve avere cardinalità maggiore a κ, quindi il ridotto di M da L_κ ad L è una L-struttura di cardinalità maggiore a κ tale che $M \vDash T$.

Per la seconda tesi basta applicare la prima al diagramma elementare $\mathrm{ED}(M)$ infatti per quanto appena dimostrato $\mathrm{ED}(M)$ ammette un modello di cardinalità maggiore o uguale a κ per ogni cardinale κ e questa struttura è un'estensione elementare di M per la proposizione 6.4.2. □

Per rafforzare la tesi di questo teorema vorremmo dire che la struttura ammette un modello esattamente di cardinalità κ, questa diventerà la forma forte del teorema verso l'alto, ma per dimostrare questo passeremo prima dall'altro risultato di Löwenheim-Skolem.

Teorema 6.5.2: *di Löwenheim-Skolem verso il basso*

Data una L-struttura infinita N ed un sottoinsieme A del dominio di N, allora esiste una sottostruttura elementare $M \preceq N$ tale che $A \subseteq M$ come insiemi e $|M| \leq |L| + |A| + \aleph_0$.

Dimostrazione. Costruiamo una sequenza di insiemi $\{A_i\}_{i\in\mathbb{N}}$ con $A_0 = A$ e dato A_i costruiamo A_{i+1}:

- data una L-formula $\varphi(x, y_1, \dots, y_k)$ diciamo che $a \in N$ è un testimone per $\varphi(x, y_1, \dots, y_k)$ a parametri in $B \subseteq N$ se esistono $b_1, \dots, b_k \in B$ tali che $N \vDash \varphi(a, b_1, \dots, b_k)$.
- per ogni L-formula $\varphi(x, y_1, \dots, y_k)$ e per ogni $b_1, \dots, b_k \in A_i$ scegliamo se esiste un testimone $a_\varphi \in N$ per $\varphi(x, y_1, \dots, y_k)$ a parametri in A_i
- definiamo A_{i+1} come l'unione tra l'insieme A_i e i testimoni scelti per ogni L-formula a parametri in A_i.

Se consideriamo adesso la sottostruttura $M = \bigcup_{i \in \mathbb{N}} A_i$ di N questa soddisfa le ipotesi del criterio di Tarski-Vaught (6.3.5) per costruzione quindi $M \preceq N$.

Vediamo inoltre che per ogni i vale $|A_i| \leq |L| + |A| + \aleph_0$ per induzione infatti $|A_0| = |A|$ e

$$|A_{i+1}| \leq \sum_{j \in \mathbb{N}} \left|A_i^j\right| |L\text{-formule}| = \aleph_0 \cdot \left|A_i^j\right| (|L| + \aleph_0) = |A| + |L| + \aleph_0$$

Esercizio 6.8 Mostrare che effettivamente dato un linguaggio L la cardinalità dell'insieme delle L-formule è $|L| + \aleph_0$.

Svolgimento. Anche solo il linguaggio vuoto ha infinite formule e per ogni simbolo del linguaggio c'è almeno una formula quindi la cardinalità è almeno $|L| + \aleph_0$, inoltre le L-formule sono un sottoinsieme delle $(L \cup *)$-stringhe finite, dove con $*$ intendo l'insieme finito dei simboli logici, questo insieme di stringhe ha cardinalità

$$\bigcup_{n \in \mathbb{N}} |L \cup *|^n \leq \bigcup_{n \in \mathbb{N}} |L \cup *| + \aleph_0 = (|L| + |*| + \aleph_0)\aleph_0 = |L| + \aleph_0$$

□

□

Esercizio 6.9: *Forma forte del teorema di Löwenheim-Skolem verso il basso* Data una L-struttura infinita N ed un sottoinsieme A del dominio di N, allora per ogni cardinale infinito κ tale che $|L| + |A| \leq \kappa \leq |N|$ esiste una sottostruttura elementare $M \preceq N$ tale che $|M| = \kappa$ ed A è contenuto nel dominio di M.

Dimostrazione. A meno di ingrandire il sottoinsieme A possiamo suppore $|L| \leq |A| = \kappa$, infatti se M contiene questo insieme più grande conterrà anche A.

Costruendo il modello come nel teorema (6.5.2) vediamo per induzione che $|A_n| = |A|$ per ogni n infatti ovviamente $|A_{i+1}| \geq |A|$ e per ipotesi induttiva

$$|A_{i+1}| \leq |A_i| + \sum_{j=0}^{k} \left|A_i^j\right| |L\text{-formule}| = \kappa + \aleph_0 \cdot |A_i|^j (|L| + \aleph_0) = \kappa + \aleph_0 \cdot \kappa \cdot (|L| + \aleph_0) = \kappa + \kappa = \kappa = |A|$$

□

Corollario 6.5.2.1: *Paradosso di Skolem*

Se la teoria degli insiemi ZFC è coerente allora ammette un modello numerabile.

Teorema 6.5.3: *di Löwenheim-Skolem verso l'alto (versione forte)*

Data una L-teoria T se per ogni $n \in \mathbb{N}$ esiste un modello di T con cardinalità maggiore o uguale ad n allora per ogni cardinalità infinita $\kappa > |L|$ esiste un modello di T con cardinalità esattamente κ.
Una versione alternativa del teorema è: data una L-struttura infinita M per ogni cardinalità infinita $\kappa > |L|$ esiste una estensione elementare N di M tale che $|N| = \kappa$.

Dimostrazione. Segue dalla forma debole del teorema verso l'alto (6.5.1) usando il teorema verso il basso in forma forte (6.9) per ottenere un modello esattamente della cardinalità richiesta. □

6.6 Categoricità e completezza

Definizione 6.6.1: *Teoria categorica*

Una teoria si dice categorica se ammette un unico modello a meno di isomorfismi.
Data una cardinalità κ una teoria si dice κ-categorica se, a meno di isomorfismi, ammette un unico modello di cardinalità κ.

Osservazione 6.6.1 Per i teoremi di Löwenheim-Skolem nella logica al primo ordine le uniche teorie categoriche sono le teorie finite, questa nozione può essere utile in altri tipi di logiche; vediamo invece che la categoricità restringendoci ad una data cardinalità ha delle conseguenze utili nella logica al primo ordine.

Proposizione 6.6.2: *Criterio di Łoś-Vaught*

Se T è una L-teoria κ-categorica con $|L| + \aleph_0 \leq \kappa$ e se T non ammette modelli finiti allora T è completa.

Dimostrazione. Supponiamo per assurdo che la teoria κ-categorica T non sia completa, ovvero esiste una L-formula φ e due modelli M_1 ed M_2 di T tali che $M_1 \vDash \varphi$ ed $M_2 \vDash \neg\varphi$, dato che M_1 che M_2 devono avere cardinalità infinita si possono applicare i teoremi di Löwenheim-Skolem verso il basso (6.9) o verso l'alto (6.5.3) ottenendo due modelli N_1 ed N_2 di cardinalità esattamente κ elementarmente equivalenti rispettivamente ad M_1 ed M_2 quindi $N_1 \vDash \varphi$ ed $N_2 \vDash \neg\varphi$ ma questo è assurdo perché per ipotesi N_1 ed N_2 devono essere isomorfi. □

Esempio 6.6.2 Tramite questa proposizione possiamo dimostrare direttamente che la teoria degli ordini lineari densi senza estremi T_{DLO} è completa, infatti per il teorema di isomorfismo di Cantor a meno di isomorfismo esiste un unico ordine lineare denso senza estremi numerabile, ovvero T_{DLO} è $\aleph_0$-categorica e per densità è ovvio che T_{DLO} non ha modelli finiti.
Analogamente la teoria dei campi algebricamente chiusi di caratteristica zero è $2^{\aleph_0}$-categorica e non ha modelli finiti (in quanto di caratteristica zero) quindi è completa.

Esercizio 6.10 Vedere che succederebbe nel criterio di Łoś-Vaught se la teoria avesse un modello finito.

Svoglimento. La dimostrazione non funziona perché il teorema di Löwenheim-Skolem verso l'alto nella formulazione per le strutture richiede che la struttura da estendere sia infinita, infatti le strutture finite non hanno estensioni elementari proprie (6.5.1), non essendo elementarmente equivalenti il modello finito e quello di cardinalità κ la teoria non può essere completa; il procedimento usato nella dimostrazione però riesce comunque a dirci che tutti i modelli *infiniti* di T sono elementarmente equivalenti tra loro. □

Esempio 6.6.3 La $L = \varnothing$-teoria degli insiemi infiniti è completa.
Se indichiamo con φ_n la $\varnothing$-formula che afferma l'esistenza di n elementi distinti la teoria è assiomatizzata da

$$\{\varphi_n \mid n \in \mathbb{N}^+\}$$

e chiaramente non ha modelli finiti.
Questa teoria è $\aleph_0$-categorica (o più in generale è κ-categorica per ogni cardinale infinito κ) in quanto i cardinali infiniti sono esattamente le classi di isomorfismo dei modelli di questa teoria, quindi per il criterio di Łoś-Vaught (6.6.2) questa teoria è completa.

Esempio 6.6.4 Sia $\mathbb{K}$ un campo infinito; la teoria dei K-spazi vettoriali non banali ($\mathbb{K} - VS$) è completa, infatti la teoria non ha modelli finiti quindi per Łoś-Vaught rimane da mostrare che è κ-categorica per qualche cardinale κ.
Se $\kappa > |\mathbb{K}|$ tutti i $\mathbb{K}$-spazi vettoriali di cardinalità κ devono avere una base di cardinalità κ, quindi

sono tutti isomorfi.

Esercizio 6.11 Mostrare che la teoria completa $\mathrm{Th}(\mathbb{N}, 0, s, +, \cdot)$ ha $2^{\aleph_0}$ modelli numerabili[4]. (Suggerimento: vedere quanti numeri primi standard possono dividere un elemento infinito, che esiste almeno un modello che ammette numeri infiniti che dividono esattamente una qualunque combinazione di primi standard e che ogni modello numerabile può avere pochi 'tipi' diversi di questi elementi)

Svolgimento. Indichiamo con P l'insieme dei numeri primi standard e $T = \mathrm{Th}(\mathbb{N}, 0, s, +, \cdot)$ e fissiamo una costante c al di fuori del linguaggio dell'aritmetica; dato che è finitamente coerente la teoria

$$T \cup \{\exists\, x.c = x \cdot 2, \exists\, x.c = x \cdot 3, \exists\, x.c = x \cdot 5, \ldots\} = T \cup \{\exists\, x.c = x \cdot p \mid p \in P\}$$

è finitamente coerente, quindi è coerente, cioè T ammette come modello una struttura non-standard in cui esiste un elemento multiplo di tutti i primi standard.

Analogamente dato un qualunque sottoinsieme $A \subseteq P$ è finitamente coerente anche la teoria

$$T \cup \{\exists\, x.c = x \cdot p \mid p \in A\} \cup \{\forall\, x.c \neq x \cdot p \mid p \in P \setminus A\}$$

ovvero per ogni sottoinsieme dei primi standard esiste un modello di T che ammette almeno un elemento divisibile esattamente per i primi standard contenuti in A.

Se per assurdo T avesse una quantità al più numerabile di modelli numerabili $\{M_i\}_{i\in\mathbb{N}}$ a meno di isomorfismo allora fissato $i \in \mathbb{N}$ e fissato $a \in M_i$ possiamo definire la firma di a come

$$P_a = \{p \in P \mid \exists\, x.a = x \cdot p\}$$

e quindi l'insieme delle firme degli elementi di M_i

$$P_{M_i} = \{A \subseteq P \mid \exists\, a \in M_i.A = P_a\}$$

è un sottoinsieme al più numerabile di $\mathscr{P}(P)$ ma per quanto visto in precedenza deve valere

$$\bigcup_{i\in\mathbb{N}} P_{M_i} = \mathscr{P}(P)$$

Ma questo è assurdo perché una unione numerabile di insiemi numerabili è ancora numerabile.

Inoltre le strutture numerabili nel linguaggio dell'aritmetica sono $2^{\aleph_0}$ a meno di isomorfismo, infatti data una struttura M numerabile nel linguaggio dell'aritmetica possiamo fissare una enumerazione degli elementi del suo dominio (e quindi senza perdita di generalità dire che ha come dominio $\mathbb{N}$) per poi definire univocamente M descrivendo chi è 0_M, e cosa fanno $s, +, \cdot$ su M, essendo queste ultime tre funzioni da insiemi numerabili in insiemi numerabili ci sono $2^{\aleph_0}$ combinazioni possibili ovvero $2^{\aleph_0}$ strutture numerabili dell'aritmetica. □

[4] A meno di isomorfismo, altrimenti sarebbe ovviamente una classe propria

Parte III

Computabilità ed i teoremi di Gödel

Questa parte del corso si connette alle precedenti in quanto sono nate insieme, capire che cosa voglia dire calcolare una risposta è stato giustificato dal dovere decidere se una formula è vera oppure no in un dato linguaggio, come ad esempio nei numeri naturali.

Fino ad ora abbiamo studiato quando formule sono vere o false in un contesto mente adesso ci concentriamo sulla teoria dietro alla ricerca di algoritmi che permettano di calcolare data una formula questo valore di verità, in particolare per le formule aritmetiche ($L = \{0, s, +, \cdot\}$).

L'obbiettivo del prossimo capitolo è di dire quali sono le funzioni calcolabili e gli insiemi decidibili; non entreremo nella teoria della complessità computazionale e non andremo al cuore della teoria della computabilità, che invece studia le cose che non sono calcolabili.

Ci sono due strategie principali per descrivere le funzioni calcolabili, la prima ha origine dai teoremi di Gödel e costruisce le funzioni calcolabili a partire dalle funzioni primitive ricorsive in maniera algebrica (usando operatori di chiusura) mentre la seconda esibisce modelli idealizzati di macchine da calcolo (ad esempio le macchine di Turing, che sono le più usate in quanto si adattano bene a misurare le risorse utilizzate nel calcolo).

In questo corso vedremo prima cosa sono le funzioni calcolabili alla Kleene, descriveremo poi le macchine di Turing e le corrispondenti funzioni *Turing-calcolabili* e cercheremo di verificare che le due nozioni di funzioni calcolabili così ottenute sono le stesse.

Nel capitolo successivo vedremo poi altri risultati di computabilità collegati alle funzioni calcolabili, il teorema S_n^m, il teorema del punto fisso e le relazioni tra insiemi decidibili, semidecidibili e ricorsivamente enumerabili.

Successivamente introdurremo un modo di classificare le formule aritmetiche, detto *gerarchia aritmetica*, e come questo si collega al capitolo precedente ottenendo una nozione di decidibilità o semidecidibilità per le formule; con questo potremo poi dimostrare il lemma di diagonalizzazione di Gödel che sarà cruciale nella dimostrazione del primo teorema di incompletezza di Gödel.

Dopo avere visto i teoremi di incompletezza di Gödel concluderemo mostrando a grandi linee una soluzione per il decimo problema di Hilbert che sfrutta i risultati di computabilità ed incompletezza visti in precedenza.

Capitolo 7

Due diverse nozioni di computabilità

7.1 Funzioni e predicati primitivi ricorsivi

Iniziamo introducendo una classe più ristretta rispetto alle funzioni calcolabili, quella delle funzioni *primitive ricorsive*, in quanto su queste è più facile dimostrare risultati più forti rispetto alle funzioni calcolabili (che in questa interpretazione chiameremo funzioni *ricorsive*), queste sono effettivamente una classe più piccola di tutte le funzioni calcolabili ma vedremo più avanti che con pochi passaggi si possono ottenere tutte le funzioni ricorsive partendo soltanto da funzioni primitive ricorsive (7.6.4.4).

Definizione 7.1.1: *Funzione primitiva ricorsiva*

Definiamo la *classe delle funzioni primitive ricorsive* come il più piccolo insieme di funzioni da $\mathbb{N}^k$ in $\mathbb{N}$ per qualche $k \in \mathbb{N}$ tale che

- la funzione costantemente zero $0 : \mathbb{N} \to \mathbb{N}$ è primitiva ricorsiva;
- la funzione successore $s : \mathbb{N} \to \mathbb{N}$ è primitiva ricorsiva;
- per ogni $k \in \mathbb{N}^+$ e per ogni $i \leq k$ la proiezione di $\mathbb{N}^k$ sulla i-esima coordinata $\pi_i^k : \mathbb{N}^k \to \mathbb{N}$ è primitiva ricorsiva;
- (chiusura per composizione) se $f : \mathbb{N}^h \to \mathbb{N}$ è primitiva ricorsiva e per ogni $i \leq h$ le funzioni $g_i : \mathbb{N}^k \to \mathbb{N}$ sono primitive ricorsive allora la funzione da $\mathbb{N}^k \to \mathbb{N}$ che mappa $(x_1, \ldots, x_k)$ in

  $$f(g_1(x_1, \ldots, x_k), \ldots, g_h((x_1, \ldots, x_k)))$$

  è primitiva ricorsiva;
- (chiusura per *ricorsione primitiva*) se $h : \mathbb{N}^k \to \mathbb{N}$ e $g : \mathbb{N}^{k+2} \to \mathbb{N}$ sono primitive ricorsive allora la (unica) funzione f tale che per ogni $(x_1, \ldots, x_k) \in \mathbb{N}^k$

  $$\begin{aligned} f(x_1, \ldots, x_k, 0) &= h(x_1, \ldots, x_k) \\ f(x_1, \ldots, x_k, y+1) &= g(x_1, \ldots, x_k, y, f(x_1, \ldots, x_k, y)) \end{aligned}$$

  è primitiva ricorsiva.

Esempio 7.1.1: *Esempi di funzioni primitive ricorsive*

costanti Tutte le funzioni costanti sono primitive ricorsive, ad esempio la funzione $f : \mathbb{N}^3 \to \mathbb{N}$ che manda tutto in 4 si può costruire come

$$f(x, y, z) = s(s(s(s(0(\pi_1^3(x, y, z))))))$$

operazioni aritmetiche Le operazioni aritmetiche sono primitive ricorsive, per queste usiamo la

ricorsione primitiva, ad esempio con $f(x,y) = x + y$:

$$\begin{aligned} f(x,0) &= \pi_1^1(x) \quad (= x) \\ f(x,y+1) &= g(x,y,f(x,y)) \qquad \text{dove } g(x,y,z) \doteq s(\pi_3^3(x,y,z)) \quad (= s(z)) \end{aligned}$$

a partire dalla somma nello stesso modo definiamo il prodotto e poi da questo sempre nello stesso modo l'esponenziale.

predecessore La funzione predecessore, ovvero la funzione che vale 0 in 0 ed $x-1$ per ogni $x > 0$ è primitiva ricorsiva infatti per ricorsione primitiva

$$\begin{aligned} pred(0) &= 0 \\ pred(y+1) &= \pi_1^2(y, pred(y)) \quad (= y) \end{aligned}$$

sottrazione La sottrazione nei naturali $\dot{-}$ cioè l'operazione che dà $x - y$ se $x \geq y$ e 0 altrimenti è primitiva ricorsiva infatti per ricorsione primitiva

$$\begin{aligned} x \dot{-} 0 &= \pi_1^1(x) \quad (= x) \\ x \dot{-} (y+1) &= g(x,y,x \dot{-} y) \qquad \text{dove } g(x,y,z) \doteq pred(\pi_3^3(x,y,z)) \quad (= pred(z)) \end{aligned}$$

permutazioni Se $f : \mathbb{N}^k \to \mathbb{N}$ è primitiva ricorsiva e $\pi \in S^k$ è una permutazione di k elementi allora componendo con le opportune proiezioni anche la funzione che manda

$$(x_1, \ldots, x_k) \to f(x_{\pi(1)}, \ldots, x_{\pi(k)})$$

è primitiva ricorsiva.

Definizione 7.1.2: *Predicato primitivo ricorsivo*

Diciamo *predicato ricorsivo* un sottoinsieme $S \subseteq \mathbb{N}^k$ se esiste una funzione primitiva ricorsiva $f : \mathbb{N}^k \to \mathbb{N}$ tale che $\overline{x} \in S$ se e solo se $f(\overline{x}) = 0$.

Esempio 7.1.2 la funzione $zero? : \mathbb{N} \to \mathbb{N}$ definita ponendo

$$zero?(x) = \begin{cases} 0 & \text{se } x = 0 \\ 1 & \text{altrimenti} \end{cases}$$

è primitiva ricorsiva infatti per ricorsione primitiva possiamo porre

$$\begin{aligned} zero?(0) &= 0 \\ zero?(x+1) &= 1 \end{aligned}$$

in quanto abbiamo già visto che le costanti sono primitive ricorsive

Osservazione 7.1.3: *Funzione caratteristica* Un predicato $P \subseteq \mathbb{N}^k$ è primitivo ricorsivo se e solo se esiste una funzione primitiva ricorsiva $f : \mathbb{N}^k \to \mathbb{N}$ tale che

$$f(\overline{x}) = \begin{cases} 0 & \text{se } \overline{x} \in P \\ 1 & \text{se } \overline{x} \notin P \end{cases}$$

ovvero se e solo se la *funzione caratteristica* di P è primitiva ricorsiva.
Infatti se P è primitivo ricorsivo esiste $\varphi \mathbb{N}^k \to \mathbb{N}$ funzione primitiva ricosiva che si annulla esattamente su P, allora la funzione $\psi \doteq 1 \dot{-} \varphi$ (che è primitiva ricorsiva per composizione) si annulla esattamente fuori da φ e vale 1 altrimenti, quindi $1 \dot{-} \psi$ è la funzione caratteristica di P ed è primitiva ricorsiva.

Osservazione 7.1.4: *Complementare di predicati primitivi ricorsivi* Se $P \subseteq \mathbb{N}^k$ è un predicato primitivo ricorsivo allora anche il complementare di P (l'insieme $\mathbb{N}^k \setminus P$) è un predicato primitivo ricorsivo; infatti possiamo costruire la sua funzione caratteristica come $1 \dot{-} f$ dove f è òa funzione caratteristica di P che abbiamo costruito in maniera primitiva ricorsiva nell'osservazione precedente.

Lemma 7.1.3: *Unione ed intersezione di predicati primitivi ricorsivi*

Se $P, Q \in \mathbb{N}^k$ sono predicati primitivi ricorsivi allora anche $P \cap Q$ e $P \cup Q$ sono primitivi ricorsivi.

Dimostrazione. Per l'osservazione precedente (7.1.3) la funzioni caratteristiche di P e Q sono primitive ricorsive, la somma di queste due descrive $P \cap Q$ mentre il loro prodotto descrive $P \cup Q$ e sono entrambe funzioni primitive ricorsive. □

Osservazione 7.1.5 Il lemma e l'osservazione precedenti ci dicono che i predicati primitivi ricorsivi sono un'algebra di Boole.

Esempio 7.1.6: *Relazioni* Le seguenti relazioni su $\mathbb{N}^2$ sono predicati primitivi ricorsivi:

$$x < y \quad x \leq y \quad x = y \quad x \neq y$$

infatti:

- il minore o uguale è descritto dalla funzione primitiva ricorsiva $x \dot{-} y$
- l'uguale è descritto dalla funzione primitiva ricorsiva $(x \dot{-} y) + (y \dot{-} x)$
- il diverso è il complementare dell'uguale
- la minore stretto è l'intersezione del minore o uguale con il diverso.

Esempio 7.1.7: *Definizione per casi* Dati $P \subseteq \mathbb{N}^k$ predicato primitivo ricorsivo ed $f, g : \mathbb{N}^k \to \mathbb{N}$ funzioni primitive ricorsive allora

$$h(\overline{x}) = \begin{cases} f(\overline{x}) & \text{se } \overline{x} \in P \\ g(\overline{x}) & \text{altrimenti} \end{cases}$$

è una funzione primitiva ricorsiva.
Infatti se χ_P è la funzione caratteristica di P allora possiamo costruire $h = \chi_P \cdot g + (1 \dot{-} \chi_P) \cdot f$.

Osservazione 7.1.8 Vedremo che questa costruzione non si generalizza in maniera soddisfacente al caso computabile in generale, perché definendo la nostra funzione come $\chi_P \cdot g + (1 - \chi_P) \cdot f$ se ad esempio ci fosse un caso in cui $\chi_P = 0$ ma g va in *loop* questa operazione non termina, ma effettivamente h è calcolabile perché ci interessa g soltanto in quei casi in cui $\chi_P \neq 0$.
Il metodo di definizione per casi rimmarrà legittimo anche nel caso generale ma serve una costruzione diversa per renderlo tale.

Esempio 7.1.9: *Modulo* Vediamo che il modulo è una funzione primitiva ricorsiva ($x \bmod y = z$) dove scegliamo una definizione qualunque per $x \bmod 0$ in quanto non ce n'è alcuna che sia sensata. Usiamo la ricorsione primitiva su x invece che su y, vorremmo quindi definire per casi

$$(x+1) \bmod y = \begin{cases} (x \bmod y) + 1 & \text{se } (x \bmod y) + 1 < y \\ 0 & \text{altrimenti} \end{cases}$$

nella forma di una funzione primitiva ricorsiva $h(y, x, (x \bmod y))$, quindi usiamo

$$h(y, x, \alpha) = \begin{cases} \alpha + 1 & \text{se } \alpha + 1 < y \\ 0 & \text{altrimenti} \end{cases}$$

che è primitiva ricorsiva per gli esempi precedenti (7.1.6 e 7.1.7).

Esempio 7.1.10 Vediamo che le somme parziali sono primitive ricorsive, ovvero se $f : \mathbb{N}^{k+1} \to \mathbb{N}$ è una funzione primitiva ricorsiva allora la funzione da $\mathbb{N}^{k+1} \to \mathbb{N}$ tale che

$$(\overline{x}, y) \to \sum_{i<y} f(\overline{x}, i)$$

è primitiva ricorsiva.
Infatti per ricorsione primitiva su y partiamo da 0 quando $y = 0$ e

$$\sum_{i<y+1} f(\overline{x}, i) = \sum_{i<y} f(\overline{x}, i) + f(\overline{x}, y)$$

che è nella forma $h(\overline{x}, y, \sum_{i<y} f(\overline{x}, i))$ con h primitiva ricorsiva.
Analogamente per la produttoria partendo da 1 quando $y = 0$.

Esempio 7.1.11 Vediamo che dato un predicato primitivo ricorsivo $P \subset \mathbb{N}^k$ la funzione da $\mathbb{N}^{k+1}$ in $\mathbb{N}$ tale che

$$(\overline{x}, y) \to |\{(\overline{x}, i) \mid i < y \wedge (\overline{x}, i) \in P\}|$$

è primitiva ricorsiva, infatti questa è la somma della funzione caratteristica di P ($\sum_{i<y} \chi_P$) che abbiamo gia visto essere primitiva ricorsiva.

Esempio 7.1.12: *Divisione* La divisione intera (ovvero $x \operatorname{div} y = \left\lfloor \frac{x}{y} \right\rfloor$) è primitiva ricorsiva infatti è il numero di elementi minori o uguali ad x che sono multipli di y, ovvero il numero di elementi i minori di x che soddisfano il predicato ricorsivo $(i + 1) \bmod y = 0$

$$x \operatorname{div} y = |\{i \mid i < x \wedge (i + 1) \bmod y = 0\}|$$

7.2 Liste

Introduciamo un metodo per codificare coppie di numeri naturali ed a partire da queste anche liste finite arbitrariamente lunghe in una maniera univoca con un singolo numero naturale, ed in modo da potere ottenere da queste codifiche diverse informazioni in maniera primitiva ricorsiva; in quanto questo ci servirà più avanti per effettuare diverse operazioni.

Esempio 7.2.1: *Coppie* Cerchiamo di numerare le coppie di numeri in maniera primitiva ricorsiva. Associando ad ogni coppia (x, y) la codifica primitiva ricorsiva

$$cons^1(x, y) = \frac{(x + y)(x + y + 1)}{2} + x + 1$$

otteniamo una codifica univoca per le coppie che si espande in diagonale, ovvero:

y	$\vdots$				
3	7	$\ddots$			
2	4	8	$\ddots$		
1	2	5	9	$\ddots$	
0	1	3	6	10	$\dots$
	0	1	2	3	x

Data una codifica possiamo estrarre in maniera primitiva ricorsiva il primo e secondo elemento con $car : \mathbb{N} \to \mathbb{N}$ e $cdr : \mathbb{N} \to \mathbb{N}$ tali che

$$car(cons(x, y)) = x \qquad cdr(cons(x, y)) = y$$

Per costruire car iniziamo costruendo una funzione primitiva ricorsiva che ci dice quanti numeri triangolari sono minori o uguali di un dato numero z come:

$$tri(z) = \left| \left\{ n \;\middle|\; n < z \wedge \frac{n(n+1)}{2} < z \wedge n > 0 \right\} \right|$$

infatti l'n-esimo numero triangolare è sempre maggiore o uguale ad n e non dobbiamo contare 0 in quanto il primo numero triangolare è 1.
Applicando tri a $cons(x, y)$ per costruzione otteniamo che $tri(cons(x, y)) = x + y$ quindi abbiamo calcolato $x + y$ in maniera primitiva ricorsiva, quindi possiamo definire

$$car(z) = z \dot{-} \left(\frac{tri(z)(tri(z) + 1)}{2} + 1 \right)$$

ottenendo per costruzione che effettivamente $car(cons(x, y)) = x$, e da questo possiamo poi definire cdr sottraendo car ad $x + y$ ovvero

$$cdr(z) = tri(z) \dot{-} car(z)$$

Definizione 7.2.1: *Liste*

A partire dalla codifica delle coppie definiamo la codifica della lista $(x_1, \dots, x_k)$ ponendo

$$\langle\rangle = 0^{2}$$
$$\langle x_1, \dots, x_k \rangle = cons(x_1, \langle x_2, \dots, x_k \rangle)$$

Esercizio 7.1 Le seguenti operazioni sulle codifiche sono primitive ricorsive:

1. la lunghezza di una lista $len(l)$
2. la funzione che estrae l'n-esimo elemento di una lista $nth(l, n)$
3. la concatenazione di due liste $cat(l_1, l_2)$
4. la funzione che estrae la sottolista dei primi n elementi $head(l, n)$

[1] i nomi $cons$ (constructor), car e cdr vengono dalla prima versione del linguaggio di programmazione Lisp
[2] per questo abbiamo messo il $+1$ alla fine della definizione di $cons$, così sappiamo esattamente quando fermarci espandendo la lista in quanto nessuna coppia ha come codice 0

Svolgimento. 1. definiamo per ricorsione primitiva su n una funzione da $\mathbb{N}^2$ in $\mathbb{N}$ che manda (x,n) in $(cdr)^n(x)$:

$$f(x,0) = x$$
$$f(x,n+1) = cdr(f(x,n))$$

il numero di n tali che $(cdr)^n(x,n) \neq 0$ sarà la lunghezza di n e dato che per costruzione delle coppie $(cdr)^x(x) = 0$ per ogni x allora possiamo limitarci a verificare x volte, ovvero possiamo definire

$$len(l) = |\{n < l \mid cdr^n(l) \neq 0\}|$$

2. Per dimostrare il punto 1. abbiamo visto anche che esiste una funzione che manda (x,n) in $(cdr)^n(x)$, per definire nth basta comporre

$$nth(l,n) = car(cdr^{n \dot{-} 1}(x))$$

3. Per costruire $cat(l_1,l_2)$ dimostriamo prima il seguente lemma:

Lemma 7.2.2

Date tre funzioni $g : \mathbb{N}^{a+1} \to \mathbb{N}$, $h : \mathbb{N}^{a+3} \to \mathbb{N}$, $k : \mathbb{N} \to \mathbb{N}$ primitive ricorsive se per ogni $x \in \mathbb{N}$ vale $k(x) \leq x$ allora $f : \mathbb{N}^{k+2} \to \mathbb{N}$ descritta ricorsivamente[3]

$$f(x,\overline{y},0) = g(x,\overline{y})$$
$$f(x,\overline{y},z+1) = h(x,\overline{y},z,f(k(x),\overline{y},z))$$

è primitiva ricorsiva.

Dimostrazione[4]**.** Definiamo per ricorsione primitiva $G = \mathbb{N}^{a+1} \to \mathbb{N}$ ponendo

$$G(0,\overline{y}) \doteq \langle g(0,\overline{y})\rangle$$
$$G(n+1,\overline{y}) \doteq cons(g(n+1,\overline{y}), G(n,\overline{y}))$$

così che per ogni $x \in \mathbb{N}$ vale

$$G(x,\overline{y}) = \langle g(x,\overline{y}), g(x-1,\overline{y}), \dots, g(0,\overline{y})\rangle$$

e costruiamo sempre per ricorsione primitiva $H : \mathbb{N}^{a+3} \to \mathbb{N}$

$$H(0,\overline{y},z,u) \doteq \langle h(0,\overline{y},z,nth^{len(u)}(u))\rangle$$
$$H(n+1,\overline{y},z,u) \doteq cons\left(h(n+1,\overline{y},z,nth^{len(u)\dot{-}k(n+1)}(u)), H(n,\overline{y},z,u)\right)$$

in questo modo se esistesse f tale che il numero u fosse il codice della lista

$$u = \langle f(x,\overline{y},z), f(x-1,\overline{y},z), \dots, f(0,\overline{y},z)\rangle$$

allora[5]

$$H(x,\overline{y},z,u) = \langle h(x,\overline{y},z,f(k(x),\overline{y},z)), h(x-1,\overline{y},z,f(k(x-1),\overline{y},z)), \dots, h(0,\overline{y},z,f(k(0),\overline{y},z))\rangle$$

quindi possiamo definire $F : \mathbb{N}^{k+2} \to \mathbb{N}$ per ricorsione primitiva come

$$F(x,\overline{y},0) \doteq G(x,\overline{y})$$
$$F(x,\overline{y},z+1) \doteq H(x,\overline{y},z,F(x,\overline{y},z))$$

e da questo possiamo definire f come il primo elemento della lista F, cioè

$$f(x,\overline{y},z) \doteq car(F(x,\overline{y},z))$$

ottenendo per costruzione che f è esattamente come richiesto dalla tesi. □

[3] Questa non è propriamente una ricorsione primitiva

[4] Questa dimostrazione è fortemente ispirata alle risposte dell'utente *Marc van Leeuwen* ad un quesito sul Mathematics Stackexchange, raggiungibile dal seguente link: https://math.stackexchange.com/questions/85712/how-to-prove-that-this-function-is-primitive-recursive

[5] a meno forse di un errore *off by one* quando faccio $len(u) \dot{-} k(n+1)$ nella definizione ma non ho voglia di calcolare se effettivamente ci va un ± 1 da qualche parte

Tornando al punto 3. dell'esercizio, grazie a quest'ultimo lemma e dato che cdr è una funzione decrescente possiamo definire la funzione ausiliaria $catAux(l_1, n, l_2)$ come

$$\begin{aligned} catAux(l_1, 0, l_2) &\doteq l2 \\ catAux(l_1, n+1, l_2) &\doteq cons(car(l_1), catAux(cdr(l_1), n, l_2)) \end{aligned}$$

così da potere definire $cat(l_1, l_2)$ come:

$$cat(l_1, l_2) = catAux(l_1, len(l_1), l_2)$$

4. Sempre grazie al lemma 7.2.2 dato che cdr è decrescente definiamo $head(l, n)$ come:

$$\begin{aligned} head(l, 0) &\doteq \langle\rangle \qquad (= 0) \\ head(l, n+1) &\doteq cons(car(l), head(cdr(l), n)) \end{aligned}$$

□

7.3 Funzioni calcolabili

Sebbene la classe delle funzioni primitive ricorsive contenga una grande quantità di semplici funzioni calcolabili dalla definizione possiamo vedere che le funzioni primitive ricorsive (7.1.1) rappresentano tutte quelle che in un linguaggio di programmazione potremmo calcolare usando il ciclo `for`, ovvero sapendo dall'inizio quante iterazioni dobbiamo fare, questo ci dovrebbe fare realizzare che esistono funzioni calcolabili (per una qualche definizione ragionevole di cosa sia una funzione calcolabile) che però non sono primitive ricorsive.

Esempio 7.3.1 Diamo un esempio, anche se dal valore puramente teorico, di una funzione non primitiva ricorsiva.
Per come sono definite le funzioni primitive ricorsive è possibile costruirne esplicitamente una enumerazione, allora indicando l'n-esima funzione primitiva ricorsiva f_n possiamo costruire una funzione $g : \mathbb{N} \to \mathbb{N}$ ponendo $f(n) = f_n(n) + 1$, riuscendo effettivamente ad esplicitare la numerazione delle funzioni primitive ricorsive questa con una qualunque definizione ragionevole di calcolabilità dovrà essere una funzione calcolabile ma per costruzione non è primitiva ricorsiva.

Esempio 7.3.2: *Funzione di Ackermann* Diamo un altro esempio di funzione calcolabile non primitiva ricosiva, stavolta una funzione effettivamente utile al di fuori del trovare una controesempio alla calcolabilità, descrivendo la funzione di Ackermann.
Definiamo la funzione di Ackerman in maniera ricorsiva come la funzione da $\mathbb{N}^2$ in $\mathbb{N}$ tale che

$$\begin{aligned} f(m, 0) &= s(m) \\ f(0, n+1) &= f(1, n) \\ f(m+1, n+1) &= f(f(m, n+1), n) \end{aligned}$$

Risulta da questa costruzione che sia $f(x, 0) : \mathbb{N} \to \mathbb{N}$ come anche $f(x, 1)$ crescono come $O(x)$, mentre $f(x, 2)$ cresce come $O(2x)$, però già $f(x, 3)$ cresce come un esponenziale, $f(x, 4)$ cresce come la tetrazione etc...
Pur crescendo così velocemente è calcolabile in quanto possiamo sempre ridurre il calcolo di $f(m, n)$ ad un numero finito di casi. Questo si vede per assurdo usando il principio del minimo infatti: se per assurdo non fosse così esisterebbe il minimo n_0 tale che esiste m per cui $f(m, n_0)$ non può essere ridotto ad un numero finito di casi base; ancora una volta possiamo scegliere il minimo m_0 tale che $f(m_0, n_0)$ non può essere ridotto ad un numero finito di casi base allora $m_0 \neq 0$ ed $n_0 \neq 0$ quindi per definizione

$$f(m_0, n_0) = f(f(m_0 - 1, n_0), n_0 - 1)$$

ma questo è un assurdo in quanto questa costruzione è calcolabile: $f(m_0 - 1, n_0)$ è calcolabile per minimalità di m_0 e quindi $f(f(m_0 - 1, n_0), n_0 - 1)$ è calcolabile sempre per minimalità ma stavolta la minimalità di n_0.
Invece per dimostrare che la funzione di Ackermann non è primitiva ricorsiva l'idea è vedere che la $(n+2)$-esima riga cresce più velocemente di ogni funzione primitiva ricorsiva che possiamo costruire con al più n ricorsioni primitive, da cui segue che la funzione di Ackermann non può essere primitiva ricorsiva.

Nota 7.3.3 Indichiamo $\mathbb{N}_\perp = \mathbb{N} \cup \{\perp\}$.

Definizione 7.3.1: *Funzioni ricorsive*

Definiamo la classe delle *funzioni ricorsive* come il più piccolo insieme delle funzioni da $\mathbb{N}_\perp^k$ in $\mathbb{N}_\perp$ per qualche $k \in \mathbb{N}^+$ tale che:

- la proiezione sulla i-esima coordinata di $\mathbb{N}^k$ estesa a $\perp$ se almeno una delle coordinate è $\perp$ è ricorsiva, ovvero $\pi_i^k : \mathbb{N}_\perp^k \to \mathbb{N}_\perp$ tale che
$$\pi_i^k(x_1, \dots, x_k) = \begin{cases} x_i & \text{se } (x_1, \dots, x_k) \in \mathbb{N}^k \\ \perp & \text{altrimenti} \end{cases}$$
è una funzione ricorsiva;
- il successore $s : \mathbb{N}_\perp \to \mathbb{N}_\perp$ tale che
$$s(x) = \begin{cases} x+1 & \text{se } x \in \mathbb{N}^k \\ \perp & \text{altrimenti} \end{cases}$$
è una funzione ricorsiva;
- la costante zero $0(x) : \mathbb{N}_\perp \to \mathbb{N}_\perp$ tale che
$$0(x) = \begin{cases} 0 & \text{se } x \in \mathbb{N}^k \\ \perp & \text{altrimenti} \end{cases}$$
è una funzione ricorsiva;
- (chiusura per composizione) se $f : \mathbb{N}_\perp^h \to \mathbb{N}_\perp$ è ricorsiva e per ogni $i \leq h$ le funzioni $g_i : \mathbb{N}_\perp^k \to \mathbb{N}_\perp$ sono ricorsive allora la funzione da $\mathbb{N}_\perp^k \to \mathbb{N}_\perp$ che mappa $(x_1, \dots, x_k)$ in
$$f(g_1(x_1, \dots, x_k), \dots, g_h((x_1, \dots, x_k)))$$
è ricorsiva;
- (chiusura per ricorsione primitiva) se $h : \mathbb{N}_\perp^k \to \mathbb{N}_\perp$ e $g : \mathbb{N}_\perp^{k+2} \to \mathbb{N}_\perp$ sono ricorsive allora la (unica) funzione f tale che per ogni $(x_1, \dots, x_k) \in \mathbb{N}_\perp^k$
$$f(x_1, \dots, x_k, 0) = h(x_1, \dots, x_k) \tag{7.1}$$
$$f(x_1, \dots, x_k, y+1) = g(x_1, \dots, x_k, y, f(x_1, \dots, x_k, y)) \tag{7.2}$$
$$f(x_1, \dots, x_k, \perp) = \perp \tag{7.3}$$
è ricorsiva;
- (*operatore di minimalizzazione*) se $f : \mathbb{N}_\perp^{k+1} \to \mathbb{N}_\perp$ è ricorsiva allora l'operatore di minimalizzazione su x_{k+1} di $f(x_1, \dots, x_{k+1}) = 0$ ovvero $\mu_{x_{k+1}}(f(x_1, \dots, x_{k+1}) = 0) : \mathbb{N}_\perp^{k+1} \to \mathbb{N}_\perp$ definita ponendo
$$\mu_{x_{k+1}}(f(x_1, \dots, x_{k+1}) = 0)(a_1, \dots a_k) = \\ = \begin{cases} b & \text{se } b \in \mathbb{N} \wedge f(a, \dots, a_k, b) = 0 \wedge \forall x < b. f(a, \dots, a_k, b) \in \mathbb{N}^+ \\ \perp & \text{altrimenti} \end{cases}$$
è ricorsiva.

Osservazione 7.3.4 Per quanto riguarda l'operatore di minimalizzazione notiamo che questo può fare $\perp$ in due modi:

- o c'è un particolare n tale che $f(a,\dots,a_k,n) = \perp$ e tale che $f(a,\dots,a_k,k) \in \mathbb{N}^+$ per tutti i $k < n$,
- oppure $f(a,\dots,a_k,n) \neq 0$ per ogni $n \in \mathbb{N}$,

e non stiamo distinguendo in alcun modo i due casi.

Definizione 7.3.2: *Funzione ricorsiva totale*

Una funzione ricorsiva f si dice *ricorsiva totale* $\mathrm{Im}(f\,|_{\mathbb{N}^k}) \subseteq \mathbb{N}$.

Osservazione 7.3.5 Notiamo che:

$$\text{primitive ricorsive} \subsetneq \text{ricorsive totali} \subsetneq \text{ricorsive}$$

Definizione 7.3.3: *Insieme (semi)decidibile*

Un sottoinsieme $A \subseteq \mathbb{N}^k$ per qualche $k \in \mathbb{N}^+$ si dice:

decidibile se esiste $f : \mathbb{N}^k \to \mathbb{N}$ ricorsiva totale tale che

$$A = \left\{\overline{x} \in \mathbb{N}^k \;\middle|\; f(\overline{x}) = 0\right\}$$

semidecidibile se esiste $f : \mathbb{N}^k \to \mathbb{N}_\perp$ ricorsiva tale che

$$A = \left\{\overline{x} \in \mathbb{N}^k \;\middle|\; f(\overline{x}) = 0\right\}$$

7.4 Le macchine di Turing

Definizione 7.4.1: *Macchina di Turing*

Dati due insiemi finiti Σ e Q, che chiamiamo rispettivamente *simboli* e *stati*, diciamo *macchina di Turing* M la tripla (Σ, Q, δ) dove

$$\delta : Q \times \Sigma \to Q \times \Sigma \times \{\leftarrow, \downarrow, \rightarrow\}$$

è detta *funzione di transizione*, interpretiamo M come una macchina che applicata ad un nastro contenente simboli in Σ ad ogni posizione in $\mathbb{N}$ a partire da uno stato $q \in Q$ e dalla posizione 0 in cui è prestente il simbolo $s \in \Sigma$ se $\delta(q,s) = (q', s', d)$ cambia il valore nella posizione attuale da s in s', va nello stato q' e si sposta sul nastro secondo la direzione d (ovvero $\leftarrow$ va indietro di una posizione, $\downarrow$ rimane nella stessa posizione e $\rightarrow$ va avanti di una posizione).
Diciamo *configurazione* di M una tripla (s,p,n) dove $s \in Q$ è uno stato, $p \in \mathbb{N}$ è la posizione ed

$$n \in \left\{t \in \Sigma^{\mathbb{N}} \;\middle|\; |\{i \mid t_i \neq 0\}| \in \mathbb{N}\right\}$$

è la configurazione del nastro interpretata come una sequenza (che supponiamo sia uguale ad un simbolo standard $0 \in \Sigma$ eccetto per un numero finito di posizioni).
Date due configurazioni (s,p,n) ed (s',p',n') diciamo che la seconda è *raggiungibile in un singolo passo di* M dalla prima $(s,p,n) \overset{M}{\to} (s',p',n')$ se

$$s' = \delta(s, n_p)_1$$
$$n'_i = \begin{cases} \delta(s,n_p)_2 & \text{se } i = p \\ n_i & \text{altrimenti} \end{cases}$$
$$p' = p + \delta(s,n_p)_3 \dot{-} 1$$

dove interpretiamo $\leftarrow = 0, \downarrow = 1, \rightarrow = 2$.
Diciamo invece che (s', p', n') è *raggiungibile in* $k \in \mathbb{N}$ *passi di* M da (s, p, n) indicato come $(s, p, n) \overset{M^k}{\to} (s', p', n')$ ricorsivamente su k dicendo che:

$$(s, p, n) = (s', p', n') \text{ se } k = 0$$
$$\exists (s', p", n").(s, p, n) \overset{M^{k-1}}{\to} (s", p", n") \overset{M}{\to} (s', p', n') \text{ se } k = n + 1$$

Infine diciamo che (s', p', n') è *raggiungibile tramite* M da (s, p, n) indicato come $(s, p, n) \overset{M^\star}{\to} (s', p', n')$ se esiste $k \in \mathbb{N}$ tale che $(s, p, n) \overset{M^k}{\to} (s', p', n')$.

Esempio 7.4.1 Vediamo che esiste una macchina di Turing che, data una stringa di 1 di lunghezza n aggiunge in fondo un altro 1 e torna in posizione zero.
Il linguaggio sarà $\Sigma = \{0, 1\}$ ed avremo bisogno quattro stati se vogliamo che la macchina termini in posizione zero (altrimenti ne basterebbero 2), indichiamo questi quattro stati come s_0, s_1, s_2, s_3, con s_1 lo stato di partenza:

	0	1
s_0	$s_0, 0, \downarrow$	$s_0, 1, \downarrow$
s_1	$s_0, 1, \rightarrow$	$s_2, 0, \rightarrow$
s_2	$s_3, 1, \leftarrow$	$s_2, 1, \rightarrow$
s_3	$s_0, 1, \downarrow$	$s_3, 1, \leftarrow$

Se il nastro è composto tutto di zeri questa macchina aggiunge un 1 all'inizio e va in stop.
Se il nastro ha esattamente un 1 la macchina lo cambia in zero, va avanti di una posizione, la cambia in 1, torna indietro cambia lo 0 in 1 e va in stop.
Se invece il nastro ha $n + 1$ volte 1 con $n > 1$ allora in partenza la macchina cambia l'1 in 0, va fino in fondo, aggiunge un 1 e torna in cima dove corregge lo 0 in 1 e va in stop.

Esercizio 7.2

facile costruisci una macchina di Turing che riceve in input una sequenza finita σ di zeri e uni seguita da un due seguita da tutti zeri e produce tutti 1 se σ è palindroma, tutti 0 altrimenti.

difficile dimostra che una qualunque macchina di Turing che compie l'operazione precedente richiede al caso pessimo $O(n^2)$ passi.

(Suggerimento per l'esercizio difficile: l'idea è che la macchina deve fare per forza avanti e indietro per controllare che il primo è uguale all'ultimo, poi il secondo uguale al penultimo etc...
Per dimostrare che effettivamente questo è necessario immaginiamo il caso per la stringa divisa in tre sottostringhe $s, s", s'$ di lunghezza n, con $s"$ centrale tutta di zeri, scegliamo una posizione in $s"$ e guardiamo quante volte la macchina la deve attraversare e vedere che deve succedere $O(n)$ volte)

7.5 Funzioni Turing-computabili

Definizione 7.5.1: *Funzione Turing-computabile*

Una funzione $f : \mathbb{N}^k \to \mathbb{N}_\perp$ si dice *Turing-computabile* se esiste una macchina di Turing $M = (\Sigma, Q, \delta)$ tale che

$$0, 1, \triangleright^{6} \in \Sigma$$
$$0, 1 \in Q$$
$$\forall x \in \Sigma. \delta(0, x) = (0, x, \downarrow)$$

(ovvero il nastro su cui agisce M ha almeno quei tre simboli e la macchina ha almeno due stati di cui lo stato 0 è uno stato 'di stop') e tale che definendo

$$input(x_1, \dots, x_n) = (1, 0, n_1), \qquad output(y) = (0, 0, n_2)$$

$$\text{con } n_1 = (\triangleright, \overbrace{1, \dots, 1}^{x_1}, 0, \overbrace{1, \dots, 1}^{x_2}, 0, \dots, \overbrace{1, \dots, 1}^{x_n}, 0, 0, \dots)$$

$$\text{ed } n_2 = (\triangleright, \overbrace{1, \dots, 1}^{y}, 0, 0, \dots)$$

se esiste $y \neq \perp$ tale che $f(x_1, \dots, x_k) = y$ allora

$$input(x_1, \dots, x_k) \overset{M^\star}{\to} output(y)$$

se invece $f(x_1, \dots, x_k) = \perp$ allora

$$input(x_1, \dots, x_k) \overset{M^\star}{\not\to} (0, \cdot, \cdot)$$

ovvero con tale input la macchina non raggiunge mai lo stato di stop.

7.6 Equivalenza delle due nozioni di computabilità

Teorema 7.6.1

Se $f : \mathbb{N}^k \to \mathbb{N}_\perp$ è ricorsiva[7] allora è Turing-computabile.

Dimostrazione. L'idea della dimostrazione è mostrare che le funzioni di base sono Turing-computabili e che la classe delle funzioni Turing-computabili è chiusa per composizione, ricorsione primitiva e minimalizzazione.

Adesso vediamo passo passo con attenzione il caso particolare della composizione in cui $f : \mathbb{N} \to \mathbb{N}_\perp$ e $g : \mathbb{N} \to \mathbb{N}_\perp$ sono Turing-computabili e vediamo che la composizione $f(g(x)) : \mathbb{N} \to \mathbb{N}_\perp$ è anch'essa una funzione Turing-computabile.

Il nastro di input per $x \to f(g(x))$ sarà

$$(\triangleright, \overbrace{1, \dots, 1}^{x}, 0, 0, \dots)$$

Se $F = (\Sigma_F, Q_F, \delta_F)$ e $G = (\Sigma_G, Q_G, \delta_G)$ sono macchine di Turing che applicano rispettivamente f e g, se applichiamo G a questo input se va in loop allora $f(g(x)) = \perp$ altrimenti otteniamo come output

$$(\triangleright, \overbrace{1, \dots, 1}^{g(x)}, 0, 0, \dots)$$

concludendo nello stato 0 in posizione 0, se sostituissimo questo stato con 1 ed applicassimo a questo la macchina F per costruzione se $f(g(x)) = \perp$ andremmo in loop altrimenti otterremmo come output

$$(\triangleright, \overbrace{1, \dots, 1}^{f(g(x))}, 0, 0, \dots)$$

[6] Se vogliamo restringerci ad usare solo $\mathbb{N}$ possiamo sostituire $\triangleright$ con qualunque numero diverso da 0 ed 1, abbiamo usato questa notazione con il triangolo semplicemente per comodità al livello didattico

[7] Notiamo che dal punto di vista notazionale questo è tecnicamente sbagliato in quanto una funzione ricosiva ha come dominio $\mathbb{N}_\perp^k$ ma chiaramente una volta definita f su $\mathbb{N}^k$ esiste al più una unica sua estensione ad $\mathbb{N}_\perp^k$ come funzione ricorsiva in quanto per costruzione se uno qualunque dei valori in input è $\perp$ allora applicato ad f si ottiene $\perp$

nello stato 0 in posizione 0, ovvero avremmo definito una macchina che applica $f \circ g$; per fare questo formalmente basta definire la macchina (Σ, Q, δ) tale che

$$\Sigma = \Sigma_F \cup \Sigma_G$$
$$Q = Q_F \sqcup [8] Q_G$$
$$\delta(q,x) = \begin{cases} \delta_G(q,x) & \text{se } q \in Q_G \setminus 0_G \\ \delta_F(1_F,x) & \text{se } q = 0_G \\ \delta_F(q,x) & \text{altrimenti} \end{cases}$$

dove definiamo gli stati 1 e 0 come $1 \doteq 1_G$ e $0 \doteq 0_F$.

Notiamo che in questo modo abbiamo visto che se indichiamo $1 \to A \to 0$ e $1 \to B \to 0$ due macchine di Turing allora la loro concatenazione $1 \to A \to B \to 0$ è una macchina di Turing.

Per proseguire definiamo una notazione, se ci troviamo in posizione i nello stato s con un nastro come segue

$$(\dots, \triangleright, \overbrace{1,\dots,1}^{a_1}, 0, \overbrace{1,\dots,1}^{a_2}, 0, \dots, \overbrace{1,\dots,1}^{a_n}, 0, 0, \dots)$$

dove il simbolo $\triangleright$ in rosso è nella posizione i e nelle posizioni precedenti ci sono simboli qualunque indichiamo la situazione come $s \triangleright a_1, \dots, a_n$[9] e cerchiamo di costruire macchine che non si sposteranno mai dietro il simbolo in rosso

Supponiamo adesso che esistano macchine di turing che compiono le seguenti operazioni (con la restrizione di non andare mai dietro a $\triangleright$ quindi senza cambiare niente nella parte precedente del nastro):

$$s \to push_{n,i} \to s'(s \triangleright a_1, \dots, a_n) = s' \triangleright a_1, \dots, a_n, a_i$$
$$s \to rem_{n,i} \to s'(s \triangleright a_1, \dots, a_n) = s' \triangleright a_1, \dots, \hat{a_i}[10], \dots, a_n$$
$$s \to exec_{n,k} f \to s'(s \triangleright a_1, \dots, a_n) = s' \triangleright a_1, \dots, a_{n-k}, f(a_{n-k+1}, \dots, a_k)$$
$$s \to if(a_i = 0)^{\to s'}_{\to s''}(s \triangleright a_1, \dots, a_n) = \begin{cases} s' \triangleright a_1, \dots, a_n & \text{se } a_i = 0 \\ s'' \triangleright a_1, \dots, a_n & \text{altrimenti} \end{cases}$$
$$+1 \quad \dot{-}1$$

dove s, s', s'' sono stati ed f è una funzione Turing-computabile.

Con queste macchine di Turing costruiamo altre macchine di Turing o funzioni Turing-computabili per i vari punti necessari a dimostrare il teorema; concluderemo poi dimostrando che queste macchine di Turing che abbiamo definito adesso effettivamente esistono.

- Il successore corrisponde alla funzione $+1$, la cui costruzione abbiamo già visto nell'esempio 7.4.1 (che può essere banalmente adattata a questo caso partendo da $\triangleright$), ed in maniera analoga al successore anticipiamo che è facile costruire anche la funzione $\dot{-}1$.

- Costruiamo una macchina di Turing per la funzione $0 : \mathbb{N} \to \mathbb{N}_\perp$ ponendo:

	0	1	$\triangleright$
s_0	$s_0, 0, \downarrow$	$s_0, 1, \downarrow$	$s_0, \triangleright, \downarrow$
s_1	$s_1, 0, \to$	$s_2, 0, \leftarrow$	$s_1, \triangleright, \to$
s_2	$s_2, 0, \leftarrow$	$s_2, 1, \leftarrow$	$s_0, \triangleright, \downarrow$

- grazie alle macchine $rem_{n,i}$ è immediato costruire una macchina che esegue la proiezione sulla j-esima coordinata $\pi_{n,j}$ cancellando tutti gli input tranne il j-esimo

[8] per i simboli è necessario che l'unione non sia disgiunta in quanto voglio avere 0 ed 1 di F e di G identificati mentre per gli stati è necessario che l'unione sia in qualche modo disgiunta in quanto ci saranno degli stati potenzialmente diversi ma con lo stesso nome (come lo stato iniziale 1)

[9] notiamo che dato un qualunque numero di zeri possiamo appendere questi in coda nella notazione senza cambiare il nastro, ovvero $s \triangleright a_1, \dots, a_n$ è la stessa configurazione del nastro di $s \triangleright a_1, \dots, a_n, 0, \dots, 0$ eccetto al più per quanto riguarda i simboli precedenti a $\triangleright$ e l'indice di posizione di questo simbolo

[10] usiamo questa notazione per dire che l'elemento a_i non compare nell'elenco, ovvero ad esempio in questo caso particolare $a_1, \dots, \hat{a_i}[11], \dots, a_n = a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n$

- Vediamo il caso particolare della composizione della forma

$$(x, y) \to f(g_1(x, y), g_2(x, y))$$

con f, g_1, g_2 Turing-computabili; l'input di questa funzione sarà $1\triangleright, x, y$, applicandovi le varie funzioni Turing-computabili definite in precedenza

$$\begin{aligned} 1 \to push_{2,1} \to 2(1\triangleright, x, y) &= 2 \triangleright x, y, x \\ 2 \to push_{3,2} \to 3(2\triangleright, x, y, x) &= 3 \triangleright x, y, x, y \\ 3 \to exec_{4,2} g_1 \to 4(3 \triangleright x, y, x, y) &= 4 \triangleright x, y, g_1(x, y) \\ 4 \to push_{3,1} \to push_{4,2} \to exec_{5,2} g_2 \to 5(4 \triangleright x, y, g_1(x, y)) &= 5 \triangleright x, y, g_1(x, y), g_2(x, y) \\ 5 \to exec_{4,2} f \to rem_{3,1} \to rem_{2,1} \to 0(5 \triangleright x, y, g_1(x, y), g_2(x, y)) &= 0 \triangleright f(g_1(x, y), g_2(x, y)) \end{aligned}$$

che per costruzione diverge quando $f(g_1(x, y), g_2(x, y)) = \perp$ ed altrimenti è esattamente il risultato richiesto, supponendo di sapere che le varie funzioni qua usate sono Turing-computabili è chiaro che, come visto per il caso della composizione con un solo argomento, è possibile concatenare le varie macchine di Turing che applicano le singole funzioni costruendo una macchina di Turing che applica $f(g_1(x, y), g_2(x, y))$ ovvero questa composizione è Turing-computabile.

- Come nel caso precedente è possibile mostrare Turing-computabile una composizione arbitraria

$$(x_1, \ldots, x_k) \to f(g_1(x_1, \ldots, x_k), \ldots, g_h(x_1, \ldots, x_k))$$

se $f, g_1, \ldots, g_h$ sono Turing-computabili

- Ricordando le equazioni che definiscono la ricorsione primitiva (7.1) supponendo che $g : \mathbb{N}^k \to \mathbb{N}_\perp$ e $h : \mathbb{N}^{k+2} \to \mathbb{N}_\perp$ siano Turing-computabili consideriamo l'input $1 \triangleright x_1, \ldots, x_k, y$, che per semplificare la notazione indicheremo come $1 \triangleright \overline{x}, y$ e cerchiamo di costruire $f(\overline{x}, y)$ dove f si ottiene da g ed h per ricorsione primitiva. Costruiamo la macchina di Turing concatenando quelle definite in precedenza in questo modo:

$$1 \to push_{k+1,1\ldots k} \to exec_{2k+2,k} g \to 2$$

in questo modo arriveremo nella configurazione $2 \triangleright \overline{x}, y, 0, g(\overline{x})$ dove lo 0 ci servirà più avanti per applicare h, in questo caso se $y = 0$ ci dobbiamo fermare ma se $y > 0$ dobbiamo ancora fare calcoli

$$2 \to if(a_{k+1} = 0)^{\to 3}_{\to 4}$$

per sfruttare più in generale questo if cerchiamo di arrivare nello stato 2 soltanto in configurazioni della forma $2 \triangleright \overline{x}, l, m, f(\overline{x}, m)$ dove $l + m = y$ così che se $l = 0$ andiamo nello stato 3 da dove

$$3 \to rem_{k+3,1\ldots k} \to rem_{3,1} \to rem_{2,1} \to 0$$

arrivando in $0 \triangleright f(\overline{x}, y)$.

Se invece andiamo nello stato 4 vuol dire che dovremo applicare h ancora l volte quindi

$$4 \to push_{k+3,k+1} \to exec_{k+4,1}(\dot{-}1) \to push_{k+4,k+2} \to exec_{k+5,1}(+1) \to 5$$

in questo modo 'aggiorniamo' i contatori, cioè dalla configurazione $4 \triangleright \overline{x}, l, m, f(\overline{x}, m)$ andiamo in $5 \triangleright \overline{x}, l, m, f(\overline{x}, m), l - 1, m + 1$, da questa vogliamo applicare h ad $(\overline{x}, m, f(\overline{x}, m))$

$$5 \to push_{k+5,1\ldots k} \to push_{2k+5,k+2} \to push_{2k+6,k+3} \to exec_{2k+7,k+2}(h) \to 6$$

arrivando nella configurazione $6 \triangleright \overline{x}, l, m, f(\overline{x}, m), l - 1, m + 1, f(\overline{x}, m + 1)$ (infatti per definizione $f(\overline{x}, m + 1) = h(\overline{x}, m, f(\overline{x}, m))$) adesso abbiamo tutti gli elementi necessari per tornare nello stato 2 avendo fatto un passo in più, ci basta soltanto rimuovere gli elementi di troppo:

$$6 \to remk + 6, k + 3 \to remk + 5, k + 3 \to remk + 4, k + 1 \to 2$$

in questo modo abbiamo costruito una macchina che valuta esattamente $f(\overline{x}, y)$ e va in loop se e solo se $f(\overline{x}, y) = \perp$.

-

Esercizio 7.3 Costruire una macchina di Turing per l'operatore di minimalizzazione (Suggerimento: è analogo a quanto fatto fino ad ora)

Svolgimento. Se $f : \mathbb{N}^{k+1} \to \mathbb{N}_\perp$ è Turing-computabile costruiamo l'operatore di minimalizzazione di f come

$$\begin{aligned}
&1 \to push_{k+1,1\dots k+1} \to exec_{2k+2,k+1}(f) \to 2\\
&2 \to if(a_{k+2} = 0)^{\to 3}_{\to 4}\\
&3 \to rem_{k+2,k+2} \to rem_{k+1,1\dots,k} \to 0\\
&4 \to rem_{k+2,k+2} \to exec_{k+1,1}(+1) \to 1
\end{aligned}$$

dove notiamo che partire con k elementi nell'input è equivalente a partire con $k+1$ elementi dove l'ultimo elemento è 0.

Questa così ottenuta è esattamente l'operatore di minimalizzazione, infatti dato $\overline{x} \in \mathbb{N}^k$ se esiste b tale che $f(\overline{x}, b) = 0$ e per ogni $a < b$ vale $f(\overline{x}, c) \in \mathbb{N}^+$ allora per costruzione la macchina termina come $output(b)$, altrimenti se $f(\overline{x}, b) \neq 0$ per ogni b la macchina non arriva mai nello stato 3 quindi non termina, altrimenti necessariamente esiste c tale che $f(\overline{x}, c) = \perp$ e per ogni $d < c$ vale $f(\overline{x}, d) \in \mathbb{N}^+$, in tale caso la macchina si ritrova a cercare di calcolare $f(\overline{x}, c)$ e quindi non termina. □

Per quanto riguarda dimostrare che esistono le macchine $push_{n,i}$, $rem_{n,i}$, $exec_{n,k}f$, $if(a_i = 0)$, $+1$, $\dot{-}1$ abbiamo anticipato che l'esempio 7.4.1 ci mostra come costruire la macchina $+1$ ed analogamente si costruisce $\dot{-}1$.

Per costruire $exec_{n,k}f$ se $n = k$ allora possiamo usare esattamente la macchiana per f, altrimenti $n < k$ e costruiamo una macchina che partendo da $\triangleright$ usa $n-k$ stati per andare avanti di $n-k$ variabili, al posto dello 0 che separa la $(n-k)$-esima dalla $(n-k+1)$-esima variabile inseriamo un $\triangleright$ e ci posizioniamo nello stato 1_f di partenza di una macchina che esegue f, sostituendo lo stato finale 0_f allo stato iniziale di una macchina che rimuove il $\triangleright$ in partenza e torna indietro fino al $\triangleright$ precedente.

Per $if(a_i = 0)^{\to s'}_{\to s''}$ usiamo i stati per andare avanti fino allo 0 che separa la $(i-1)$-esima dalla i-esima variabile, da li andiamo avanti di una posizione, se troviamo un 1 allora andiamo in uno stato che fa tornare la macchina in cima e quando trova $\triangleright$ va nello stato s'', altrimenti $a_i = 0$ e quindi andiamo in uno stato diverso, che ancora una volta fa tornare indietro la macchina fino a $\triangleright$ ma a quel punto va nello stato s'.

Esercizio 7.4 Costruire macchine di Turing per $push_{n,i}$ e $rem_{n,i}$.

Svolgimento. Per costruire $push_{n,i}$ fissato n iniziamo costruendo $push_{n,1}$ come

		0	1	$\triangleright$
	0	$0,0,\downarrow$	$0,1,\downarrow$	$0,\triangleright,\downarrow$
	1	$e,0,\leftarrow$	$a_0,\triangleright,\to$	$1,0,\to$
	e	$0,\triangleright,\downarrow$		$e,1,\leftarrow$
$(\forall\, j < n)$	a_j	$a_{j+1},0,\to$	$a_j,1,\to$	
	a_n	$r,1,\leftarrow$	$a_n,1,\to$	
	r	$r,0,\leftarrow$	$r,1,\leftarrow$	$1,\triangleright,\downarrow$

dove negli spazi vuoti possiamo mettere quello che vogliamo in quanto con un input ben formato la macchina non ci andrà mai.

In questo modo possiamo costruire $push_{n,i}$ per ogni $i > 1$ a partire da $push_{n-i+1,1}$ con concatenazione con altre macchine ovviamente banali da costruire:

$push_{n,1} \doteq$

$1 \to$ avanti di $i-1$ zeri $\to 2$

$2 \to$ inserisci un $\triangleright \to push_{n-i+1,1} \to 3$

$3 \to$ inserisci uno $0 \to$ torna indietro fino al precedente $\triangleright \to 0$

Anche per $rem_{n,i}$ iniziamo fissando N e costruendo $rem_{n,1}$.

La macchian $rem_{1,1}$ è semplicemente la macchina che va avanti fino a trovare uno zero e poi torna indietro scrivendo 0 in tutte le celle con 0 oppure 1 e si ferma quando ritorna al $\triangleright$.

Per costruire $rem_{n,1}$ con $n > 1$ iniziamo con una macchina che va avanti di n zeri, sostituisce un $\triangleright$ all'ultimo zero e poi torna alla posizione iniziale; a questa concateniamo la seguente se $a_1 \neq 0$

	0	1	$\triangleright$
0	$0, 0, \downarrow$	$0, 1, \downarrow$	$0, \triangleright, \downarrow$
1	$b, \triangleright, \leftarrow$	$1, 1, \rightarrow$	$1, \triangleright, \rightarrow$
b		$b, 1, \leftarrow$	$t, \triangleright, \rightarrow$
t		$n, \triangleright, \rightarrow$	
n	$n, 0, \rightarrow$	$n, 1, \rightarrow$	$r, 0, \rightarrow$
r	$c_0, 0, \leftarrow$	$c_1, 1, \leftarrow$	$e, 0, \leftarrow$
c_0	$c_0, 0, \leftarrow$	$c_0, 1, \leftarrow$	$t, 0, \rightarrow$
c_1	$c_1, 0, \leftarrow$	$c_1, 1, \leftarrow$	$t, 1, \rightarrow$
e	$e, 0, \leftarrow$	$e, 0, \leftarrow$	$ee, 0, \leftarrow$
ee	$ee, 0, \leftarrow$	$ee, 1, \leftarrow$	$0, \triangleright, \downarrow$

dove gli stati $1, b$ sostituiscono il primo zero con un $\triangleright$ e tornano alla posizione di partenza arrivando alla prima cifra dopo il $\triangleright$ (necessariamente un 1) nello stato t; in tale configurazione grazie agli stati t, n, r, c_0, c_1 la macchina inserisce un $\triangleright$ ed avanza fino al prossimo $\triangleright$; 'sposta' avanti quest'ultimo di una posizione leggendo nello stato r la cifra che vi si trovava in precedenza, se era un 1 oppure uno 0 la macchina torna indietro, scrive questa cifra al posto del $\triangleright$ inserito da t e ripete il procedimento dalla cella successiva, se invece la cifra letta nello stato r era $\triangleright$ allora la macchina ha copiato indietro tutte le cifre (questo era necessariamente il $\triangleright$ inserito in fondo alla stringa dalla macchina che ha agito in precedenza) quindi con gli stati e, ee si ritorna alla posizione 0 cancellando tutti i simboli diversi da zero che rimangono in coda.

Se invece $a_1 = 0$ la macchina precedente non funzionerebbe perché ci sarebbe un $\triangleright$ in meno, in tale caso però il problema è in realtà più semplice in quanto sappiamo con certezza che tutti i simboli vanno shiftati a sinistra di esattamente una posizione, quindi possiamo concatenare questa macchina:

	0	1	$\triangleright$
0	$0, 0, \downarrow$	$0, 1, \downarrow$	$0, \triangleright, \downarrow$
1			$a_1, \triangleright, \rightarrow$
a_1	$a_2, 0, \rightarrow$	$a_2, 1, \rightarrow$	$e, 0, \leftarrow$
a_2	$c_0, 0, \leftarrow$	$c_1, 1, \leftarrow$	$e, 0, \leftarrow$
c_0	$a_1, 0, \rightarrow$	$a_1, 0, \rightarrow$	
c_1	$a_1, 1, \rightarrow$	$a_1, 1, \rightarrow$	
e	$e, 0, \leftarrow$	$e, 0, \leftarrow$	
ee	$ee, 0, \leftarrow$	$ee, 1, \leftarrow$	$0, \triangleright, \downarrow$

In questo modo possiamo costruire $rem_{n,i}$ per ogni $i > 1$ come la concatenazione:

$remn, 1 \doteq$

$1 \rightarrow$ avanti di $i - 1$ zeri $\rightarrow 2$

$2 \rightarrow$ inserisci un $\triangleright \rightarrow rem_{n-i+1,1} \rightarrow 3$

$3 \rightarrow$ inserisci uno $0 \rightarrow$ torna indietro fino al precedente $\triangleright \rightarrow 0$

□

□

Teorema 7.6.2

Esiste una funzione ricorsiva $u : \mathbb{N}_{\perp}^2 \to \mathbb{N}$ tale che se f è una qualunque funzione Turing-computabile allora esiste un *codice di* f (denotato come $\ulcorner f \urcorner \in \mathbb{N}$) per il quale per ogni $(x_1, \ldots, x_k) \in \mathbb{N}^k$ vale

$$f(x_1, \ldots, x_k) = u(\ulcorner f \urcorner, \langle x_1, \ldots, x_k \rangle)$$

Dimostrazione. Iniziamo definendo una 'codifica delle macchine di Turing'.

Per codificare una configurazione usiamo la lista

$$\langle stato, posizione, nastro\rangle$$

di tre numeri, dove il nastro è il codice della lista finita dei valori $< s_1, \dots, s_n >$ nel nastro dove per ogni $n' > n$ vale $s_{n'} = 0$.

In questo modo una macchina di Turing è descritta completamente dalla funzione di transizione δ che, dati stato e simbolo in input produce come output uno stato, un simbolo ed una direzione di spostamento. Essendo il numero di stati e simboli entrambi finiti possiamo codificare δ con una lista $\ulcorner\delta\urcorner$ ponendo

$$nth(\ulcorner\delta\urcorner, \langle stato, simbolo\rangle) \doteq \delta(stato, simbolo) = \langle stato', simbolo', spostamento\rangle$$

Lemma 7.6.3

Esiste una funzione primitiva ricorsiva $step$ tale che data una funzione di transizione δ di una macchina di Turing M e data una configurazione c vale

$$c \xrightarrow{M} step(\ulcorner\delta\urcorner, c)$$

Dimostrazione. essendo nth primitiva ricorsiva possiamo calcolare

$$stato = nth(c, 0) \qquad posizione = nth(c, 1) \qquad nastro = nth(c, 2)$$

da queste informazioni possiamo separare il nastro in tre parti usando $head$, nth e cdr^n:

$$testa = head(nastro, posizione) \quad simbolo = nth(nastro, posizione) \quad coda = cdr^{posizione+1}(nastro)$$

in maniera primitiva ricorsiva, quindi possiamo calcolare cosa deve fare la funzione di transizione nella configurazione c come

$$nth(\ulcorner\delta\urcorner, \langle stato, simbolo\rangle) = \gamma$$

dove

$$stato' = nth(\gamma, 0) \qquad simbolo' = nth(\gamma, 1) \qquad direzione^{12} = nth(\gamma, 2)$$

allora in maniera primitiva ricorsiva possiamo costruire la configurazione

$$\langle stato', posizione + direzione \dot{-} 1, cat(testa, cons(simbolo', coda))\rangle$$

□

Vediamo che tramite la minimalizzazione a partire da $step$ possiamo costruire u.

Fissiamo $f : \mathbb{N}^k \to \mathbb{N}_\perp$ Turing-computabile ed un suo codice $\ulcorner f\urcorner$, nel lemma abbiamo visto che la funzione $step : \mathbb{N}^2 \to \mathbb{N}_\perp$ tale che

$$(\ulcorner f\urcorner, c) \to step(\ulcorner f\urcorner, c)$$

è primitiva ricorsiva, per ricorsione primitiva esattamente come abbiamo costruito cdr^n (7.1) è primitiva ricorsiva anche $step^n : \mathbb{N}^3 \to \mathbb{N}_\perp$ tale che

$$(k, \ulcorner f\urcorner, c) \to step^k(\ulcorner f\urcorner, c)$$

Dire che l'applicazione della macchina di f termina in k passi vuol dire che

$$nth(step^k(\ulcorner f\urcorner, c), 0) = 0 \wedge nth(step^{k-1}(\ulcorner f\urcorner, c), 0) \neq 0$$

ovvero che k è il minimo che minimalizza la funzione, quindi per definizione (7.3.1) l'operatore di minimalizzazione $\mu_1(nth(step^a(b, c), 0)) : \mathbb{N}^2 \to \mathbb{N}_\perp$ definito ponendo

$$\mu_1(nth(step^a(b,c),0))(b,c) = \\ = \begin{cases} k & \text{se } k \in \mathbb{N} \wedge nth(step^k(b,c),0) = 0 \wedge \forall\, h < k. nth(step^h(b,c),0) = 0 \in \mathbb{N} \setminus \{0\} \\ \perp & \text{se } \nexists\, k \in \mathbb{N}. nth(step^k(b,c),0) = 0 \end{cases}$$

è una funzione ricorsiva e per costruzione data una qualunque funzione Turing-computabile $f : \mathbb{N}^k \to \mathbb{N}_\perp$ e data una qualunque k-upla $(x_1, \dots, x_k) \in \mathbb{N}^k$ vale

$$f(x_1, \dots, x_k) = car(nth(step^{\mu_1(nth(step^a(b,c)(\ulcorner f\urcorner, \langle 1,0,\langle x_1,\dots,x_k\rangle\rangle),0))}(\ulcorner f\urcorner, \langle 1, 0, \langle x_1, \dots, x_k\rangle\rangle), 2)) \tag{7.4}$$

che per composizione è anch'essa ricorsiva, quindi quest'ultima è esattamente la u cercata. □

[12] ricordiamo la codifica per le direzioni di spostamento $0 = \leftarrow$, $1 = \downarrow$, $2 = rightarrow$

Definizione 7.6.4: *Funzione ricorsiva universale*

Dato che per il teorema precedente (7.6.1) tutte le funzioni ricorsive sono Turing-computabili in particolare per ogni $f : \mathbb{N}^k \to \mathbb{N}_\perp$ ricorsiva vale e per ogni $\overline{x} \in \mathbb{N}^k$ vale $f(\overline{x}) = u(\ulcorner f \urcorner, \langle \overline{x} \rangle)$, quindi chiamiamo u una *funzione ricorsiva universale*.

Corollario 7.6.4.1

Una funzione $f : \mathbb{N}^k \to \mathbb{N}_\perp$ è ricorsiva se e solo se è Turing-computabile.

Dimostrazione. Per il teorema 7.6.1 tutte le funzioni ricorsive sono Turing-computabili, e per il teorema successivo (7.6.2) se $f : \mathbb{N}^k \to \mathbb{N}_\perp$ è Turing-computabile allora è uguale alla funzione ricorsiva $u(\ulcorner f \urcorner, \dot{-}) : \mathbb{N}^k \to \mathbb{N}_\perp$. □

Corollario 7.6.4.2

Esiste una macchina di Turing universale, ovvero esiste una funzione Turing computabile $u : \mathbb{N}^2 \to \mathbb{N}_\perp$ tale che data una qualunque funzione Turing-computabile $f : \mathbb{N}^k \to \mathbb{N}_\perp$ per ogni $\overline{x} \in \mathbb{N}^k$ vale $u(\ulcorner f \urcorner, \langle \overline{x} \rangle) = f(\overline{x})$.

Corollario 7.6.4.3

Dato un qualunque $k \in \mathbb{N}^+$ esiste una funzione $u_k : \mathbb{N}^{k+1} \to \mathbb{N}_\perp$ ricorsiva tale che per ogni $f : \mathbb{N}^k \to \mathbb{N}_\perp$ ricorsiva e per ogni k-upla $\overline{x} \in \mathbb{N}^k$ vale $u_k(\ulcorner f \urcorner, \overline{x}) = f(\overline{x})$.

Osservazione 7.6.1: *Tesi di Church* Diciamo Tesi di Church l'idea che le funzioni ricorsive sono tutte e sole le funzioni 'veramente computabili', non lo chiamiamo teorema o congettura in quanto non è espresso in linguaggio matematico ma è soltanto un modo di collegare l'idea intuitiva di computabilità ai concetti matematici.

Corollario 7.6.4.4

Dato un qualunque $n \in \mathbb{N}^+$ esistono due funzioni $U : \mathbb{N} \to \mathbb{N}$ e $T_n : \mathbb{N}^{n+2} \to \mathbb{N}$ primitive ricorsive tali che per ogni funzione ricorsiva $f : \mathbb{N}^n \to \mathbb{N}_\perp$ vale

$$u_n(\ulcorner f \urcorner, x_1, \ldots, x_n) \neq \perp \iff \exists z. T_n(\ulcorner f \urcorner, x_1, \ldots, x_n, z) = 0$$
$$u_n(\ulcorner f \urcorner, x_1, \ldots, x_n) = U(\mu_z(T_n(\ulcorner f \urcorner, x_1, \ldots, x_n, z) = 0))$$

(cioè esistono T_n ed U primitive ricorsive tali che posso costruire f a partire da T_n ed U e dal numero $\ulcorner f \urcorner$ usando l'operatore di minimalizzazione una sola volta)

Dimostrazione. Consideriamo la costruzione della funzione ricorsiva universale vista in precedenza (7.4); la funzione $step^a(b, c)$ è primitiva ricorsiva, quindi possiamo costruire la funzione primitiva ricosiva T_n ponendo $T_n(\alpha, x_1, \ldots, x_n, z) = 0$ se e solo se:

$$nth(step^{car(z)}(\alpha, \langle 1, 0, \langle x_1, \ldots, x_n \rangle \rangle), 0) = 0 \quad \wedge \quad nnz(nth(step^{car(z)}(\alpha, \langle 1, 0, \langle x_1, \ldots, x_n \rangle \rangle), 2)) = cdr(z)$$

(con nnz la funzione primitiva ricorsiva che conta quanti elementi sono diversi da zero in una lista) cioè se e solo se z è il codice della coppia (k, y) dove k è un numero di passi dopo i quali applicando la macchina di Turing per α si arriva nello stato 0 ed y è il numero in output che si ottiene al passo k. Definiamo poi $U(x) = cdr(x)$ per potere leggere l'output (cioè y) da z dopo la minimalizzazione.

Effettivamente per costruzione se $u_n(\alpha, x_1, \ldots, x_n) = \perp$ allora per ogni $k \in \mathbb{N}$ lo stato che si ottiene applicando $step^k(\alpha, \langle 1, 0, \langle x_1, \ldots, x_n \rangle \rangle)$ è diverso da zero, quindi $T_n(\alpha, x_1, \ldots, x_n, z)$ è sempre diverso da zero; altrimenti per definizione esiste esiste k tale che $step^k(\alpha, \langle 1, 0, \langle x_1, \ldots, x_n \rangle \rangle) = 0$ quindi $T_n(\alpha, x_1, \ldots, x_n, z) = 0$ ha soluzione e per costruzione il valore in output di $u_n(\alpha, x_1, \ldots, x_n)$ è esattamente

$$U(\mu_z(T_n(\alpha, x_1, \ldots, x_n, z) = 0))$$

□

Capitolo 8

Altri risultati di computabilità

8.1 Il teorema S_n^m ed il teorema del punto fisso

Adesso vediamo due risultati che sono importanti nella teoria della computabilità anche se non ci serviranno più in questo corso.

Teorema 8.1.1: S_n^m

Dati $m, n \in \mathbb{N}$ esiste una funzione ricorsiva totale (ed in particolare primitiva ricorsiva) $S_n^m : \mathbb{N}^{n+1} \to \mathbb{N}$ tale per ogni α codice di una macchina di Turing ed $x_1, \dots, x_m, y_1, \dots y_n \in \mathbb{N}$ vale

$$u_{m+n}(\alpha, x_1, \dots, x_m, y_1, \dots y_n) = u_n(S_n^m(\alpha, x_1, \dots, x_m), y_1, \dots, y_n)$$

Osservazione 8.1.1: *Interpreti e compilatori* Una interpretazione informatica di questo teorema è che esso dica che è possibile trasformare un interprete in un compilatore, cioè nel caso $u_2(\alpha, x, y) = u_1(s_1^1(\alpha, x), y)$ se α è un interprete x è il codice della programma ed y è l'input allora la funzione $s_1^1(\alpha, x)$ è il programma compilato, cioè basta calcolarla una volta e poi da questa applicandovi l'input y si ottiene l'output $u_2(\alpha, x, y)$.
Più in generale possiamo interpretare la tesi del teorema S_n^m dicendo che data una funzione computabile ne possiamo fissare una quantità arbitraria di input in maniera computabile, cioè se $\alpha(x_1, \dots, x_k) : \mathbb{N}^k \to \mathbb{N}_\perp$ è computabile allora anche $\alpha(1, 2, 4, 10, 0, x_6, \dots x_k) : \mathbb{N}^{k-6} \to \mathbb{N}_\perp$ è computabile.

Dimostrazione del teorema 8.1.1. Notiamo che basta dimostrare il caso $m = 1$ in quanto con $m > 1$ basta iterare m volte S_n^1.

Cerchiamo quindi S_m^1 tale che

$$u_{n+1}(\alpha, x, y_1, \dots, y_n) = u_n(S_n^1(\alpha, x), y_1, \dots, y_n)$$

Cioè vogliamo che $S_n^1(\alpha, x)$ sia il codice di una macchina di Turing che partendo con input $\triangleright y_1, \dots, y_n$ lo trasforma in $\triangleright x, y_1, \dots, y_n$ ed applica α.

Costruiamo la macchina di Turing

$$1 \to \overbrace{exec_{n+1,1}(+1) \to \dots \to exec_{n+1,1}(+1)}^{x} \to$$
$$\to \overbrace{push_{n+1,1} \to rem_{n+2,1} \to \dots \to push_{n+1,1} \to rem_{n+2,1}}^{n} \to exec_{n+1,n+1}(\alpha) \to 0$$

fissati α ed x questo deve essere $S_n^1(\alpha, x)$; per costruire effettivamente S_n^1 per ricorsione primitiva sfruttiamo il prossimo lemma.

Lemma 8.1.2

Se α, β sono i codici di due macchine di Turing allora la funzione $TMcat$ che mappa (α, β) in $\alpha \to \beta$ è primitiva ricorsiva.

Dimostrazione. La funzione $TMcat$ deve:

- calcolare il massimo stato m della macchina di Turing codificata da α;
- rimpiazzare tutte le occorrenze dello stato 0 con $m+1$ ottenendo la macchina α'
- sommare m a tutte le occorrenze di tutti gli stati della macchina codificata da β eccetto le occorrenze di 0 ottenendo β'
- applicare $cat(\alpha', \beta')$

e tutti questi passaggi possono essere fatti in maniera primitiva ricorsiva. □

Con questo lemma si ottiene che per ogni $n \in \mathbb{N}$ la funzione

$$shift_{n+1,n} \doteq \overbrace{push_{n+1,1} \to rem_{n+2,1} \to \cdots \to push_{n+1,1} \to rem_{n+2,1}}^{n}$$

è primitiva ricorsiva, quindi possiamo definire S^1_n per ricorsione primitiva su x ponendo

$$S^1_n(\alpha, 0) \doteq TMcat(shift_{n+1,n}, exec_{n+1,n+1}(\alpha))$$
$$S^1_n(\alpha, x+1) \doteq TMcat(exec_{n+1,1}(+1), S^1_n(\alpha, x))$$

□

Teorema 8.1.3: *(secondo) Teorema del punto fisso*

Sia $h : \mathbb{N} \to \mathbb{N}$ una funzione ricorsiva totale, fissato $n \in \mathbb{N}^+$ esiste $\alpha \in \mathbb{N}$ tale che per ogni $\overline{x} \in \mathbb{N}^n$ vale

$$u_n(\alpha, \overline{x}) = u_n(h(\alpha), \overline{x})$$

Dimostrazione. L'idea dietro la dimostrazione è questa: cerchiamo di costruire una funzione ricorsiva F (che identifichiamo con il suo codice $\ulcorner F \urcorner$) che manda ogni x in $h(x(x))$[1] e calcoliamo $F(F)$ che per definizione è $h(F(F))$; cioè F è un punto fisso di h.

Adesso cerchiamo di adattare questo ragionamento al caso attuale.

Definiamo la funzione ricorsiva $g : \mathbb{N}^{n+1} \to \mathbb{N}_\perp$ per composizione di funzioni ricorsive come

$$g(x, \overline{y}) \doteq u_n(h(u_1(x, x)), \overline{y})$$

per poi porre $F(x) \doteq S^1_n(\ulcorner g \urcorner, x)$ e vediamo che $F(\ulcorner F \urcorner)$ è l'α richiesto, infatti dato che S^1_n è primitiva ricorsiva allora è ricorsiva totale, quindi $S^1_n(\ulcorner g \urcorner, \ulcorner F \urcorner) \in \mathbb{N}$, e dato un qualunque $\overline{y} \in \mathbb{N}^n$ per costruzione vale:

$$u_n(F(\ulcorner F \urcorner), \overline{y}) = u_n(S^1_n(\ulcorner g \urcorner, \ulcorner F \urcorner), \overline{y}) = u_{n+1}(\ulcorner g \urcorner, \ulcorner F \urcorner, \overline{y}) = g(\ulcorner F \urcorner, \overline{y})$$

e per costruzione di g e definizione della funzione universale vale

$$g(\ulcorner F \urcorner, \overline{y}) = u_n(h(u_1(\ulcorner F \urcorner, \ulcorner F \urcorner)), \overline{y}) = u_n(h(F(\ulcorner F \urcorner)), \overline{y})$$

cioè $u_n(F(\ulcorner F \urcorner), \overline{y}) = u_n(h(F(\ulcorner F \urcorner)), \overline{y})$. □

Esempio 8.1.2 Abbiamo già visto che la funzione di Ackermann è calcolabile da un punto di vista intuitivo (7.3.2) ed abbiamo descritto l'idea di come dimostrare che non è primitiva ricorsiva, adesso invece dimostriamo che è ricorsiva.

[1] la 'difficoltà' qua sta nel vedere che ogni x può essere visto come codice di una funzione ricorsiva e quindi applicato ad ogni $y \in \mathbb{N}$, in particolare quindi anche a se stesso, per fare questo basterà usare la funzione universale

Data la funzione ricorsiva universale a due parametri u_2 possiamo costruire una funzione $O : \mathbb{N}^3 \to \mathbb{N}_\perp$ definendola per casi come:

$$O(c,x,y) = \begin{cases} y+1 & \text{se } x = 0 \\ u_2(c, x \dot{-} 1, 1) & \text{se } x \neq 0 \wedge y = 0 \\ u_2(c, x \dot{-} 1, u_2(c, x \dot{-} 1, y \dot{-} 1)) & \text{altrimenti} \end{cases}$$

questa è ricorsiva in quanto è definita per casi a partire da funzioni ricorsive, quindi ammette una codifica e per il teorema S_n^m possiamo fissare c ottenendo il codice $d = S_2^1(\ulcorner O \urcorner, c)$ tale che per ogni $(x,y) \in \mathbb{N}^2$ vale $O(c,x,y) = u_2(d,x,y)$.
La mappa $S_2^1(\ulcorner O \urcorner, \cdot)$ che manda c in d è primitiva ricorsiva, quindi possiamo applicarvi il teorema del punto fisso (8.1.3) ottenendo che esiste α tale che $u_2(\alpha,x,y) = u_2(S_2^1(\ulcorner O \urcorner, \alpha), x, y)$ e quindi per costruzione

$$u_2(\alpha,x,y) = u_2(S_2^1(\ulcorner O \urcorner, \alpha), x, y) = O(\alpha,x,y) = \begin{cases} y+1 & x = 0 \\ u_2(\alpha, x \dot{-} 1, 1) & x \neq 0 \wedge y = 0 \\ u_2(\alpha, x \dot{-} 1, u_2(\alpha, x \dot{-} 1, y \dot{-} 1)) & \text{altrimenti} \end{cases}$$

ovvero per definizione $u_2(\alpha,\cdot,\cdot)$ è la funzione di Ackermann.

8.2 Semidecidibilità, decidibilità ed insiemi ricorsivamente enumerabili

Ricordiamo le definizioni viste in precedenza di insiemi decidibili e semidecidibili (7.3.3)

Definizione 8.2.1: *Insieme ricorsivamente enumerabile*

Un insieme $X \subseteq \mathbb{N}^k$ non vuoto si dice ricorsivamente enumerabile se esiste una funzione $g : \mathbb{N} \to \mathbb{N}$ ricorsiva totale tale che

$$(x_1, \dots, x_n) \in X \qquad \iff \qquad \exists\, y.g(y) = \langle x_1, \dots, x_n \rangle$$

Proposizione 8.2.2

Un insieme $X \subseteq \mathbb{N}^k$ non vuoto è semidecidibile se e solo se è ricorsivamente enumerabile e se e solo se è il dominio di una funzione ricorsiva (ovvero l'insieme degli elementi $\overline{x} \in \mathbb{N}^k$ tali che $f(\overline{x}) \neq \perp$)

Dimostrazione. Sia $X \subseteq \mathbb{N}^k$ un insieme semidecidibile, quindi esiste f ricorsiva tale che

$$X = \left\{ \overline{x} \in \mathbb{N}^k \;\middle|\; f(\overline{x}) = 0 \right\}$$

dove tutti gli $\overline{x}$ tali che $f(\overline{x}) = 0$ sono della forma $\langle x_1, \dots, x_n \rangle$.

Dato che per ipotesi $X \neq \varnothing$ possiamo scegliere $k \in X$.

Per costruzione $\overline{x} \in X$ se e solo se $f(\overline{x}) = 0$ e per il corollario 7.6.4.4 $f(\overline{x}) = 0$ se e solo se esiste $z \in \mathbb{N}$ tale che

$$T_k(\ulcorner f \urcorner, \overline{x}, z) = 0 \wedge U(z) = 0$$

dove T_k ed U sono primitive ricorsive, quindi in particolare sono ricorsive totali ovvero questa condizione è verificata se e solo se esiste $t \in \mathbb{N}$ tale che $g(t) = \langle \overline{x} \rangle$ dove definiamo g per casi come

$$g(t) = \begin{cases} car(t) & \text{se } T_k(f, nth(car(t),0), \dots, nth(car(t), k-1), cdr(t)) = 0 \wedge U(cdr(t)) = 0 \\ \langle k \rangle & \text{altrimenti} \end{cases}$$

e g è per costruzione primitiva ricorsiva (e quindi ricorsiva totale), quindi X è ricorsivamente enumerabile.

Se invece X è un insieme enumerato da f ricorsiva totale, ovvero $n \in X$ se e solo se esiste $x \in \mathbb{N}$ tale che $f(x) = n$ e questo equivale a dire che esiste x tale che $h(x) = 0$ dove

$$h(x) = 0(\mu_x(f(x) = n)^{2})$$

ovvero X è semidecidibile tramite h ricorsiva. Inoltre se $n \notin X$ allora $\nexists x.f(x) = n$, quindi $h(x) = \perp$ ovvero se X è ricorsivamente enumerabile allora è il dominio di h ricorsiva.

Per concludere basta notare che se X è il dominio di una funzione ricorsiva $r(x)$ allora X è semidecidibile dalla funzione ricorsiva $0(r(x))$. □

Esercizio 8.1 Definito l'insieme

$$TOT = \{x \mid u_1(x, \cdot) \text{ è totale}\}$$

dimostra che TOT non è semidecidibile.

Svolgimento. Supponiamo per assurdo che TOT sia ricorsivamente enumerabile, ovvero che esista una funzione ricorsiva totale f tale che $x \in TOT$ se e solo se esiste y tale che $f(y) = x$.

Allora consideriamo la funzione g che manda x in $g(x) = u_1(f(x), x) + 1$ anch'essa ricorsiva totale in quanto per ogni x vale $f(x) \in TOT$; allora per costruzione di f esiste $n \in \mathbb{N}$ tale che $g = f(n)$ ovvero tale che per ogni $x \in \mathbb{N}$ vale

$$g(x) = u_1(\ulcorner g \urcorner, x) = u_1(g(x), x)$$

ma questo è assurdo perché valutando x in n si ottiene per costruzione di g che

$$u_1(f(n), n) = g(n) = u_1(f(n), n) + 1$$

quindi TOT non è ricorsivamente enumerabile, ovvero per la proposizione 8.2.2 non è semidecidibile. □

Un'altra soluzione, che usa l'esercizio 8.3. Per definizione $(f, x) \in \overline{H_1}$ se e solo se $u_1(f, x) = \perp$, quindi se e solo se per ogni $k \in \mathbb{N}$ vale che lo stato di $step^k(f, x)$ è diverso da zero, con questo possiamo costruire la macchina $g_{f,x} : \mathbb{N} \to \mathbb{N}_\perp$ tale che

$$g_{f,x}(k) = \begin{cases} \perp & \text{se } nth(step^k(f, x), 0) \neq 0 \\ 0 & \text{altrimenti} \end{cases}$$

questa è una funzione ricorsiva totale se e solo se $(f, x) \in \overline{H_1}$, ovvero se per assurdo TOT fosse semidecidibile usando l'algoritmo che semidecide TOT sul codice della funzione ricorsiva $g_{f,x}$ per ogni coppia (f, x) otterremmo un algoritmo che semidecide $\overline{H_1}$ ma per l'esercizio 8.3 questo insieme non è semidecidibile. □

Esercizio 8.2 Un insieme $A \subseteq \mathbb{N}^k$ non vuoto è decidibile se e solo se è immagine di una funzione ricorsiva totale crescente, ovvero se esiste $f : \mathbb{N} \to \mathbb{N}$ ricorsiva totale crescente tale che dato un qualunque $\overline{x} \in \mathbb{N}^k$

$$\overline{x} \in A \iff \exists n.f(n) = \langle \overline{x} \rangle$$

Svolgimento. Se A è decidibile sia $f : \mathbb{N}^k \to \mathbb{N}$ ricorsiva totale tale che $A = \left\{\overline{x} \in \mathbb{N}^k \;\middle|\; f(\overline{x}) = 0\right\}$ e consideriamo $\chi_A : \mathbb{N} \to \mathbb{N}$ ricorsiva totale tale che

$$\chi_A(n) = \begin{cases} 0 & \text{se } \exists\, \overline{x} \in \mathbb{N}^k.n = \langle \overline{x} \rangle \wedge f(\overline{x}) = 0^{3} \\ 1 & \text{altrimenti} \end{cases}$$

Essendo $A \neq \varnothing$ esiste il minimo $n_0 \in \mathbb{N}$ tale che $\chi_A(n_0) = 0$; costruiamo per ricorsione primitiva $g : \mathbb{N} \to \mathbb{N}$ ponendo

$$g(0) \doteq n_0$$
$$g(n+1) \doteq g(n)\chi_A(n+1) + (n+1)(1 \dot{-} \chi_A(n+1))$$

[2] abbiamo definito solo il minimo tale che la funzione sia 0, ma possiamo estenderlo ad un qualunque $n \in \mathbb{N}$ definendolo come $\mu_x((f(x) \dot{-} n) + (n \dot{-} f(x)) = 0)$

[3] Per dire questo in maniera ricorsiva totale possiamo usare car e crd^n per verificare che n è il codice di una lista di k elementi e poi estrarre questi elementi ad uno ad uno per inserirli come variabili in f

questa g è ricorsiva totale crescente e l'immagine di g sono per costruzione tutti e soli i codici delle k-uple di elementi di A.

Se invece A è immagine di una funzione ricorsiva totale crescente $f : \mathbb{N} \to \mathbb{N}$ distinguiamo due casi:

- se A è finito allora è chiaramente decidibile.
- se A è infinito allora f è superiormente illimitata, quindi per ogni $x \in \mathbb{N}$ esiste $y \in \mathbb{N}$ tale che $f(y) > x$, ovvero $\mu_y(x \dot{-} f(y) = 0)$ è ricorsiva totale, quindi definendo

$$g(\overline{x}) = f\left(\mu_y(\overline{x} \dot{-} f(y) = 0)\right) \dot{-} \langle x \rangle$$

questa è una funzione ricorsiva totale tale che $g(\overline{x}) = 0$ se e solo se il più piccolo elemento dell'immagine di f maggiore o uguale a $\langle \overline{x} \rangle$ è esattamente $\overline{x}$, cioè se e solo se $\overline{x} \in A$.

□

Proposizione 8.2.3

Un sottoinsieme $X \subseteq \mathbb{N}^k$ è decidibile se e solo se sia X che il suo complementare $\overline{X} (= \mathbb{N}^k \setminus X)$ sono semidecidibili.

Dimostrazione. Se X è decidibile allora $\overline{X}$ è semidecidibile, quindi rimane da verificare l'implicazione inversa.

Supponiamo quindi che sia X che $\overline{X}$ siano semidecidibili; se $X = \varnothing$ oppure $X = \mathbb{N}^k$ allora X è decidibile, altrimenti per la proposizione 8.2.2 possiamo scegliere $f, g : \mathbb{N} \to \mathbb{N}$ funzioni ricorsive totali che enumerano rispettivamente X ed $\overline{X}$.

L'idea è di costruire un algoritmo che valuta f e g un elemento alla volta fino a quando trova l'elemento cercato o nell'immagine di f o nell'immagine di g, infatti questa macchina termina sempre in quanto $X \cup \overline{X} = \mathbb{N}^k$.

La seguente funzione è ricorsiva totale:

$$\varphi(\overline{x}) \doteq \mu_n(f(n) = \langle \overline{x} \rangle \vee g(n) = \langle \overline{x} \rangle)^{4}$$

in quanto f e g sono entrambe ricorsive totali ed ogni $\overline{x} \in \mathbb{N}^k$ appartiene ad esattamente uno tra X ed $\overline{X}$ quindi anche

$$\psi(\overline{x}) = (\langle \overline{x} \rangle \dot{-} f(\varphi(\overline{x}))) + (f(\varphi(\overline{x})) \dot{-} \langle \overline{x} \rangle)$$

è ricorsiva totale, se $\psi(\overline{x}) = 0$ allora $f(\overline{x}) = 0$ ovvero $\overline{x} \in X$, altrimenti per costruzione $g(\overline{x}) = 0$ ovvero $\overline{x} \notin X$, cioè ψ decide X. □

Definizione 8.2.4: *Halting set*

Definiamo l'insieme

$$H_1 = \{(a, x) \mid u_1(a, x) \neq \perp\}$$

halting set o *insieme della fermata* per funzioni unarie.

Proposizione 8.2.5: *Problema della fermata*

L'halting set H_1 non è decidibile.

Dimostrazione. Se per assurdo H_1 fosse decidibile allora esisterebbe

$$f(a, x) = \begin{cases} 0 & \text{se } (a, x) \in H_1 \\ 1 & \text{altrimenti} \end{cases}$$

quindi possiamo costruire $g : \mathbb{N} \to \mathbb{N}$ ricorsiva totale tale che

$$g(a) = \begin{cases} u_1(a, a) + 1 & \text{se } u_1(a, a) \neq \perp \\ 0 & \text{altrimenti} \end{cases}$$

[4] abbiamo già visto come trasformare $a(x) = y$ in $a'(x, y) = 0$, una volta che trasformiamo $f(x) = y$ in $f'(x, y) = 0$ e $g(x) = y$ in $g'(x, y) = 0$ basta imporre $\mu_n(f'(x, y) = 0 \vee g'(x, y) = 0) \doteq \mu_n(f'(x, y)g'(x, y) = 0)$

infatti per l'ipotesi assurda possiamo verificare se $u_1(a,a) \neq \perp$ in maniera ricorsiva totale calcolando $f(a,a)$.

Allora possiamo calcolare $g(\ulcorner g \urcorner) \neq \perp$ ma questo è assurdo infatti per definizione della funzione ricorsiva universale $u_1(\ulcorner g \urcorner, \ulcorner g \urcorner) = g(\ulcorner g \urcorner)$ e per costruzione di g dato che $(\ulcorner g \urcorner, \ulcorner g \urcorner) \in H_1$ vale

$$g(\ulcorner g \urcorner) = u_1(\ulcorner g \urcorner, \ulcorner g \urcorner) + 1$$

□

Esercizio 8.3 L'halting set H_1 è semidecidibile mentre il suo complementare $\overline{H}_1$ non lo è.

Svolgimento. Per la proposizione 8.2.3 dato che H_1 non è decidibile allora almeno uno tra H_1 e $\overline{H}_1$ deve essere non semidecidibile, inoltre H_1 è semidecidibile in quanto

$$0(u_1(a,x)) = 0 \qquad \Longleftrightarrow \qquad (a,x) \in H_1$$

□

Esercizio 8.4 Il complementare $\overline{TOT}$ dell'insieme TOT delle funzioni ricorsive totali non è semidecidibile.
(Suggerimento: mostrare che esiste una funzione ricorsiva totale f tale che $\alpha \in \overline{H_1}$ se e solo se $f(\alpha) \in \overline{TOT}$, in questo modo se $\overline{TOT}$ fosse semidecidibile allora avremmo un algoritmo che semidecide $\overline{H_1}$)

Svolgimento. Se $(f,x) \in \overline{H_1}$ allora $u_1(f,x) = \perp$, quindi la macchina $g_{f,x}(y) \doteq u_1(f, x(y))$ (dove $x(y)$ è la funzione costantemente x) non è una funzione ricorsiva totale; se invece $(f,x) \in H_1$ allora $g_{f,x}$ è ricorsiva totale; cioè $(f,x) \in \overline{H_1}$ se e solo se $g_{f,x} \in \overline{TOT}$.

Quindi se supponiamo per assurdo che $\overline{TOT}$ sia semidecidibile dato un algoritmo che semidecide $\overline{TOT}$ applicando questo a $g_{f,x}$ per ogni coppia (f,x) otterremmo un algoritmo che semidecide $\overline{H_1}$. □

Esercizio 8.5 Esistono A e B sottoinsiemi di $\mathbb{N}$ semidecidibili inseparabili, ovvero tali che $A \cap B = \varnothing$ e non esiste X decidibile tale che $A \subset X$ e $B \cap X \neq \varnothing$.

Svolgimento che usa il teorema di Rosser (10.3.4). Definiamo A come l'insieme dei codici $\ulcorner \varphi \urcorner$ tali che $Q \vdash \varphi$ e B l'insieme dei codici $\ulcorner \psi \urcorner$ tali che $Q \vdash \neg\psi$, questi sono semidecidibili in quanto possiamo 'esplorare' le varie dimostrazioni per verificare se ce n'è una per φ o $\neg\psi$ (se l'algoritmo non si ferma necessariamente $Q \nvdash \varphi$ o $Q \nvdash \neg\psi$ rispettivamente).

Se per assurdo esistesse C decidibile tale che $A \subset C$ e $B \cap C = \varnothing$ data una qualunque formula φ possiamo verificare in maniera ricorsiva totale se $\ulcorner \varphi \urcorner \in C$ e $\ulcorner \neg\varphi \urcorner \in C$, sfruttiamo questo per costruire una teoria ricorsivamente assiomatizzata coerente e completa che espande Q:

- Fissiamo una enumerazione delle formule aritmetiche $\varphi_1, \varphi_2, \ldots$.
- Al primo passo $T_0 = Q$ e vediamo se $\ulcorner \varphi_1 \urcorner \in C$ e se $\ulcorner \neg\varphi_1 \urcorner \in C$:
  - se $\ulcorner \varphi_1 \urcorner \in C$ e $\ulcorner \neg\varphi_1 \urcorner \notin C$ allora poniamo $T_1 = T_0 \cup \{\varphi_1\}$ infatti sia nel caso in cui $Q \vdash \varphi_1$ che nel caso in cui $Q \nvdash \varphi_1$ questa teoria rimane comunque deduttivamente coerente;
  - se $\ulcorner \varphi_1 \urcorner \notin C$ e $\ulcorner \neg\varphi_1 \urcorner \in C$ allora poniamo $T_1 = T_0 \cup \{\neg\varphi_1\}$ infatti sia nel caso in cui $Q \vdash \neg\varphi_1$ che nel caso in cui$Q \nvdash \neg\varphi_1$ questa teoria rimane comunque deduttivamente coerente;
  - se sia $\ulcorner \varphi_1 \urcorner \in C$ che $\ulcorner \neg\varphi_1 \urcorner \in C$ allora necessariamente $Q \nvdash \neg\varphi_1$ (se Q dimostrasse $\neg\varphi$ allora $\ulcorner \varphi_1 \urcorner \notin C$) quindi ponendo $T_1 = T_0 \cup \{\varphi_1\}$ questa è deduttivamente coerente;
  - altrimenti sia $\ulcorner \varphi_1 \urcorner \notin C$ che $\ulcorner \neg\varphi_1 \urcorner \notin C$ allora necessariamente $Q \nvdash \varphi_1$ (se Q dimostrasse φ_1 allora $\ulcorner \varphi_1 \urcorner \in C$) quindi ponendo $T_1 = T_0 \cup \{\neg\varphi_1\}$ questa è deduttivamente coerente.

- Al passo $(n+1)$-esimo partendo dalla teoria $T_n = Q \cup \{\psi_1, \dots, \psi_n\}$ dove $\psi_i \in \{\varphi_i, \neg\varphi_i\}$ vediamo se

$$\ulcorner(\psi_1 \wedge \cdots \wedge \psi_n) \to \varphi_{n+1}\urcorner \in C \qquad \text{e} \qquad \ulcorner(\psi_1 \wedge \cdots \wedge \psi_n) \to \neg\varphi_{n+1}\urcorner \in C$$

  a seconda dei quattro casi possibili possiamo poi aggiungere φ_{n+1} oppure $\neg\varphi_{n+1}$ a T_n ottenendo T_{n+1}.

La teoria così costruita è finitamente coerente quindi è coerente, per costruzione estende Q e sempre per costruzione è sia ricorsivamente assiomatizzata che completa, ma questo contraddice il teorema di Rosser (10.3.4). □

Un'altra soluzione[5]**.** Definiamo gli insiemi A e B come

$$A = \{x \mid u_1(x, x) = 0\}$$
$$B = \{x \mid u_1(x, x) = 1\}$$

Questi sono semidecidibili perché la funzione ricorsiva universale è per definizione ricorsiva, se per assurdo esistesse C dedicibile tale che $A \subset C$ e $B \cap C = \varnothing$ allora la funzione caratteristica

$$\chi_C(x) = \begin{cases} 1 & \text{se } x \in C \\ 0 & \text{altrimenti} \end{cases}$$

sarebbe una funzione ricorsiva (totale), potremmo quindi chiederci se $\ulcorner\chi_C\urcorner \in A$ oppure no:

- Se $\ulcorner\chi_C\urcorner \in A$ allora per definizione di A vale $u_1(\ulcorner\chi_C\urcorner, \ulcorner\chi_C\urcorner) = 0$ ovvero $\chi_C(\ulcorner\chi_C\urcorner) = 0$ e quindi $\chi_C \notin C$ ma questo è assurdo perché $A \subset C$.
- Altrimenti necessariamente $\ulcorner\chi_C\urcorner \notin A$ e quindi $u_1(\ulcorner\chi_C\urcorner, \ulcorner\chi_C\urcorner) \neq 0$ ma per costruzione di χ_C questo vuol dire che $u_1(\ulcorner\chi_C\urcorner, \ulcorner\chi_C\urcorner) = 1$ ovvero $\ulcorner\chi_C\urcorner \in B \cap C$ ed anche questo è assurdo.

□

[5] Questa dimostrazione è tratta dalle risposte dell'utente *William* ad un quesito sul Mathematics Stackexchange, raggiungibile dal seguente link: https://math.stackexchange.com/questions/320093/recursively-inseparable-sets

Capitolo 9

La gerarchia aritmetica

Il nostro scopo è riuscire a parlare delle formule con il linguaggio aritmetico.

Fissiamo la struttura $\mathbb{N} = (\mathbb{N}, 0, s, +, \cdot)$ nel linguaggio dell'aritmetica e quindi quando parliamo di formule aritmetiche saranno formule nel linguaggio $L = \{0, s, +, \cdot\}$ con le ovvie arietà. Cercheremo di capire quali sono gli insiemi definibili in questa struttura.

Definizione 9.0.1: *Quantificatori limitati*

Nel linguaggio dell'aritmetica definiamo la formula

$$\forall x \leq t.\varphi$$

come l'abbreviazione

$$\forall x.x \leq t^{1} \to \varphi$$

ed analogamente con il quantificatore esistenziale

$$\exists x \leq t.\varphi \quad \doteq \quad \exists x.x \leq t \to \varphi$$

Definiamo i vari livelli della gerarchia che vogliamo costruire a partire dal livello zero, che sarà l'insieme delle formule aritmetiche in cui gli unici quantificatori che possiamo usare sono i quantificatori limitati.

Definizione 9.0.2: *Classe* Δ_0^0

Diciamo che una formula aritmetica φ è *di classe* Δ_0^0[2]se è composta di: formule atomiche, $\vee$, $\wedge$, $\neg$ e quantificatori limitati, la classe Δ_0^0 è uguale alla classe Σ_0^0 ed alla classe Π_0^0.

Definizione 9.0.3: *Classi* Σ *e* Π

Diciamo che una formula aritmetica φ è *di classe* Σ_{n+1}^0 se è della forma

$$\varphi = \exists x_1, \ldots, \exists x_k.\psi$$

dove $\psi \in \Pi_n^0$ ed analogamente che φ è *di classe* Π_{n+1}^0 se invece è della forma

$$\varphi = \forall x_1, \ldots, \forall x_k.\psi$$

dove $\psi \in \Sigma_n^0$.
Diciamo gerarchia aritmetica l'unione di tutti i $\Sigma_\cdot^0$ e $\Pi_\cdot^0$.

[1]Nel linguaggio dell'aritmetica formalmente non c'è un simbolo di minore o uguale, però possiamo definire anche questo come una abbreviazione $x \leq t \doteq \exists y.x + y = t$

[2]in questo corso l'apice sarà sempre 0 e cambierà solo il pedice, quindi solitamente ometteremo l'apice indicandolo solo come Δ_0

Osservazione 9.0.1: *Forma normale premessa* Data una qualunque formula aritmetica φ esiste ψ nella gerarchia aritmetica tale che $\vdash \varphi \longleftrightarrow \psi$ (ovvero φ è logicamente equivalente a ψ).
Infatti in qualunque linguaggio L possiamo portare i quantificatori tutti all'inizio, in quella che si chiama *forma normale premessa*, cioè per ogni L-formula φ esiste una L-formula ψ logicamente equivalente a φ della forma

$$Q_1\, a_1, \ldots, Q_n\, a_n.\theta$$

dove θ è una L-formula priva di quantificatori e per ogni i: $Q_i \in \{\forall, \exists\}$ e a_i è una variabile.
Per dimostrare questo basta procedere per induzione sulla complessità di φ (dove essendo $\wedge, \neg$ un insieme completo di connettivi possiamo supporre che $\vee$ e $\to$ non compaiano in φ):

- se φ è atomica allora è necessariamente in forma normale premessa.
- Se φ è della forma $\exists\, x_i.\theta$ oppure $\forall\, x_i.\theta$ e come ipotesi induttiva $\theta \equiv \theta'$ dove θ' in forma normale premessa allora φ è logicamente equivalente rispettivamente a $\exists\, x_i.\theta'$ oppure $\forall\, x_i.\theta'$ entrambe in forma normale premessa.

Esercizio 9.1 Concludere la dimostrazione con i punti per $\wedge$ e $\neg$.

Svolgimento.

- Se φ è della forma $\neg\psi$ dove per ipotesi induttiva ψ è in forma normale premessa

  $$\psi = Q_1\, a_1, \ldots, Q_n\, a_n.\theta$$

  con θ priva di quantificatori allora indicando con $\overline{Q}_i$ il quantificatore diverso da Q_i allora

  $$\neg\psi \equiv \overline{Q}_1\, a_1.\neg Q_2\, a_2, \ldots, Q_n.a_n.\theta$$

  quindi con una semplice induzione su n si ricava che anche $\neg\psi$ è equivalente ad una formula in forma normale premessa

- Altrimenti φ è della forma $\psi_1 \wedge \psi_2$ dove per ipotesi induttiva

  $$\psi_1 \equiv Q_1\, a_1, \ldots, Q_n\, a_n.\theta \qquad \text{e} \qquad \psi_2 \equiv R_1\, b_1, \ldots, R_m\, b_m.\eta$$

  vediamo per induzione su n che esistono n variabili $c_1, \ldots, c_n$ tali che φ è equivalente a

  $$Q_1\, c_1, \ldots, Q_n\, c_n.(\theta\left[{}^{c_1}\!/_{a_1}, \ldots, {}^{c_n}\!/_{a_n}\right] \wedge \psi_2) \tag{9.1}$$

  infatti:

  - con $n = 0$ la tesi è vera a vuoto;
  - con $n > 0$ per finitezza delle formule esiste una variabile $x \notin \mathrm{vl}(\psi_1) \cup \mathrm{vl}(\psi_2)$ allora ψ_1 è equivalente a

    $$Q_1\, x, Q_2\, a_2, \ldots, Q_n\, a_n.\theta\left[{}^{x}\!/_{a_1}\right]$$

    e per costruzione φ è equivalente a

    $$Q_1\, x(Q_2\, a_2, \ldots, Q_n\, a_n.\theta\left[{}^{x}\!/_{a_1}\right] \wedge \psi_2)$$

    da cui si conclude grazie all'ipotesi induttiva.

  Per concludere basta notare che una formula della forma (9.1) è equivalente a:

  $$Q_1\, x_1, \ldots, Q_n\, x_n.(\psi_2 \wedge \theta\left[{}^{c_1}\!/_{x_1}, \ldots, {}^{c_n}\!/_{x_n}\right])$$

  per commutatività della congiunzione; quindi basta applicare di nuovo ciò che abbiamo appena fatto (stavolta per portare in testa $R_1\, b_1, \ldots, R_m\, b_m$) per ottenere che φ è equivalente a

  $$Q_1\, x_1, \ldots, Q_n\, x_n.R_1\, y_1, \ldots, R_m\, y_m.\left(\eta\left[{}^{y_1}\!/_{b_1}, \ldots, {}^{y_n}\!/_{b_m}\right] \wedge \theta\left[{}^{c_1}\!/_{x_1}, \ldots, {}^{c_n}\!/_{x_n}\right]\right)$$

□

Osservazione 9.0.2 Data una formula φ di classe Σ_n^0 per ogni $m > n$ aggiungendo $m - n$ quantificazioni esistenziali o universali per variabili al di fuori di $\mathrm{vl}(\varphi)$ in testa a φ si ottiene che φ è equivalente sia ad una formula di classe Σ_m^0 che ad una di classe Π_m^0 ed analogamente se φ è di classe Π_n^0, cioè

$$\Sigma_n^0 \cup \Pi_n^0 \subset \Sigma_{n+1}^0 \qquad \text{e} \qquad \Sigma_n^0 \cup \Pi_n^0 \subset \Pi_{n+1}^0$$

Inoltre esattamente come fatto per dimostrare che tutte le formule con $\wedge$ sono in forma normale premessa se φ e ψ sono di classe Σ_1^0 allora a meno di rinominare le variabili per evitare conflitti con le variabili libere dell'altra formula possiamo 'estrarre' i quantificatori esistenziali di testa ottenendo che $\varphi \wedge \psi$ è anch'essa una formula Σ_1^0, e possiamo procedere nella stessa maniera anche per Π_1^0, quindi sia Σ_1^0 che Π_1^0 sono chiusi per congiunzione.
Invece usando il fatto che $\neg\exists\, x.\varphi \equiv \forall\, x.\neg\varphi$ possiamo osservare che Σ_n^0 e Π_n^0 'commutano' per negazione, ovvero se φ è di classe Σ_n^0 allora $\neg\varphi$ è di classe Π_n^0 e viceversa.
Infine notiamo che le due classi sono chiuse anche per quantificatori limitati, infatti se $\varphi = \exists\, x.\psi$ è di classe Σ_1^0 allora

$$\exists\, y \leq t.\exists\, x.\psi \equiv \exists\, k.\exists\, y \leq t.\exists\, x \leq k.\psi$$
$$\forall\, y \leq t.\exists\, x.\psi \equiv \exists\, k.\forall\, y \leq t.\exists\, x \leq k.\psi$$

ovvero sono entrambe di classe Σ_1^0 ed analogamente se $\varphi = \forall\, x.\psi$ è di classe Π_1^0 allora

$$\exists\, y \leq t.\forall\, x.\psi \equiv \forall\, k.\exists\, y \leq t.\forall\, x \leq k.\psi$$
$$\forall\, y \leq t.\forall\, x.\psi \equiv \forall\, k.\forall\, y \leq t.\forall\, x \leq k.\psi$$

ovvero sono entrambe di classe Π_1^0, ancora una volta quindi per induzione si può usare lo stesso ragionamento per ogni Σ_n^0 e Π_n^0.

Definizione 9.0.4

Diciamo *Aritmetico* un insieme definibile in $(\mathbb{N}, 0, s, +, \cdot)$.
Se X è aritmetico diciamo che X è di classe $\spadesuit$ se esiste una formula aritmetica di classe $\spadesuit$ tale che

$$(a_1, \ldots, a_n) \in X \iff N \vDash \varphi(a_1, \ldots, a_n)$$

dove esiste n tale che $\spadesuit \in \{\Delta_0^0, \Sigma_n^0, \Pi_n^0\}$.
Se X è sia di classe Σ_n^0 che di classe Π_n^0 diciamo che è di classe Δ_n^0.

9.1 Semidecidibilità e Σ_1^0

Adesso il nostro obbiettivo sarà vedere che per ogni insieme X valgono le seguenti:

$$\text{polinomiale} \subseteq \text{di classe } \Delta_0^0 \subseteq \text{primitivo ricorsivo} \subseteq \text{decidibile} \subseteq \text{semidecidibile} = \Sigma_1^0$$

dove un insieme è polinomiale se è l'insieme delle radici di un qualche polinomio.

Notiamo che la prima inclusione è ovvia e per definizione la terza e la quarta inclusione sono entrambe vere, quindi effettivamente rimangono da vedere la seconda inclusione e l'uguaglianza finale.

Notiamo che per definizione Σ_1^0 è $\overline{\exists}\,\Delta_0^0$, cioè per ogni insieme X di classe Σ_1^0 esiste $k \in \mathbb{N}$ ed esiste $\overline{x} \in \mathbb{N}^k$ tale che esiste φ di classe Δ_0^0 per cui $\exists\, \overline{x}.\varphi$ descrive X, quindi applicando un $\overline{\exists}$ a tutte le classi tra Δ_0^0 e Σ_1^0 si collassano tutte i contenimenti in uguaglianze.

Lemma 9.1.1: *Funzione β di Gödel*

Esiste una funzione $\beta : \mathbb{N}^3 \to \mathbb{N}$ di classe Σ_1^0[3]detta β *di Gödel* tale che dato un qualunque $n \in \mathbb{N}$ per ogni n-upla $(x_0, \ldots, x_{n-1}) \in \mathbb{N}^n$ esistono a, b tali che per ogni $i < n$

$$\beta(a, b, i) = x_i$$

Dimostrazione. La β di Gödel è definita come

$$\beta(a,b,i) = a \bmod (b(i+1)+1)$$

infatti per fare funzionare questo dati $n, x_0, \dots, x_{n-1}$ dobbiamo trovare a e b che rispolvono il seguente sistema di equazioni

$$\begin{cases} a \mod (b+1) = x_0 \\ a \mod (2\,b+1) = x_1 \\ \vdots \\ a \mod (n\,b+1) = x_{n-1} \end{cases}$$

perché questo sistema abbia soluzione per il teorema cinese del resto basta che $b+1, \dots, n\,b+1$ siano tutti coprimi e che per ogni $i < n$ valga $(i+1)b+1 > x_i$.

Per fare questo basta scegliere $b = (n!)^k$ dove k è abbastanza grande che per ogni $i < n$ vale $b > x_i$, infatti fissati i, j con $0 < j < i \leq n$ se per assurdo esistesse l primo che divide sia $i\,b+1$ che $j\,b+1$, allora per l'algoritmo di euclide $l \mid b(i-j)$ ma l non divide b in quanto divisore di $i\,b+1$ ed l non divide $i-j$ in quanto altrimenti dividerebbe b (perché $i-j < i \leq n$); quindi l'unico divisore comune di $i\,b+1$ e $j\,b+1$ è 1, ovvero i due sono coprimi.

Per concludere basta scrivere $\beta(a,b,i) = a \bmod d(b(i+1)+1)$ con una formula di classe Σ_1^0 e $a \bmod (b(i+1)+1) = c$ se e solo se

$$\mathbb{N} \vDash c < b(i+1)+1 \wedge \exists t.t(b(i+1)+1)+c = a$$

grazie alla chiusura per quantificatori limitati e per congiunzione l'unica parte non immediatamente Σ_1^0 di questa formula è la sottoformula $c < b(i+1)+1$; possiamo concludere descrivendo quest'ultima con la formula Σ_1^0

$$\exists t.c + t = b(i+1)+1$$

□

Lemma 9.1.2

Ogni funzione ricorsiva è di classe Σ_1^0 ovvero data una funzione $f : \mathbb{N}^k \to \mathbb{N}_\perp$ ricorsiva esiste una formula φ di classe Σ_1^0 tale che $f(x_1, \dots, x_k) = y$ se e solo se $\mathbb{N} \vDash \varphi(x_1, \dots, x_k, y)$

Dimostrazione. Procediamo per induzione sulla complessità della definizione di f (7.3.1). Per i passi base:

- se $f \doteq 0$ è la funzione costantemente nulla allora basta porre $\varphi(x,y) \equiv y = 0$
- se $f \doteq s$ allora basta porre $\varphi(x,y) \equiv s(x) = y$
- altrimenti $f \doteq \pi_i^k$ proiezione di $\mathbb{N}^k$ sulla i-esima coordinata, quindi basta porre $\varphi(x_1, \dots, x_k, y) \equiv x_i = y$

per i passi induttivi:

- per la composizione se $f \doteq F(g_1, \dots, g_h)$ dove $F : \mathbb{N}^h \to \mathbb{N}_\perp$ e per ogni $i \leq h$ anche $g_i : \mathbb{N}^k \to \mathbb{N}_\perp$ sono ricorsive per le quali vale la tesi, ovvero esistono formule aritmetiche φ e $\psi_1, \dots, \psi_h$ di classe Σ_1^0 tali che

$$\begin{array}{ccc} y = F(x_1, \dots, x_h) & \iff & \mathbb{N} \vDash \varphi(x_1, \dots, x_h, y) \\ y = g_1(x_1, \dots, x_k) & \iff & \mathbb{N} \vDash \psi_1(x_1, \dots, x_k, y) \\ \vdots & \vdots & \vdots \\ y = g_h(x_1, \dots, x_k) & \iff & \mathbb{N} \vDash \varphi_h(x_1, \dots, x_k, y) \end{array}$$

  allora vale $f(x_1, \dots, x_k) = y$ se e solo se

$$\mathbb{N} \vDash \exists y_1, \dots, \exists y_h.\varphi(y_1, \dots, y_h, y) \wedge \psi_1(x_1, \dots, x_k, y_1) \wedge \dots \wedge \psi_h(x_1, \dots, x_k, y_h)$$

  che per l'osservazione 9.0.2 è anch'essa una formula di classe Σ_1^0

[3] Formalmente non abbiamo definito le classi Δ, Σ, Π per funzioni, quello che vogliamo dire con questo è che $\beta(x,y,z) = t$ è esprimibile tramite una formula di classe Σ_1^0, ovvero esiste φ di classe Σ_1^0 tale che $\beta(x,y,z) = t \iff \mathbb{N} \vDash \varphi(x,y,z,t)$

- per la ricorsione primitiva supponiamo che $h : \mathbb{N}^k \to \mathbb{N}_\perp$ e $g : \mathbb{N}^{k+2} \to \mathbb{N}_\perp$ siano ricorsive che soddisfano la tesi e consideriamo la funzione $f : \mathbb{N}^{k+1} \to \mathbb{N}_\perp$ costruita per ricorsione primitiva a partire da h e g, ovvero tale che per ogni $\overline{x} \in \mathbb{N}^k$

$$f(\overline{x}, 0) = h(\overline{x})$$
$$f(\overline{x}, y+1) = g(\overline{x}, y, f(\overline{x}, y))$$

  Vorremmo poter concludere dicendo che $f(\overline{x}, y) = z$ se e solo se

$$N \vDash \exists\, t_0, \ldots, \exists\, t_y . t_0 = h(\overline{x}) \wedge (\forall\, i < y . t_{i+1} = g(\overline{x}, i, t_i)) \wedge t_y = z$$

  ma questa non è formalmente una formula al variare di y in quanto y è anche il numero di quantificatori esistenziali ovvero dati due di y diversi questo corrisponde a due formule diverse; per ottenere una formula valida che fa questo possiamo però usare la β di Gödel (9.1.1), dicendo che $f(\overline{x}, y) = z$ se e solo se

$$N \vDash \exists\, a, b . \beta(a, b, 0) = h(\overline{x}) \wedge (\forall\, i < y . \beta(a, b, i+1) = g(\overline{x}, i, \beta(a, b, i))) \wedge \beta(a, b, y) = z$$

  e questa è una formula di classe Σ_1^0 dato che la classe è chiusa per $\wedge$, $\exists$, composizione (per il punto appena visto) e quantificatore universale limitato.

- per la minimalizzazione sia $g : \mathbb{N}^{k+1} \to \mathbb{N}_\perp$ ricorsiva tale che esiste φ di classe Σ_1^0 tale che

$$g(\overline{x}, y) = z \iff \mathbb{N} \vDash \varphi(\overline{x}, y, z)$$

  e consideriamo la funzione ricorsiva $f(\overline{x}) = \mu_y(g(\overline{x}, y) = 0)$, vediamo che $f(\overline{x}) = z$ se e solo se

$$g(\overline{x}, z) = 0 \wedge \forall\, t < z . g(\overline{x}, t) \in \mathbb{N}^+$$

  e questa formula è di classe Σ_1^0 infatti è chiusa per congiunzione, per ipotesi induttiva $g(\overline{x}, z) = 0$ e si può scrivere il secondo termine della congiunzione come

$$\forall\, t < z . \exists\, i . g(\overline{x}, t) = i \wedge i \neq 0$$

  che è anch'essa Σ_1^0 in quanto la classe è chiusa per quantificatori limitati e per congiunzione ed $i \neq 0$ è una formula di classe Δ_0^0.

□

Lemma 9.1.3

Se $A \subseteq \mathbb{N}^k$ è un insieme di classe Δ_0^0 esiste una funzione primitiva ricorsiva $f : \mathbb{N}^k \to \mathbb{N}$ tale che $\overline{x} \in A \iff f(\overline{x}) = 0$.

Dimostrazione. Verifichiamo la tesi per induzione sulla complessità della formula $\varphi(\overline{x}, y)$ di classe Δ_0^0 che descrive A.

- i predicati atomici dell'aritmetica sono della forma $p(x_1, \ldots, x_n) = q(y_1, \ldots, y_m)$, dove p e q sono polinomi; abbiamo già dimostrato che $+$ e $\cdot$ sono primitive ricorsive (7.1.1), quindi basta notare che $p = q$ se e solo se $(p \dot{-} q) + (q \dot{-} p) = 0$;
- se $\varphi = \neg\psi$ ed $\mathbb{N} \vDash \psi \iff f = 0$ con f primitiva ricorsiva allora $\mathbb{N} \vDash \varphi$ se e solo se $1 \dot{-} f = 0$;
- se $\varphi = \psi_1 \wedge \psi_2$ ed

$$\mathbb{N} \vDash \psi_1 \iff f = 0 \qquad \text{e} \qquad \mathbb{N} \vDash \psi_2 \iff g = 0$$

  con f e g primitive ricorsive allora $\mathbb{N} \vDash \varphi$ se e solo se $f + g = 0$
- se $\varphi = \neg\psi$ ed $\mathbb{N} \vDash \psi \iff f = 0$ con f primitiva ricorsiva allora $\mathbb{N} \vDash \varphi$ se e solo se $1 \dot{-} f = 0$;
- se $\varphi = \forall\, y < t . \psi$ ed $\mathbb{N} \vDash \psi \iff f(\overline{x}, y) = 0$ allora $\mathbb{N} \vDash \varphi$ se e solo se

$$|\{x < t \mid f(\overline{x}, y) \neq 0\}| = 0$$

  ed abbiamo già visto che la funzione che conta la cardinalità di questo insieme è primitiva ricorsiva (7.1.10);

- se $\varphi = \exists\, y < t.\psi$ ed $\mathbb{N} \vDash \psi \iff f(\overline{x}, y) = 0$ allora $\mathbb{N} \vDash \varphi$ se e solo se

$$|\{x < t \mid f(\overline{x}, y) = 0\}| \neq 0$$

  ed anche questa è primitiva ricorsiva.

□

Teorema 9.1.4

Un sottoinsieme A di $\mathbb{N}^k$ è semidecidibile se e solo se è di classe Σ_1^0.

Dimostrazione. Se A è semidecidibile esiste f ricorsiva tale che $f(\overline{x}) = 0$ se e solo se $\overline{x} \in A$ e il lemma precedente (9.1.2) questa è di classe Σ_1^0, ovvero esiste φ di classe Σ_1^0 tale che

$$\overline{x} \in A \iff f(\overline{x}) = 0 \iff N \vDash \varphi(\overline{x}, 0)$$

ovvero A è di classe Σ_1^0.

Se invece A è di classe Σ_1^0 allora esiste una formula aritmetica φ di classe Σ_1^0 tale che $\overline{x} \in A \iff \mathbb{N} \vDash \varphi(\overline{x})$, e per definizione possiamo scrivere

$$\varphi(\overline{x}) = \exists\, y_1, \ldots, \exists\, y_m.\psi(y_1, \ldots, y_m, \overline{x})$$

dove ψ è di classe Δ_0^0.

Per il lemma 9.1.3 esiste f primitiva ricorsiva tale che $\mathbb{N} \vDash \psi(y_1, \ldots, y_m, \overline{x})$ se e solo se

$$f(y_1, \ldots, y_m, \overline{x}) = 0$$

allora possiamo costruire la funzione ricorsiva

$$g(\overline{x}) = 0(\mu_t(f(nth(t, 0), \ldots, nth(t, n-1), \overline{x}) = 0))$$

essendo f primitiva ricorsiva è anche ricorsiva totale, quindi $g(\overline{x}) = 0$ se $\mathbb{N} \vDash \varphi(\overline{x})$ e $g(\overline{x}) = \perp$ altrimenti, ovvero A è di classe Σ_1^0. □

Corollario 9.1.4.1

La verità aritmetica non è decidibile, ovvero fissata una codifica per le formule aritmetiche l'insieme $P \subseteq \mathbb{N}$ tale che $\ulcorner\varphi\urcorner \in P$ se e solo se $\mathbb{N} \vDash \varphi$ non è un insieme decidibile.

Dimostrazione. Per il teorema precedente (9.1.4) la funzione ricorsiva universale u_1 è Σ_1^0 ovvero esiste una formula aritmetica φ tale che

$$u_1(x, y) = z \iff \mathbb{N} \vDash \varphi(x, y, z)$$

e quindi data una qualunque coppia $(x, y) \in \mathbb{N}^2$

$$(x, y) \in H_1 \iff \mathbb{N} \vDash \exists\, z.\varphi(x, y, z)$$

ma se per assurdo la verità aritmetica fosse decidibile allora dati qualunque (x, y) la formula $\exists\, z.\varphi(x, y, z)$ sarebbe decidibile, quindi l'halting set sarebbe decidibile, che contraddice il problema della fermata (8.2.5). □

Esercizio 9.2 La proposizione $P(\ulcorner\varphi\urcorner) = \mathbb{N} \vDash \varphi$ non è semidecidibile.

Svolgimento. Se per assurdo tale proposizione fosse semidecidibile data una qualunque φ allora sarebbe vero uno tra $P(\ulcorner\varphi\urcorner)$ e $P(\ulcorner\neg\varphi\urcorner)$ in quanto $\mathbb{N} \vDash \varphi$ o $\mathbb{N} \vDash \neg\varphi$ ma allora potremmo costruire un algoritmo che fa alternamente un passo per valutare $P(\ulcorner\varphi\urcorner)$ e poi uno per $P(\ulcorner\neg\varphi\urcorner)$ fino a ricavare quale delle due (unicamente) è vera, e questo algoritmo termina per ogni φ, e questo è assurdo per il corollario precedente (9.1.4.1). □

Proposizione 9.1.5

Un insieme $X \subseteq \mathbb{N}^k$ è decidibile se e solo se è di classe Δ_1^0.

Dimostrazione. Se X è decidibile allora è semidecidibile, quindi per il teorema 9.1.4 è di classe Σ_1^0 ma essendo decidibile anche il suo complementare $\overline{X}$ è semidecidibile (8.2.3) quindi esiste ψ di classe Σ_1^0 tale che

$$\overline{x} \in \overline{X} \qquad \iff \qquad \mathbb{N} \vDash \psi(\overline{x})$$

ovvero

$$\overline{x} \in X \qquad \iff \qquad \mathbb{N} \vDash \neg\psi(\overline{x})$$

e la negazione di una formula Σ_1^0 è di classe Π_1^0 quindi X è di classe Δ_1^0.

Se invece X è di classe Δ_1^0 allora è di classe Σ_1^0 quindi X è semidecidibile e con lo stesso ragionamento appena usato anche $\overline{X}$ è semidecidibile quindi X è decidibile. □

9.2 L'aritmetica come teoria del primo ordine

Abbiamo già introdotto due teorie dell'aritmetica al primo ordine (2.3.10): la teoria di Peano PA e la Q di Robinson; queste differiscono in quanto la teoria di peano usa infiniti assiomi per soddisfare il principio di induzione mentre la Q ha un assioma

$$Q_7: \qquad x \neq 0 \to \exists\, y.x = s(y)$$

(che è un caso particolare dell'induzione) e con l'esercizio (2.6) abbiamo verificato che Q è strettamente più debole di PA in quanto non può dimostrare tutti gli assiomi di induzione.

L'origine degli assiomi della Q di Robinson è che sono un insieme minimale necessario a far funzionare i teoremi di incompletezza di Gödel.

Definizione 9.2.1: *Formula decidibile*

Data una L-teoria T ed una L-formula φ diciamo che T *decide* φ (e quindi che φ è *decidibile* in T) se $T \vdash \varphi$ oppure $T \vdash \neg\varphi$.

Il nostro obbiettivo ora sarà dimostrare che per tutte le formule chiuse φ di classe Δ_0^0 e Σ_1^0 vale che

$$\mathbb{N} \vDash \varphi \iff Q \vdash \varphi$$

con il teorema 9.2.9, prima però avremo bisogno di diversi lemmi.

Definizione 9.2.2: *Numerali*

Dato $n \in \mathbb{N}$ definiamo il *numerale* n come come il termine

$$\overline{n} \qquad \doteq \qquad \overbrace{s(\dots(s(}^{n}0))\dots)$$

nel linguaggio dell'aritmetica.

Definizione 9.2.3: *Elementi standard e non-standard*

Dato un modello M della Q di Robinson ed $x \in M$ diciamo che x è

standard se esiste un numerale $\overline{n}$ tale che $M \vDash x = \overline{n}$;

non-standard altrimenti.

Osservazione 9.2.1 Tutti i modelli $M \vDash Q$ contengono $\mathbb{N}$; eventualmente possono contenere anche altri elementi e tali elementi, come il punto all'infinito nell'esercizio 2.6, sono esattamente gli elementi non-standard della struttura M.

Lemma 9.2.4

Dato un termine aritmetico t se t è chiuso allora esiste $n \in \mathbb{N}$ tale che $Q \vdash t = \overline{n}$ dove $n = \overline{\{\}_{\mathbb{N}}\, t}$[4].

Dimostrazione. Iniziamo notando che un termine aritmetico chiuso è necessariamente una concatenazione di applicazioni di $s, +, \cdot$ all'unico simbolo di costante 0 (in quanto non deve contenere variabili).

Per induzione strutturale su t basta verificare i seguenti:

$$Q \vdash \overline{0} = \overline{0}$$
$$Q \vdash s(\overline{n}) = \overline{s(n)}$$
$$Q \vdash \overline{m} + \overline{n} = \overline{m+n}$$
$$Q \vdash \overline{m} \cdot \overline{n} = \overline{m \cdot n}$$

Le prime due sono banalmente vere per ispezione della formula (e per definizione del numerale $\bar{\cdot}$).

Esercizio 9.3 Completare la dimostrazione per $+$ e $\cdot$.

Svolgimento. Vediamo per induzione su n che $Q \vdash \overline{m} + \overline{n} = \overline{m+n}$:

- Con $n = 0$ allora dagli assiomi di Q segue che $Q \vdash \overline{m} + \overline{0} = \overline{m}$ e nella struttura $\mathbb{N}$ vale $m = m + 0$ quindi $\vdash \overline{m} = \overline{m+0}$.
- Con $n = s(k)$ se per ipotesi induttiva $Q \vdash \overline{m} + \overline{k} = \overline{m+k}$ allora per gli assiomi di Q vale $Q \vdash \overline{m} + s(\overline{k}) = s(\overline{m} + \overline{k})$ e quindi grazie all'ipotesi induttiva $Q \vdash \overline{m} + \overline{n} = s\left(\overline{m+k}\right)$ dove per definizione dei numerali $s(\overline{m+k}) \equiv \overline{s(m+k)}$ e nella struttura $\mathbb{N}$ vale $s(m+k) = m + s(k) = m + n$ ovvero $\vdash \overline{s(m+k)} = \overline{m+n}$.

Il prodotto si dimostra per induzione come la somma. □

□

Lemma 9.2.5

Data una formula aritmetica atomica φ se φ è chiusa φ è decidibile in Q ed in particolare:

$$\mathbb{N} \vDash \varphi \iff Q \vdash \varphi$$
$$\mathbb{N} \vDash \neg\varphi \iff Q \vdash \neg\varphi$$

Dimostrazione. Una formula atomica chiusa nel linguaggio dell'aritmetica può essere soltanto $t_1 = t_2$ con t_1 e t_2 termini chiusi.

Indichiamo $n = \{\}_{\mathbb{N}}\, t_1$ ed $m = \{\}_{\mathbb{N}}\, t_2$; allora $\mathbb{N} \vDash \varphi$ se e solo se $n_1 = n_2$.

Se $n_1 = n_2$ allora per il lemma precedente (9.2.4) $Q \vdash t_1 = \overline{n}_1$ e $Q \vdash t_2 = \overline{n}_1$ quindi $Q \vdash t_1 = t_2 (\doteq \varphi)$.

Se $n_1 \neq n_2$ allora Q deve dimostrare $\neg\varphi$ e per fare questo basta dimostrare che $Q \vdash \neg\overline{n}_1 = \overline{n}_2$. Senza perdita di generalità possiamo assumere $n_1 < n_2$, allora procediamo per induzione[5] su n_2:

- Se $n_2 = 0$ è vero a vuoto;
- Se $n_2 = s(m_2)$ abbiamo due sottocasi con $n_1 = 0$ oppure $n_1 > 0$:
  - se $n_1 = 0$ bisogna dimostrare che $Q \vdash \neg 0 = s(\overline{m}_2)$ e questo è vero assiomaticamente;
  - altrimenti $n_1 > 0$ quindi per l'assioma Q_7 esiste m_1 tale che $n_1 = s(m_1)$ e bisogna dimostrare che $Q \vdash \neg s(\overline{m}_1) = s(\overline{m}_2)$ che segue da $Q \vdash \neg\overline{m}_1 = \overline{m}_2$ e questo è vero per ipotesi induttiva in quanto $m_2 < n_2$ ed $m_1 < n_1 \leq m_2$.

Essendo Q coerente non possono valere sia $Q \vdash \varphi$ che $Q \vdash \neg\varphi$ quindi dalle due implicazioni che abbiamo dimostrato delle quattro nella tesi si ricavano anche le altre due e dato che vale esattamente una tra $\mathbb{N} \vDash \varphi$ ed $\mathbb{N} \vDash \neg\varphi$ allora Q decide φ. □

[4] Questo è il numerale ($\bar{\cdot}$) della valutazione in $\mathbb{N}$ di t, dove la valutazione è vuota in quanto essendo t chiuso non importa quali variabili ci sono nella valutazione (2.1.4.1)

[5] Questa induzione è 'esterna' alla struttura, non potrebbe essere atrimenti in quanto Q non ha gli assiomi di induzione

Definizione 9.2.6: *Minore o uguale*

Dati due termini aritmetici t_1 e t_2 definiamo $t_1 \leq t_2$ come una abbreviazione per la formula aritmetica

$$\exists x.x + t_1 = t_2$$

Esercizio 9.4 Mostrare che esistono modelli della Q di Robinson in cui la somma non è commutativa.

Svolgimento. In maniera analoga all'esercizio 2.6 costruiamo un modello di Q dove la somma non è commutativa. Consideriamo la struttura dell'aritmetica che ha come dominio $\mathbb{N} \cup \{i, j\}$ estendendo le interpretazioni su $\mathbb{N}$ ponendo per i e j:

$$\begin{aligned}
i + 0 &= i & j + 0 &= j \\
i + s(n) &= s(i + n) & j + s(n) &= s(j + n) \\
n + i &= j & n + j &= i \\
i + j &= i & j + i &= j \\
i + i &= j & j + j &= i \\
i \cdot 0 &= 0 & j \cdot 0 &= 0 \\
i \cdot s(n) &= i \cdot n + i & j \cdot s(n) &= j \cdot n + j \\
n \cdot i &= i & n \cdot j &= \begin{cases} i & \text{se } n \text{ pari} \\ j & \text{se } n \text{ dispari} \end{cases} \\
i \cdot j &= j & j \cdot i &= i \\
i \cdot i &= j & j \cdot j &= i
\end{aligned}$$

in questa struttura la somma non è commutativa e vediamo che è un modello di Q.

Q_1 Per costruzione non esistono elementi il cui successore è 0.

Q_2 Per costruzione il successore è iniettivo.

Q_3 Per costruzione per ogni x vale $x + 0 = x$.

Q_4 Dati x, y nel modello vediamo che vale il quarto assioma di Q:

- se $x, y \in \mathbb{N}$ allora $x + s(y) = s(x + y)$ perché è vero in $\mathbb{N}$;
- se $x = i$ ed $y \in \mathbb{N}$ allora per costruzione $x + s(y) = i + s(y) = s(i + y)$, ed analogamente se $x = j$ ed $y \in \mathbb{N}$;
- se $x = y = i$ allora $x + s(y) = i + s(i) = i + j = i = s(j) = s(i + i)$ ed analogamente se $x = y = j$.
- se $x = i$ ed $y = j$ allora $x + s(y) = i + s(j) = i + i = j$ ed anche $s(x + y) = s(i + j) = s(i) = j$, ed analogamente se $x = j$ ed $y = i$;
- se $x \in \mathbb{N}$ ed $y = i$ allora $x + s(y) = x + s(i) = x + j = i = s(j) = s(x + i)$, altrimenti $x \in \mathbb{N}$ ed $y = j$ ed anche questo caso è analogo al precedente.

Q_5 Per costruzione per ogni x vale $x \cdot 0 = 0$.

Q_6 Dati x, y nel modello vediamo che vale il sesto assioma di Q:

- se $x, y \in \mathbb{N}$ allora $x \cdot s(y) = x \cdot y + x$ perché è vero in $\mathbb{N}$;
- se $x = i$ ed $y \in \mathbb{N}$ allora per costruzione $x \cdot s(y) = i \cdot s(y) = i \cdot y + i$, ed analogamente se $x = j$ ed $y \in \mathbb{N}$;
- se $x = y = i$ allora $x \cdot s(y) = i \cdot s(i) = i \cdot j = j$ ed anche $x \cdot y + x = i \cdot i + i = j + i = j$ ed analogamente se $x = y = j$;

- se $x = i$ ed $y = j$ allora $x \cdot s(y) = i \cdot s(j) = i \cdot i = j$ ed anche $i \cdot j + i = j + i = j$, ed analogamente se $x = j$ ed $y = i$;
- se $x \in \mathbb{N}$ ed $y = i$ allora notiamo che quando $n \in \mathbb{N}$ è pari allora nel modello così costruito si ottiene che $i + n = i$ e $j + n = j$ mentre se $n \in \mathbb{N}$ è dispari vale $i + n = j$ e $j + n = i$ ed ogni $x \in \mathbb{N}$ è o pari o dispari quindi:
  - se x è pari allora $x \cdot s(y) = x \cdot s(i) = x \cdot j = i$ ed anche $x \cdot y + x = x \cdot i + x = i + x = i$;
  - altrmenti x è dispari, allora $x \cdot s(y) = x \cdot s(i) = x \cdot j = j$ ed anche $x \cdot y + x = x \cdot i + x = i + x = j$;
- altrimenti $x \in \mathbb{N}$ ed $y = j$ allora:
  - se x è pari $x \cdot s(y) = x \cdot s(j) = x \cdot i = i$ ed anche $x \cdot j + x = i + x = i$;
  - altrimenti x è dispari, allora $x \cdot s(y) = x \cdot s(j) = x \cdot i = i$ ed anche $x \cdot j + x = j + x = i$.

Q$_7$ Per costruzione tutti gli elementi diversi da 0 sono successori di qualche altro elemento.

□

Da questo esercizio segue che nella Q di Robinson $t_1 \leq t_2$ definito come sopra a priori non è la stessa cosa di

$$\exists x.t_1 + x = t_2$$

ovviamente avremmo anche potuto scegliere questa come definizione del $\leq$, con la definizione che abbiamo scelto noi possiamo dimostrare che dato M modello di Q ed $x \in M$ non-standard allora x è molto grande, cioè per ogni numerale $\overline{n}$ vale $M \vDash \overline{n} \leq x$; mentre con l'altra definizione saremmo in grado di dimostrare che

$$Q \vdash \forall x.\forall y.x \leq s(y) \to (x = s(y) \vee x \leq y)$$

Abbiamo scelto la prima delle due definizioni perché ci è più utile avere il primo dei due risultati rispetto al secondo.

Osservazione 9.2.2 Sui numeri standard quello che abbiamo definito è esattamente il classico ordine $\leq$, ma dato un qualunque modello M di Q il $\leq$ come lo abbiamo definito non sarà neanche necessariamente un ordine.

Lemma 9.2.7

Per ogni $n \in \mathbb{N}$ gli unici numeri minori o uguali ad n in Q sono standard, cioè:

$$Q \vdash \forall a.(a \leq \overline{n}) \longleftrightarrow (a = 0 \vee a = s(0) \vee \cdots \vee a = \overline{n})$$

Dimostrazione. Procediamo per induzione su n:

- per il passo base con $n = 0$ dobbiamo dimostrare che

  $$Q \vdash \forall a.a \leq 0 \longleftrightarrow a = 0$$

  ovvero che

  $$Q \vdash \forall a.\exists x.x + a = 0 \longleftrightarrow a = 0$$

  e per assioma $a = 0$ oppure $\exists b.a = s(b)$, se $a = 0$ allora $a \leq 0$ mentre se $a = s(b)$ allora dato un qualunque x vale $x + a = s(a + b)$ ma sempre per assioma $s(a + b) \neq 0$, quindi Q dimostra il se e solo se

- per il passo induttivo con $n = m + 1$ dimostriamo che

  $$Q \vdash \forall a.(a \leq \overline{m+1}) \longleftrightarrow (a = 0 \vee \exists b.a = s(b) \wedge b \leq \overline{m}) \tag{9.2}$$

  infatti dimostrato questo possiamo usare l'ipotesi induttiva su m ottenendo che

  $$Q \vdash \forall a.(a \leq \overline{m+1}) \longleftrightarrow (a = 0 \vee \exists b.a = s(b) \wedge (b = 0 \vee \cdots \vee b = \overline{m}))$$

  ovvero

  $$Q \vdash \forall a.(a \leq \overline{m+1}) \longleftrightarrow (a = 0 \vee a = s(0) \vee \cdots \vee a = \overline{n})$$

quindi iniziamo con l'implicazione $\to$ della (9.2): supponendo che $\exists\, x.x + a = \overline{m} + 1$ se $a = 0$ non c'è niente da dimostrare, se invece $a \neq 0$ allora esiste b tale che $a = s(b)$ e rimane da dimostrare che $\exists\, y.y + b = \overline{m}$ e questo è verificato in quanto se $x + a = \overline{m+1}$ per costruzione $x + s(b) = \overline{m+1}$ allora $s(x + b) = \overline{m+1}$ quindi $x + b = \overline{m}$ ovvero possiamo scegliere $y = x$.

Per l'implicazione inversa supponendo che $a = 0 \vee \exists\, b.a = s(b) \wedge b \leq \overline{m}$ se $a = 0$ allora vale $a \leq \overline{m+1}$ altrimenti $\exists\, b.a = s(b) \wedge b \leq \overline{m}$ allora per definizione $\exists\, x.x + b = \overline{m}$ quindi applicando il successore si ricava che $\exists\, x.x + s(b) = s(\overline{m})$ $(= \overline{m+1})$.

□

Lemma 9.2.8

Dato un modello M di Q ed $\alpha \in M$ un numero non-standard, se $n \in \mathbb{N}$ allora $M \vDash \overline{n} \leq \alpha$.

Dimostrazione. Procediamo per induzione su n per dimostrare che dato un qualunque $\alpha \in M$ non-standard $M \vDash \exists\, x.x + \overline{n} = \alpha$:

- se $n = 0$ allora qualunque sia α è vero con $x = \alpha$;
- se $n = m + 1$ dove dato un qualunque γ non-standard $M \vDash \exists\, x.x + \overline{m} = \gamma$ allora essendo α non-standard per assioma α ammette un predecessore β (tale che $\alpha = s(\beta)$) e β è necessariamente non-standard (altrimenti α sarebbe standard) quindi per l'ipotesi induttiva $M \vDash \exists\, x.x + \overline{m} = \beta$ quindi per assioma $M \vDash \exists\, x.x + \overline{m+1} = s(\beta)$ dove $\overline{m+1} = \overline{n}$ e $s(\beta) = \alpha$.

□

Teorema 9.2.9

Data una formula aritmetica chiusa φ se φ è di classe Δ_0^0 allora φ è decidibile nella Q di Robinson e più precisamente

$$\mathbb{N} \vDash \varphi \iff Q \vdash \varphi$$
$$\mathbb{N} \vDash \neg\varphi \iff Q \vdash \neg\varphi$$

se invece φ è di classe Σ_1^0 allora vale soltanto[6]

$$\mathbb{N} \vDash \varphi \iff Q \vdash \varphi$$

Dimostrazione. Iniziamo dimostrando che se la formula chiusa φ è di classe Δ_0^0 allora

$$\mathbb{N} \vDash \varphi \iff Q \vdash \varphi$$
$$\mathbb{N} \vDash \neg\varphi \iff Q \vdash \neg\varphi$$

dove in realtà ci basta dimostrare che $\mathbb{N} \vDash \varphi \iff Q \vdash \varphi$ in quanto se φ è chiusa di classe Δ_0^0 allora anche $\neg\varphi$ è chiusa e di classe Δ_0^0, però esplicitiamo la negazione in quanto ci sarà utile nell'argomento per induzione.

È immediato che se $Q \vdash \varphi$ allora $\mathbb{N} \vDash \varphi$ e che se $Q \vdash \neg\varphi$ allora $\mathbb{N} \vDash \neg\varphi$ in quanto $\mathbb{N}$ è un modello di Q. Per l'altra implicazione procediamo per induzione strutturale su φ:

- Se φ è atomica allora per il lemma 9.2.5 se $\mathbb{N} \vDash \varphi$ allora $Q \vdash \varphi$ e se $\mathbb{N} \vDash \neg\varphi$ allora $Q \vdash \neg\varphi$.
- Se $\varphi \doteq \neg\psi$ ed $\mathbb{N} \vDash \varphi$ allora per definizione $\mathbb{N} \vDash \neg\psi$ e ψ è una formula chiusa Δ_0^0 quindi per ipotesi induttiva $Q \vdash \neg\psi (= \varphi)$, e se $\mathbb{N} \vDash \neg\varphi$ allora per definizione $\mathbb{N} \vDash \neg(\neg\psi)$ quindi per la semantica di Tarski $\mathbb{N} \vDash \psi$ da cui per ipotesi induttiva $Q \vdash \neg\varphi$.

[6] Dato che la negazione di una formula Δ_0^0 rimane Δ_0^0 allora potremmo omettere $\mathbb{N} \vDash \neg\varphi \iff Q \vdash \neg\varphi$ dal caso Δ_0^0 senza cambiare la tesi ma non vale la stessa cosa nel secondo caso, infatti la negazione di una formula di classe Σ_1^0 è invece di classe Π_1^0, nel caso di una formula φ di classe Σ_1^0 se $\mathbb{N} \vDash \neg\varphi$ il teorema ci dice soltanto che $Q \nvdash \varphi$ ed in generale da questo non segue che $Q \vdash \neg\varphi$

- Se $\varphi \doteq \psi_1 \wedge \psi_2$ ed $\mathbb{N} \vDash \varphi$ allora per la semantica di Tarski (2.1.2) valgono sia $\mathbb{N} \vDash \psi_1$ che $\mathbb{N} \vDash \psi_2$, sia ψ_1 che ψ_2 sono Δ_0^0 chiuse quindi per ipotesi induttiva valgono sia $Q \vdash \psi_1$ che $Q \vdash \psi_2$, quindi possiamo usare l'introduzione della congiunzione per ottenere che $Q \vdash \psi_1 \wedge \psi_2$. Se invece $\mathbb{N} \vDash \neg\varphi$ allora o $\mathbb{N} \vDash \neg\psi_1$ oppure $\mathbb{N} \vDash \neg\psi_2$, in entrambi i casi possiamo usare l'ipotesi induttiva ottenendo che $Q \vdash \neg\varphi$.

- Se $\varphi \doteq \psi_1 \vee \psi_2$ sappiamo che

  $$\vdash (\psi_1 \vee \psi_2) \longleftrightarrow \neg(\neg\psi_1 \wedge \neg\psi_2)$$

  ed essendo sia ψ_1 che ψ_2 formule Δ_0^0 chiuse possiamo usare i casi già dimostrati per ottenere che la tesi vale anche su φ.

- Se $\varphi \doteq \psi_1 \to \psi_2$ sappiamo che

  $$\vdash (\psi_1 \to \psi_2) \longleftrightarrow \neg(\psi_1 \wedge \neg\psi_2)$$

  ed essendo sia ψ_1 che ψ_2 formule Δ_0^0 chiuse possiamo usare i casi già dimostrati per ottenere che la tesi vale anche su φ.

- Se $\varphi \doteq \forall x \leq t.\psi$ allora essendo φ chiusa il terminte t è necessariamente chiuso, allora per il lemma 9.2.4 esiste $n \in \mathbb{N}$ tale che $\{\}_{\mathbb{N}}\, t = n$, quindi per il lemma 9.2.7 vale

  $$Q \vdash \varphi \longleftrightarrow \forall x.(x = 0 \vee x = s(0) \vee \cdots \vee x = \overline{n}) \to \psi$$

  ovvero

  $$Q \vdash \varphi \longleftrightarrow [(\forall x.x = 0 \to \psi) \wedge (\forall x.x = s(0) \to \psi) \wedge \cdots \wedge (\forall x.x = \overline{n} \to \psi)]$$

  e per ogni i la formula $\forall x.x = \overline{i} \to \psi$ equivale a $\psi\left[{}^{\overline{i}}/_{x}\right]$[7] quindi

  $$Q \vdash \varphi \longleftrightarrow \psi\left[{}^{0}/_{x}\right] \wedge \psi\left[{}^{s(0)}/_{x}\right] \wedge \cdots \wedge \psi\left[{}^{\overline{n}}/_{x}\right]$$

  dove tutte le $\psi\left[{}^{i}/_{x}\right]$ sono per costruzione formule chiuse, quindi ancora una volta possiamo usare i casi già dimostrati per ottenere che la tesi vale anche su φ.

- Se $\varphi \doteq \exists x \leq t.\psi$ allora come prima esiste $n \in \mathbb{N}$ tale che $\{\}_{\mathbb{N}}\, t = n$ e vale

  $$Q \vdash \varphi \longleftrightarrow \forall \exists .(x = 0 \vee x = s(0) \vee \cdots \vee x = \overline{n}) \wedge \psi$$

  ovvero

  $$Q \vdash \varphi \longleftrightarrow [(\exists x.x = 0 \wedge \psi) \vee (\exists x.x = s(0) \wedge \psi) \vee \cdots \vee (\exists x.x = \overline{n} \wedge \psi)]$$

  ed ancora come prima per ogni i la formula $\exists x.x = \overline{i} \wedge \psi$ equivale a $\psi\left[{}^{\overline{i}}/_{x}\right]$ quindi

  $$Q \vdash \varphi \longleftrightarrow \psi\left[{}^{0}/_{x}\right] \vee \psi\left[{}^{s(0)}/_{x}\right] \vee \ldots \psi\left[{}^{\overline{n}}/_{x}\right]$$

  dove tutte le $\psi\left[{}^{i}/_{x}\right]$ sono per costruzione formule chiuse, quindi ancora una volta possiamo usare i casi già dimostrati per ottenere che la tesi vale anche su φ.

Avendo dimostrato la tesi per le formule Δ_0^0 per concludere rimane da vedere quella per le formule Σ_1^0, ovvero che se φ è chiusa di classe Σ_1^0 allora

$$\mathbb{N} \vDash \varphi \iff Q \vdash \varphi$$

Per definizione della classe Σ_1^0 esiste $k \in \mathbb{N}$ tale che

$$\varphi = \exists x_1, \ldots, \exists x_k.\psi$$

dove ψ è di classe Δ_0^0 allora vediamo separatamente le due implicazioni:

[7] Data una qualunque struttura M vediamo che $M \vDash \forall x.x = \overline{i} \to \psi$ per la semantica di Tarski fissata una qualunque valutazione v questo equivale a dire che per ogni $a \in M$ vale $M \vDash \{v\left[{}^{a}/_{x}\right]\}\, x = \overline{i} \to \psi$ che per il lemma 2.2.3 equivale a dire che per ogni $a \in M$ vale $M \vDash \{v\}\, a = \overline{i} \to \psi\left[{}^{a}/_{x}\right]$, dato che con $a \neq 0$ questo è sempre vero allora $M \vDash \{v\}\, a = \overline{i} \to \psi\left[{}^{a}/_{x}\right]$ se e solo se $M \vDash \{v\}\, \psi\left[{}^{a}/_{x}\right]$, ma tale formula è chiusa quindi questo equivale a $M \vDash \psi\left[{}^{a}/_{x}\right]$

($\Longrightarrow$) se $\mathbb{N} \vDash \varphi$ allora per la semantica di Tarski esistono $n_1, \dots, n_k \in \mathbb{N}$ tali che

$$\mathbb{N} \vDash \left\{ {}^{n_1}\!/_{x_1}, \dots, {}^{n_k}\!/_{x_k} \right\}^{8} \psi$$

e per il lemma (2.2.3) questo vale se e solo se $\mathbb{N} \vDash \psi \left[{}^{\overline{n_1}}\!/_{x_1}, \dots, {}^{\overline{n_k}}\!/_{x_k} \right]$; per costruzione ψ è di classe Δ_0^0 e tutti i termini $\overline{n}$ sono chiusi, quindi da quanto appena dimostrato per le formule Δ_0^0 segue che $Q \vdash \psi \left[{}^{n_1}\!/_{x_1}, \dots, {}^{n_k}\!/_{x_k} \right]$, ed usando la regola di introduzione dell'esistenziale k volte da questo segue che $Q \vdash \varphi$;

($\Longleftarrow$) se invece $Q \vdash \varphi$ allora per completezza (5.4.2) $Q \vDash \varphi$ ed essendo $\mathbb{N}$ un modello di Q allora $\mathbb{N} \vDash \varphi$.

□

Corollario 9.2.9.1

Data una funzione $f : \mathbb{N}^k \to \mathbb{N}_\perp$ se f è ricorsiva allora esiste una formula aritmetica $\varphi(x_1, \dots, x_k, y)$ di classe Σ_1^0 tale che data una qualunque k-upla $(x_1, \dots, x_k) \in \mathbb{N}^k$

$$\forall\, y \in \mathbb{N}.\, (Q \vdash \varphi(\overline{x}_1, \dots, \overline{x}_k, \overline{y})) \iff y = f(x_1, \dots, x_k)$$

Dimostrazione. Dato che tutte le funzioni ricorsive sono Σ_1^0 (9.1.2) esiste una formula φ di classe Σ_1^0 tale che data una qualunque k-upla $(x_1, \dots, x_k) \in \mathbb{N}^k$ e dato un qualunque $y \in \mathbb{N}$ vale

$$\mathbb{N} \vDash \varphi(x_1, \dots, x_k, y) \quad \iff \quad y = f(x_1, \dots, x_k)$$

e per come abbiamo definito i numerali

$$\mathbb{N} \vDash \varphi(x_1, \dots, x_k, y) \quad \iff \quad \mathbb{N} \vDash \varphi(\overline{x}_1, \dots, \overline{x}_k, \overline{y})$$

e φ dove sostituiamo questi numerali è una formula Σ_1^0 chiusa, quindi questo vale se e solo se $Q \vdash \varphi(\overline{x}_1, \dots, \overline{x}_k, \overline{y})$ □

Per le funzioni ricorsive totali vale una forma più forte dell'enunciato precedente:

Lemma 9.2.10

Data una funzione $f : \mathbb{N}^k \to \mathbb{N}$ se f è ricorsiva totale allora esiste una formula aritmetica φ di classe Σ_1^0 tale che data una qualunque k-upla $(x_1, \dots, x_k) \in \mathbb{N}^k$

$$Q \vdash \forall\, y. \varphi(\overline{x}_1, \dots, \overline{x}_k, y) \longleftrightarrow y = \overline{f(x_1, \dots, x_k)} \tag{9.3}$$

Dimostrazione. Una idea per dimostrare questo lemma può essere di rifare la dimostrazione del lemma sulla corrispondenza delle funzioni ricorsive con formule Σ_1^0 (9.1.2) tenendo traccia di quello che questo risultato richiede in più. Cerchiamo invece di dimostrarlo tramite un'altra strada.

Per il corollario precedente (9.2.9.1) esiste una formula aritmetica ψ di classe Σ_1^0 tale che data una qualunque k-upla $(x_1, \dots, x_k) \in \mathbb{N}^k$ ed un qualunque $y \in \mathbb{N}$ vale

$$(Q \vdash \psi(\overline{x}_1, \dots, \overline{x}_k, \overline{y})) \iff y = f(x_1, \dots, x_k)$$

e per costruzione ψ è della forma

$$\psi \doteq \exists\, z_1, \dots, \exists\, z_h. \theta(z_1, \dots, z_h, x_1, \dots, x_k, y)$$

dove $h \in \mathbb{N}$ e θ è di classe Δ_0^0.

Notiamo che questa non è necessariamente la formula che richiede il teorema in quanto fissato un modello di Q potrebbe esiste un altro y tale che $\psi(\overline{x}_1, \dots, \overline{x}_k, y)$ (anche se necessariamente questo altro y deve essere non-standard).

[8] abbiamo omesso la valutazione delle variabili v in quanto per ipotesi $\mathrm{vl}(\psi) \subseteq x_1, \dots, x_k$ quindi la valutazione di ψ in $\mathbb{N}$ dipende al più dall'assegnazione di queste variabili in v (2.1.3)

Costruiamo la formula aritmetica φ come

$$\varphi \doteq \exists N. \left(\overbrace{y \leq N \wedge \exists z_1 \leq N, \dots, \exists z_h \leq N. \theta(z_1, \dots, z_h, x_1, \dots, x_k, y)}^{\varphi_1(x_1,\dots,x_k,y,N)} \right) \wedge \\ \wedge \left(\overbrace{\forall z_1 \leq N, \dots, \forall z_h \leq N. \forall t \leq N. \theta(z_1, \dots, z_h, x_1, \dots, x_k, t) \to t = y}^{\varphi_2(x_1,\dots,x_k,y,N)} \right)$$

e cerchiamo di vedere che questa φ soddisfa la tesi (9.3).

Iniziamo con l'implicazione $\to$ supponendo per assurdo che esistano $(x_1, \dots, x_k) \in \mathbb{N}^k$ tali che

$$Q \nvdash \forall y. \varphi(\overline{x}_1, \dots, \overline{x}_k, y) \longrightarrow y = \overline{f(x_1, \dots, x_k)}$$

allora per la contronominale del teorema di completezza (5.4.2) deve esistere una struttura $M \vDash Q$ tale che

$$M \vDash \neg \forall y. \varphi(\overline{x}_1, \dots, \overline{x}_k, y) \longrightarrow y = \overline{f(x_1, \dots, x_k)}$$

ovvero tale che esiste $\alpha \in M$ per cui

$$M \vDash \neg \left[\varphi(\overline{x}_1, \dots, \overline{x}_k, \alpha) \longrightarrow \alpha = \overline{f(x_1, \dots, x_k)} \right]$$

ed essendo φ con le attuali sostituzioni una formula chiusa per la semantica di Tarski questo equivale a dire che esiste $\alpha \in M$ per cui

$$M \vDash \varphi(\overline{x}_1, \dots, \overline{x}_k, \alpha) \qquad \text{e} \qquad M \vDash \neg \alpha = \overline{f(x_1, \dots, x_k)} \tag{9.4}$$

dove la prima per costruzione equivale a dire che $M \vDash \exists N. \varphi_1(\dots) \wedge \varphi_2(\dots)$, quindi per la semantica di Tarski possiamo fissare $\beta \in M$ tale che

$$M \vDash \varphi_1(\overline{x}_1, \dots, \overline{x}_k, \alpha, \beta) \wedge \varphi_2(\overline{x}_1, \dots, \overline{x}_k, \alpha, \beta)$$

da qua per proseguire distinguiamo i casi in cui β è:

standard (in questo caso vogliamo sfruttare che $M \vDash \varphi_1$) allora per definizione esiste $n \in \mathbb{N}$ tale che $M \vDash \beta = \overline{n}$ ed per eliminazione dell'uguaglianza vale $M \vDash \varphi_1(\overline{x}_1, \dots, \overline{x}_k, \alpha, \overline{n})$ ovvero per costruzione

$$M \vDash \alpha \leq \overline{n} \wedge \exists z_1 \leq \overline{n}, \dots, \exists z_h \leq \overline{n}. \theta(z_1, \dots, z_h, x_1, \dots, x_k, \alpha)$$

quindi per il lemma 9.2.7 α è standard e possiamo scegliere tutti gli z_i standard in M ottenendo quindi che $M \vDash \theta(\overline{z}_1, \dots, \overline{z}_h, \overline{x}_1, \dots, \overline{x}_k, \overline{\alpha})$ e θ con queste sostituzioni è chiusa di classe Δ_0^0 quindi per la proposizione 9.1.5 θ è decidibile in Q; distinguiamo quindi i due sottocasi:

- se $Q \vdash \theta(\overline{z}_1, \dots, \overline{z}_h, \overline{x}_1, \dots, \overline{x}_k, \overline{\alpha})$ per costruzione di θ allora $\alpha = f(x_1, \dots, x_k)$ ma questo contraddice la (9.4)
- altrimenti $Q \vdash \neg\theta(\overline{z}_1, \dots, \overline{z}_h, \overline{x}_1, \dots, \overline{x}_k, \overline{\alpha})$ ma questo è assurdo perché $M \vDash Q$.

non-standard (in questo caso vogliamo sfruttare che $M \vDash \varphi_2$) per definizione di φ_2 vale

$$M \vDash \forall z_1 \leq \beta, \dots, \forall z_h \leq \beta. \forall t \leq \beta. \theta(z_1, \dots, z_h, x_1, \dots, x_k, t) \to t = \alpha \tag{9.5}$$

e per definizione di θ esistono $z_1, \dots, z_h \in \mathbb{N}$ tali che

$$M \vDash \theta(\overline{z}_1, \dots, \overline{z}_h, \overline{x}_1, \dots, \overline{x}_h, \overline{f(x_1, \dots, x_h)})$$

(con $f(x_1, \dots, x_h)$ per definizione anch'esso standard) e tutti i numeri standard sono minori del numero non-standard β (9.2.8) quindi soddisfano le ipotesi della implicazione in (9.5) ovvero deve valere

$$M \vDash y = \overline{f(x_1, \dots, x_h)}$$

ma anche questo è assurdo perché contraddice la (9.4).

Per l'altra implicazione ($\leftarrow$) della tesi (9.3) fissato $y \in M$ tale che $y = \overline{f(x_1, \dots, x_k)}$ dobbiamo dimostrare che $Q \vdash \varphi(\overline{x}_1, \dots, \overline{x}_k, y)$, ovvero che

$$Q \vdash \varphi(\overline{x}_1, \dots, \overline{x}_k, \overline{f(x_1, \dots, x_k)})$$

quindi dobbiamo trovare $\beta \in M$ tale che $Q \vdash \varphi_1(\dots, \beta) \wedge \varphi_2(\dots, \beta)$.

Per costruzione di θ sappiamo che

$$Q \vdash \exists\, z_1, \dots, \exists\, z_h \theta(z_1, \dots, z_h, \overline{x}_1, \dots, \overline{x}_k, \overline{f(x_1, \dots, x_k)})$$

ed $\mathbb{N} \vDash Q$, quindi esistono $z_1, \dots, z_h \in \mathbb{N}$ tali che

$$\mathbb{N} \vDash \theta(\overline{z}_1, \dots, \overline{z}_h, \overline{x}_1, \dots, \overline{x}_k, \overline{f(x_1, \dots, x_k)})$$

e questa formula è chiusa di classe Δ_0^0 quindi è decisa da Q.

Dato che $\mathbb{N} \vDash Q$ necessariamente la formula decisa da Q deve essere vera, ovvero

$$Q \vdash \theta(\overline{z}_1, \dots, \overline{z}_h, \overline{x}_1, \dots, \overline{x}_k, \overline{f(x_1, \dots, x_k)})$$

e possiamo porre

$$\beta \doteq \max(x_1, \dots, x_k, z_1, \dots z_h, f(x_1, \dots, x_k)) \in \mathbb{N}$$

ottenendo che β è standard e per costruzione che vale $Q \vdash \varphi_1(\overline{x}_1, \dots \overline{x}_k, \overline{f(x_1, \dots, x_k)}, \overline{\beta})$.

Sempre con lo stesso β rimane da verificare che Q dimostra anche φ_2 ovvero dobbiamo vedere che dato un qualunque modello M di Q

$$M \vDash \forall\, z_1 \leq \overline{\beta}, \dots, \forall\, z_h \leq \overline{\beta}. \forall\, t \leq \overline{\beta}. \theta(z_1, \dots, z_k, \overline{x}_1, \dots, \overline{x}_k, t) \to t = \overline{f(x_1, \dots, x_k)}$$

cioè dati qualunque $z_1, \dots z_k, t \in M$ dobbiamo mostrare che se

$$M \vDash z_1 \leq \overline{\beta} \wedge \dots \wedge z_h \leq \overline{\beta}. t \leq \overline{\beta}. \theta(z_1, \dots, z_k, \overline{x}_1, \dots, \overline{x}_k, t)$$

allora $M \vDash t = \overline{f(x_1, \dots, x_k)}$.

Se $M \vDash z_1 \leq \overline{\beta} \wedge \dots \wedge z_h \leq \overline{\beta}. t \leq \overline{\beta}$ allora tutti gli z_i e t sono elementi standard di M (9.2.7) e quindi

$$M \vDash \theta(\overline{z}_1, \dots, \overline{z}_k, \overline{x}_1, \dots, \overline{x}_k, \overline{t})$$

ovvero per costruzione di θ vale $M \vDash \overline{t} = \overline{f(x_1, \dots, x_k)}$. □

Corollario 9.2.10.1

Data la formula φ del lemma precedente (9.2.10) e data una qualunque k-upla $(x_1, \dots, x_k) \in \mathbb{N}^k$

$$Q \vdash \exists!\, y. \varphi(\overline{x}_1, \dots, \overline{x}_k, y)$$

Dimostrazione. Essendo f ricorsiva totale tale y deve esistere, per quanto visto fino ad ora dato un qualunque modello di Q tale y nel modello deve essere standard e per costruzione di φ non possono esistere due soluzioni standard diverse per y altrimenti f non sarebbe una funzione. □

Capitolo 10

Il teoremi di incompletezza di Gödel

La forma più semplice per il primo teorema di incompletezza di Gödel è la seguente

Teorema 10.0.1

La teoria PA dell'aritmetica di Peano al primo ordine è una teoria incompleta.

L'idea dietro la sua dimostrazione è di costruire una formula aritmetica che dice 'io non sono dimostrabile' e da questa costruire un paradosso, infatti se PA fosse completa dovrebbe decidere questa formula, se fosse vera allora dal teorema di completezza (5.4.2) si ricava una contraddizione, se fosse falsa invece la contraddizione viene dal teorema di correttezza (4.2.1).

10.1 Numerazione di Gödel

Per fare questo dobbiamo per prima cosa fare in modo che PA, quindi che il linguaggio dell'aritmetica, sia in grado di parlare delle formule, per fare questo associamo ad ogni formula aritmetica un numero; qualunque maniera ragionevole di fare questa associazione si dice *numerazione di Gödel*.

Noi daremo questa numerazione in maniera ricorsiva sulla struttura delle formule, a partire da una numerazione per i simboli del linguaggio dell'aritmetica, per le variabili e poi per i termini.

L'alfabeto delle formule aritmetiche è composto da: i simboli logici di base (che possiamo ricondurre ai soli $\neg, \to, \forall, =$), dai simboli propriamente del linguaggio $(0, s, +, \cdot)$, e dai numerabili simboli delle varie variabili (gli x_i con $i \in \mathbb{N}$). Possiamo ad esempio scegliere la seguente numerazione

$\bot$	$\to$	$\forall$	$=$	0	s	$+$	$\cdot$	x_i
0	1	2	3	4	5	6	7	$8+i$

ed indichiamo la numerazione con il simbolo $\#$[1] in questo modo il nostro 'alfabeto' sarà tutto $\mathbb{N}$ in cui i simboli e le variabili corrispondono a numeri univoci.

Dalla numerazione dei simboli definiamo ricorsivamente la numerazione dei termini $\ulcorner t \urcorner$:

- se t è un termine atomico allora $t \doteq 0$ oppure $t \doteq x_i$ per qualche i, e poniamo

$$\ulcorner 0 \urcorner \doteq \langle \#0 \rangle \qquad \text{e} \qquad \ulcorner x_i \urcorner = \langle \# x_i \rangle$$

- se $t \doteq s(t_1)$ allora $\ulcorner t \urcorner = \langle \#s, \ulcorner t_1 \urcorner \rangle$
- se $t \doteq t_1 + t_2$ allora $\ulcorner t \urcorner = \langle \#+, \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle$
- se $t \doteq t_1 \cdot t_2$ allora $\ulcorner t \urcorner = \langle \#\cdot, \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle$

Analogamente per ricorsione definiamo la numerazione delle formule $\ulcorner \varphi \urcorner$:

- se φ è una formula aritmetica atomica allora $\varphi \doteq t_1 = t_2$ oppure $\varphi \doteq \bot$ e poniamo

$$\ulcorner t_1 = t_2 \urcorner = \langle \# =, \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle \qquad \text{e} \qquad \ulcorner \bot \urcorner = \langle \# \bot \rangle$$

[1] per non confondere i codici di 0 e delle variabili con quelli dei corrispondenti termini atomici che saranno indicati con la notazione più standard $\ulcorner \cdot \urcorner$ che abbiamo usato anche per il codice delle funzioni

- se $\varphi \doteq \psi_1 \to \psi_2$ allora poniamo $\ulcorner\varphi\urcorner = \langle \#\to, \ulcorner\psi_1\urcorner, \ulcorner\psi_2\urcorner\rangle$
- se $\varphi \doteq \forall x_i.\psi$ allora poniamo $\ulcorner\varphi\urcorner = \langle \#\forall, \#x_i, \ulcorner\psi\urcorner\rangle$

Osservazione 10.1.1 Per costruzione questa numerazione è iniettiva, date due formule diverse hanno ovviamente numerazioni diverse.

10.2 Il lemma di diagonalizzazione di Gödel

Proseguiamo mostrando che alcune operazioni sulle codifiche sono computabili, con l'obbiettivo di dimostrare il lemma di diagonalizzazione di Gödel (10.2.4), che potremmo interpretare come una 'versione per le formule' del teorema di punto fisso (8.1.3).

Lemma 10.2.1

Il predicato

$$For(n) \quad \doteq \quad \exists \varphi.\, n = \ulcorner\varphi\urcorner$$

è primitivo ricorsivo.

Dimostrazione. Costruiamo prima un predicato $Term(n)$ che dice se n è la numerazione di un termine, per fare questo basta porre $Term(n)$ vero se e solo se valgono le seguenti

$$n \text{ è una lista non vuota} \quad (\longleftrightarrow n \neq 0)$$
$$\begin{cases} len(n) = 1 \land car(n) = \#0 \\ len(n) = 1 \land car(n) \geq 8 \\ len(n) = 2 \land car(n) = \#s \quad \land Term(nth(n,2)) \\ len(n) = 3 \land car(n) = \#+ \quad \land Term(nth(n,2)) \land\ Term(nth(n,3)) \\ len(n) = 3 \land car(n) = \#\cdot \quad \land Term(nth(n,2)) \land\ Term(nth(n,3)) \end{cases}$$

che è possibile fare in maniera primitiva ricorsiva in quanto dentro la definizione stiamo applicando la funzione sempre a numeri strettamente minori di n.

Analogamente a partire da $Term$ definiamo For ponendo che $For(n)$ è vero se e solo se

$$n \text{ è una lista non vuota} \quad (\longleftrightarrow n \neq 0)$$
$$\begin{cases} len(n) = 1 \land car(n) = \#\bot \\ len(n) = 3 \land car(n) = \#= \quad \land Term(nth(n,2)) \land\ Term(nth(n,3)) \\ len(n) = 3 \land car(n) = \#\to \quad \land For(nth(n,2)) \land\ For(nth(n,3)) \\ len(n) = 3 \land car(n) = \#\forall \quad \land nth(n,2) \geq 8 \land\ For(nth(n,3)) \end{cases}$$

□

Lemma 10.2.2

La funzione $Num : \mathbb{N} \to \mathbb{N}$ tale che per ogni $n \in \mathbb{N}$ vale $Num(n) = \ulcorner\overline{n}\urcorner$ è primitiva ricorsiva.

Dimostrazione. Possiamo definire per ricorsione primitiva

$$Num(0) = \ulcorner 0 \urcorner$$
$$Num(n+1) = \langle \#s, Num(n)\rangle$$

□

Lemma 10.2.3

La funzione $Sub : \mathbb{N}^3 \to \mathbb{N}$ tale che data la tripla $(\ulcorner\varphi\urcorner, i, \ulcorner t\urcorner) \in \mathbb{N}^3$ sostituisce t ad x_i in φ, ovvero

$$Sub(\ulcorner\varphi\urcorner, i, \ulcorner t\urcorner) = \ulcorner \varphi \left[{}^{t}\!/_{x_i}\right] \urcorner$$

è primitiva ricorsiva[2].

Dimostrazione. Definiamo $Sub(n,i,m)$ in maniera primitiva ricorsiva ponendo $Sub(n,i,m) = 0$ se vale $\neg(For(n) \wedge Term(m))$, altrimenti n è ben formato come formula oppure come termine ed allora procediamo per casi:

$$\begin{cases} n & \text{se } car(n) = \#\bot \\ \langle \# \to, Sub(nth(n,2),i,m), Sub(nth(n,3),i,m)\rangle & \text{se } car(n) = \# \to \\ n & \text{se } car(n) = \#\forall \wedge nth(n,2) = 8+i \\ \langle \#\forall, Sub(nth(n,2),i,m), Sub(nth(n,3),i,m)\rangle & \text{se } car(n) = \#\forall \wedge nth(n,2) \neq 8+i \\ \langle \# =, Sub(nth(n,2),i,m), Sub(nth(n,3),i,m)\rangle & \text{se } car(n) = \# = \\ n & \text{se } car(n) = \#0 \\ \langle \#s, Sub(nth(n,2),i,m)\rangle & \text{se } car(n) = \#s \\ \langle \#+, Sub(nth(n,2),i,m), Sub(nth(n,3),i,m)\rangle & \text{se } car(n) = \#+ \\ \langle \#\cdot, Sub(nth(n,2),i,m), Sub(nth(n,3),i,m)\rangle & \text{se } car(n) = \#\cdot \\ m & \text{se } car(n) = 8+i \\ n & \text{se } car(n) \geq 8 \wedge car(n) \neq 8+i \end{cases}$$

□

Lemma 10.2.4: *di diagonalizzazione di Gödel*

Data una formula aritmetica φ esiste ψ tale che

$$Q \vdash \psi \longleftrightarrow \varphi\left[{}^{\overline{\ulcorner\psi\urcorner}}\!/_{x_1}\right] \tag{10.1}$$

dove indicheremo $\varphi\left[{}^{x}\!/_{x_1}\right]$ con $\varphi(x)$ e quindi $Q \vdash \psi \longleftrightarrow \varphi(\overline{\ulcorner\psi\urcorner})$

Sfrutteremo questo lemma per dire che se φ è una formula che dice 'x è il codice di una formula non dimostrabile' allora esiste ψ formula che dice 'io non sono dimostrabile'.

Dimostrazione. L'idea è analoga a quella della dimostrazione del teorema del punto fisso[3] (8.1.3).In particolare informalmente stiamo cercando una formula ψ tale che $\psi = \varphi(\psi)$, partiremo costruendo una formula f tale che $f(x) = x(x)$ e poi una formula $\theta = \varphi(f(x))$, in questo modo applicando θ a se stessa (sempre in questa notazione informale) si ottiene che

$$\theta(\theta) = \varphi(f(\theta)) = \varphi(\theta(\theta))$$

cioè $\theta(\theta)$ sarebbe effettivamente la ψ cercata.

Per la dimostrazione è importante che fissiamo la variabile ad una specifica x_1 invece che una generica x_i (anche se poi chiaramente il teorema sarà vero anche per variabili generiche a meno di rinorminarle) in quanto avremo bisogno dei codici delle formule e rinominando le variabili cambia il codice della funzione; sempre per lo stesso motivo fissiamo $x_k \notin \mathrm{vl}\,\varphi \cup \{x_1\}$.

Per costruire $f : \mathbb{N} \to \mathbb{N}$ tale che

$$f(\ulcorner\alpha\urcorner) = \ulcorner\, \alpha\left[{}^{\overline{\ulcorner\alpha\urcorner}}\!/_{x_k}\right] \urcorner$$

[2] È irrilevante cosa succede nelle triple che non sono della forma $(\ulcorner\varphi\urcorner, i, \ulcorner t\urcorner)$, però grazie a For e $Term$ del lemma precedente (10.2.1) possiamo porre ad esempio $Sub = 0$ in tali casi in maniera primitiva ricorsiva

[3] Cronologicamente questo lemma viene prima del teorema del punto fisso, quindi potremmo dire che la dimostrazione del teorema del punto fisso è analoga a questa

in maniera primitiva ricorsiva per i lemmi precedenti 10.2.2 e 10.2.3 basta porre:

$$f(x) \doteq Sub(x, k, Num(x))$$

ed essendo primitiva ricorsiva f è ricorsiva totale, quindi possiamo usare il lemma 9.2.10 ottenendo che esiste una formula artimetica $\pi(x_k, x_1)$ di classe Σ_1^0 tale che

$$\forall x \in \mathbb{N}. Q \vdash \forall x_1.\pi \left[\overline{x}/x_k\right] \longleftrightarrow x_1 = \overline{f(x)} \tag{10.2}$$

Adesso definiamo le formule aritmetiche θ e ψ che avevamo nominato in precedenza ponendo

$$\theta \doteq \forall x_1.\pi \to \varphi$$
$$\psi \doteq \theta \left[\overline{\ulcorner\theta\urcorner}/x_k\right]$$

e cerchiamo di dimostrare che effettivamente vale la tesi (10.1) con la ψ così costruita.

Per definizione

$$\psi \equiv \forall x_1.\pi \left[\overline{\ulcorner\theta\urcorner}/x_k\right] \to \varphi \left[\overline{\ulcorner\theta\urcorner}/x_k\right]$$

e per costruzione $x_k \notin \mathrm{vl}\,\varphi$, allora

$$\psi \equiv \forall x_1.\pi \left[\overline{\ulcorner\theta\urcorner}/x_k\right] \to \varphi$$

inoltre fissando $x_1 = \ulcorner\theta\urcorner$ nella (10.2) tramite l'eliminazione del quantificatore esistenziale si ottiene che

$$Q \vdash \pi \left[\overline{\ulcorner\theta\urcorner}/x_k\right] \longleftrightarrow x_1 = \overline{f\left(\ulcorner\theta\urcorner\right)}$$

cioè nella teoria Q possiamo sostituire $x_1 = \overline{f\left(\ulcorner\theta\urcorner\right)}$ a $\pi \left[\overline{\ulcorner\theta\urcorner}/x_k\right]$, ed applicando questa sostituzione nella definizione di $\psi = \forall x_1.\pi \left[\overline{\ulcorner\theta\urcorner}/x_k\right] \to \varphi$ (dove non dobbiamo sostituire $\overline{\ulcorner\theta\urcorner}$ ad x_k in φ perché avevamo scelto $x_k \notin \mathrm{vl}(\varphi)$) si ottiene che

$$Q \vdash \psi \longleftrightarrow \left(\forall x_1.x_1 = \overline{f\left(\ulcorner\theta\urcorner\right)} \to \varphi\right)$$

e quindi[4]

$$Q \vdash \psi \longleftrightarrow \varphi \left[\overline{f\left(\ulcorner\theta\urcorner\right)}/x_1\right]$$

e rimane da verificare soltanto che $f\left(\ulcorner\theta\urcorner\right) = \ulcorner\psi\urcorner$; ed effettivamente per costruzione

$$f\left(\ulcorner\theta\urcorner\right) = Sub(\ulcorner\theta\urcorner, k, Num(\ulcorner\theta\urcorner)) = \ulcorner\theta\left[\overline{\ulcorner\theta\urcorner}/x_k\right]\urcorner = \ulcorner\psi\urcorner$$

□

10.3 Il primo teorema di incompletezza

Costruiremo un predicato $Dim_T(x, y)$ che dirà 'x è una dimostrazione di y nella teoria T', vedremo che questo si può fare sfruttando le proprietà delle teorie ricorsivamente assiomatizzabili (come ad esempio Q o PA).

Con questo dimostreremo che se $T \supseteq Q$ è una teoria ricorsivamente assiomatizzata che ha $\mathbb{N}$ come modello allora T è incompleta.

L'idea della dimostrazione è di usare il lemma di diagonalizzazione (10.2.4) per dire che esiste una formula ψ

$$Q \vdash \psi \longleftrightarrow \neg\exists x.Dim_Q(x, \ulcorner\psi\urcorner)$$

essendo a sua volta ψ una formula aritmetica potremmo chiederci se sia dimostrabile oppure no ottenendo un assurdo.

[4] è facile dimostrare che se $x \notin \mathrm{vl}(t)$ allora $\vdash (\forall x.x = t \to \varphi) \longleftrightarrow \varphi(t)$

Definizione 10.3.1: *Teoria ricorsivamente assiomatizzata*

Una teoria T si dice *ricorsivamente assiomatizzata* da P se P è un predicato ricorisivo[5] tale che

$$\varphi \in T \quad \iff \quad N \vDash P(\ulcorner \varphi \urcorner)$$

e più in generale se esiste un tale P si dice che T è *ricorsivamente assiomatizzabile*.

Esercizio 10.1 Mostrare che se T è una teoria semidecidibile allora esiste una teoria T' ricorsivamente assiomatizzabile tale che T' è equivalente a T.

Svolgimento. Se T è semidecidibile allora fissiamo una sua enumerazione ricorsiva (8.2.2) ovvero una funzione $f : \mathbb{N} \to \mathbb{N}$ ricorsiva totale tale che $T = \{\varphi_1, \varphi_2, \ldots\}$ dove per ogni i vale $\ulcorner \varphi_i \urcorner = f(i)$.

Chiaramente la teoria T' definita come

$$T' = \{\varphi_1 \\ \varphi_2 \wedge \varphi_2 \\ \varphi_2 \wedge \varphi_3 \wedge \varphi_3 \\ \vdots\}$$

è equivalente a T, in quanto è ovvio che ogni elemento di ognuna delle due è dimostrabile a partire dall'altra teoria.

Inoltre T' è ricorsivamente assiomatizzabile infatti data una formula φ possiamo verificare in maniera ricorsiva totale il massimo numero $n \in \mathbb{N}$ tale che φ è una congiunzione di n componenti ψ_φ tutte uguali fra loro; in questo modo con al più n applicazioni di φ possiamo verificare se $\varphi \in T'$ oppure no, cioè T' è decidibile quindi è ricorsivamente assiomatizzabile. □

Lemma 10.3.2

Data una teoria T ricorsivamente assiomatizzabile esiste un predicato ricorsivo $Dim_T(x, y)$ tale che

$$T \vdash \varphi \quad \iff \quad \mathbb{N} \vDash \exists\, d. Dim_T(d, \ulcorner \varphi \urcorner)$$

Dimostrazione più semplice valida per sistemi di deduzione alla Hilbert[6]. Diciamo che una sequenza $\langle \varphi_0, \ldots, \varphi_n \rangle$ è una dimostrazione di φ se:

- $\varphi_n = \varphi$
- per ogni $i \in \mathbb{N}$ o φ_i è un assioma o φ_i si ottiene dalle precedenti mediante una regola di deduzione.

dato che T è ricorsivamente assiomatizzabile questo si può verificare in maniera ricorsiva totale, quindi possiamo definire il predicato $Dim_T(d, \ulcorner \varphi \urcorner)$ come vero se valgono entrambe le condizioni:

$$nth(d, len(d)) = \ulcorner \varphi \urcorner$$
$$\forall\, i \leq d. i \leq len(d) \to \begin{cases} \varphi_i \text{ è un assioma} & \vee \\ \varphi_i \text{ si ottiene dalle precedenti mediante una regola di deduzione} \end{cases}$$

dove usiamo φ_i per indicare $nth(d, i)$.

Infatti per ipotesi è possibile verificare in maniera ricorsiva totale se φ_i è un assioma e possiamo scrivere che φ_i si ottiene dalle formule precedenti mediante una regola di deduzione come una disgiunzione

[5] In realtà non abbiamo detto cosa sia un predicato ricorsivo; la definizione di predicato ricorsivo non è ottenuta adattando la definizione che abbiamo usato per i predicati primitivi ricorsivi (7.1.2) ma invece è ottenuta adattando la definizione che dice che la funzione caratteristica è primitiva ricorsiva; queste due sono equivalenti nel caso di primitivo ricorsivo (dall'osservazione 7.1.3) ma non nel caso ricorsivo generale, infatti con questa definizione P è ricorsivo se e solo se è decidibile, con l'altra sarebbe solo nel caso semidecidibile, dall'esercizio seguente però segue che in questo caso particolare in cui P è una teoria non c'è differenza in quanto se la teoria è ricorsivamente enumerabile possiamo costruire una teoria equivalente che sia decidibile

[6] a differenza del sistema di deduzione naturale che abbiamo usato noi in un sistema di deduzione alla Hilbert la teoria presente nelle premesse non cambia mai

con tanti termini quante sono le regole e dove ad ogni regola corrisponde una formula Δ_0^0 che verifica che tra le formule precedenti c'è una combinazione valida che permette di usare la regola ottenendo φ_i. Ad esempio all'eliminazione dell'implicazione (il modus ponens) corrisponde la formula

$$\exists\, j < i . \exists\, k < i .\ulcorner \varphi_k \urcorner = \langle 1, \#\to, \ulcorner \varphi_j \urcorner, \ulcorner \varphi_i \urcorner \rangle$$

Esercizio 10.2 Esplicitare la formula per l'eliminazione dell'esistenziale
(Suggerimento: bisognerà trovare un modo per descrivere il fatto che per qualche formula ψ vale $\varphi_i = \psi\left[{}^{t}/_{x_k}\right]$ in maniera ricorsiva, per fare questo riguardare la definizione delle sostituzioni (2.2.2) notando che è una definizione ricorsiva)

□

Dimostrazione che funziona in deduzione naturale. Diciamo che una sequenza $\langle a_0, \dots, a_n \rangle$ è una dimostrazione di φ a partire da T se:

- $a_n = (p_n, \ulcorner \varphi \urcorner)$ dove p_n è una lista di regole contenute in T e $\ulcorner \varphi \urcorner$ è la numerazione di Gödel di φ;
- per ogni $m \leq n$ vale $a_m = (p_m, \ulcorner \varphi_m \urcorner)$ dove interpretando p_m come una lista di premesse la cui conclusione è φ_m si può ricavare $p_m \vdash \varphi_m$ tramite applicazione di una regola di deduzione le cui premesse sono tutte elementi che precedono a_m nella lista.

dato che T è ricorsivamente assiomatizzabile questo si può verificare in maniera ricorsiva totale, in particolare possiamo definire il predicato $Dim_T(d, \ulcorner \varphi \urcorner)$ come vero se valgono tutte e tre le condizioni:

$$crd(nth(d, len(d))) = \ulcorner \varphi \urcorner$$
$$\forall\, i \leq d . i \leq len(car(nth(d, len(d)))) \to nth(car(nth(d, len(d))), i) \in T$$
$$\forall\, i \leq d . i \leq len(d) \to car(nth(d, i)) \vdash cdr(nth(d, i)) \quad \begin{array}{l}\text{si ottiene dalle precedenti}\\ \text{mediante una regola di deduzione}\end{array}$$

Infatti la prima condizione è chiaramente primitiva ricorsiva, la seconda è ricorsiva totale supponendo che T se T è ricorsivamente assiomatizzabile quindi rimane solo da vedere come descrivere in maniera Δ_0^0 che a_i 'si ottiene dalle precedenti mediante una regola di deduzione'.

Fissato i per fare questo basta dire che

$$\forall\, i \leq d . For(cdr(nth(d, i)))$$

per ottenere che tutte le conclusioni devono essere formule valide, poi che

$$\forall\, i \leq d . \forall\, j \leq d . j \leq len(car(nth(d, i))) \to For(nth(car(nth(d, i)), j))$$

per ottenere che tutte le premesse sono liste di formule valide e poi tramite una disgiunzione vedere si applica una qualche delle seguenti formule Δ_0^0 (senza perdita di generalità riduciamoci al sistema di deduzione ridotto; per semplificare la notazione abbreviamo $a_i = (p_i, \ulcorner \varphi_i \urcorner)$ e per dire che due liste a, b hanno gli stessi elementi a meno di permutazioni diciamo $equal(a, b)$):

- per la regola di assioma:
$$len(p_i) = 1 \wedge nth(p_i, 1) = \ulcorner \varphi_i \urcorner$$
- per la regola di indebolimento:
$$\exists\, j < i . \ulcorner \varphi_i \urcorner = \ulcorner \varphi_j \urcorner \wedge \forall\, k \leq len(p_j) . \exists\, h \leq len(p_i) . nth(p_j, k) = nth(p_i, h)$$
- per la regola di riduzione ad assurdo:
$$\exists\, j < i . \ulcorner \varphi_j \urcorner = \ulcorner \bot \urcorner \wedge \exists\, k \leq len(p_j) . nth(p_j, k) = \langle \#\to, \ulcorner \varphi_i \urcorner, \bot \rangle \wedge equal(p_i, rem_{len(p_j),k}(p_j))$$
- per la regola di introduzione dell'implicazione
$$\exists\, a \leq d, \exists\, b \leq d . \ulcorner \varphi_i \urcorner = \langle \#\to, a, b \rangle \wedge$$
$$\wedge \exists\, j < i . \ulcorner \varphi_j \urcorner = b \wedge \exists\, k \leq len(p_j) . nth(p_j, k) = a \wedge equal(p_i, rem_{len(p_j),k}(p_j))$$

- per la regola di eliminazione dell'implicazione

$$\exists\, j < i, \exists\, k < i.equal(p_i, p_j) \wedge equal(p_k, p_j) \wedge \ulcorner \varphi_j \urcorner = \langle \#\to, \ulcorner \varphi_k \urcorner, \ulcorner \varphi_i \urcorner \rangle$$

- per la regola di introduzione del quantificatore esistenziale

$$\exists\, a \leq d, \exists\, b \leq d. \ulcorner \varphi_i \urcorner = \langle \#\exists, a, b \rangle \wedge \exists\, j < i.equals(p_i, p_j) \wedge \exists\, c \leq d.Term(c) \wedge \ulcorner \varphi_j \urcorner = Sub(b, a \dot{-} 8, c)$$

- per la regola di eliminazione del quantificatore esistenziale[7]

$$\exists\, j < i, \exists\, k < i, \exists\, a \leq d, \exists\, b \leq d.equal(p_i, p_i) \wedge \ulcorner \varphi_j \urcorner = \langle \#\exists, a, b \rangle \wedge \ulcorner \varphi_k \urcorner = \ulcorner \varphi_i \urcorner \wedge \\ \wedge \exists\, h \leq len(p_k).nth(p_k, h) = b \wedge equal(p_i, rem_{len(p_k),h}(p_k))$$

- per la regola di introduzione dell'uguaglianza

$$len(p_i) = 0 \wedge \exists\, a \leq d. \ulcorner \varphi_i \urcorner = \langle \# =, a, a \rangle$$

- infine per la regola di eliminazione dell'uguaglianza

$$\exists\, j < i, \exists\, k < i.equal(p_i, p_j) \wedge equal(p_i, p_k) \wedge \exists\, t \leq d, \exists\, s \leq d. \ulcorner \varphi_j \urcorner = \langle \# =, t, s \rangle \wedge \\ \wedge \exists\, a \leq d, \exists\, b \leq d.For(a) \wedge \ulcorner \varphi_i \urcorner = Sub(a, b, s) \wedge \ulcorner \varphi_j \urcorner = Sub(a, b, t)$$

Notiamo che in realtà con Dim_T così costruito vale che $\mathbb{N} \vDash \exists\, d.Dim_T(d, \ulcorner \varphi \urcorner)$ se e solo se esiste una sottoteoria $T_0 \subseteq T$ finita tale che $T_0 \vdash \varphi$ ma per compattezza sintattica (4.0.3) questo equivale a dire che $T \vdash \varphi$. □

Teorema 10.3.3: *Primo teorema di incompletezza di Gödel*

Data una teoria dell'aritmetica T ricorsivamente assiomatizzata tale che $T \vdash Q$ se $\mathbb{N} \vDash T$ allora T è incompleta, cioè esiste una formula artimetica φ tale che $T \nvdash \varphi$ e $T \nvdash \neg\varphi$.

Dimostrazione. Dal lemma di diagonalizzazione di Gödel(10.2.4) applicato a $\varphi \doteq \neg\exists\, d.Dim_T(d, x_1)$ esiste una formula aritmetica γ[8] tale che

$$Q \vdash \gamma \longleftrightarrow \neg\exists\, d.Dim_T\left(d, \overline{\ulcorner \gamma \urcorner}\right) \tag{10.3}$$

Vediamo che T non dimostra né γ né la sua negazione $\neg\gamma$:

- Se per assurdo $T \vdash \gamma$ allora per definizione di Dim_T (10.3.2) vale

$$N \vDash \exists\, d.Dim_T\left(d, \overline{\ulcorner \gamma \urcorner}\right)$$

  e Dim_T è ricorsivo, quindi questa è una formula aritmetica chiusa di classe Σ_1^0; da questo per il teorema 9.2.9 segue che

$$Q \vdash \exists\, d.Dim_T\left(d, \overline{\ulcorner \gamma \urcorner}\right)$$

  ed allora per costruzione di γ (10.3) segue che $Q \vdash \neg\gamma$ ma questo è assurdo perché $T \vdash Q, \gamma$ e T è coerente per ipotesi in quanto ammette il modello $\mathbb{N}$.

- Se invece, sempre per assurdo, $T \vdash \neg\gamma$ allora $\mathbb{N} \vDash \neg\gamma$ in quanto $\mathbb{N}$ è un modello di T. Inoltre $\mathbb{N}$ è anche un modello di Q quindi per costruzione di γ (10.3)

$$N \vDash \neg\gamma \longleftrightarrow \exists\, d.Dim_T\left(d, \overline{\ulcorner \gamma \urcorner}\right)$$

  e per la semantica di Tarski da questo segue che $N \vDash \exists\, d.Dim_T\left(d, \overline{\ulcorner \gamma \urcorner}\right)$ che per definizione del predicato di dimostrabilità vuol dire che $T \vdash \gamma$, cioè abbiamo ottenuto la stessa conseguenza assurda del punto precedente.

[7] in realtà qua dovremmo anche verificare che $x_k \notin \mathrm{vl}(T, \psi)$ ma anche questo è chiaro che si può fare in maniera decidibile perché nelle dimostrazioni che stiamo usando c'è sempre un numero finito di premesse

[8] con $T = \mathrm{PA}$ questa funzione è detta γ *di Gödel*

□

Pochi anni dopo la dimostrazione del teorema si è notato che l'ipotesi di 'ω-coerenza' (cioè che $\mathbb{N}$ sia un modello di T) è eliminabile, ottenendo una forma più forte del teorema che vale su tutte le teorie coerenti che estendono Q.

Teorema 10.3.4: *di Rosser*

Data una teoria dell'aritmetica T ricorsivamente assiomatizzata tale che $T \vdash Q$ e T è coerente allora T è incompleta, cioè esiste una formula artimetica φ tale che $T \nvdash \varphi$ e $T \nvdash \neg\varphi$.

L'idea della dimostrazione di questo teorema è di fare gli stessi passi della dimostrazione del teorema di Gödel (10.3.3) applicando però il lemma di diagonalizzazione di Gödel alla formula $\varphi \doteq \forall\, d.Dim_T(d, x_1) \to \exists\, d' \leq d.Dim_T(d', Neg(x_1))$[9] ottenendo che esiste una formula aritmetica ψ tale che

$$Q \vdash \psi \longleftrightarrow (\forall\, d.Dim_T(d, \ulcorner\psi\urcorner) \to \exists\, d' \leq d.Dim_T(d', \ulcorner\neg\psi\urcorner))$$

Esercizio 10.3 Dimostrare il teorema di Rosser.

Svolgimento. Verso la fine della dimostrazione vorrei usare che se $M \vDash Q$ e $M \vDash Dim_T(\ulcorner m\urcorner, \ulcorner n\urcorner)$ allora $\mathbb{N} \vDash Dim_T(\ulcorner m\urcorner, \ulcorner n\urcorner)$; se il predicato di dimostrabilità fosse Δ_0^0 potrei farlo ma essendo primitivo ricorsivo sappiamo soltanto che è Σ_1^0 (in realtà il contenimento $\Delta_0^0 \subseteq$ **PR** è stretto quindi è ben probabile che questa sia veramente una formula non Δ_0^0).

Essendo il predicato di dimostrabilità primitivo ricorsivo esiste una formula $\varphi(x, y)\Sigma_1^0$ tale che per ogni α codice di una formula e d codice di una dimostrazione vale

$$(\alpha, d) \in Dim_T \iff \mathbb{N} \vDash \varphi\left(\overline{\alpha}, \overline{d}\right)$$

ed essendo $\varphi(x, y)$ di classe Σ_1^0 esiste una formula $\psi(x, y, z)$ di classe Δ_0^0 tale che

$$\mathbb{N} \vDash \varphi(x, y) \iff \mathbb{N} \vDash \exists\, z.\psi(x, y, z)$$

allora possiamo costruire la formula $\overline{Dim}(x, v)$ di classe Δ_0^0 come

$$\overline{Dim}(x, v) \doteq \psi(x, car(v), cdr(v))$$

e procediamo nella dimostrazione usando $\overline{Dim}$ invece di Dim_T.

Possiamo applicare il lemma di diagonalizzazione (10.2.4) alla formula $\varphi \doteq \forall\, d.\overline{Dim}(x_1, d) \to \exists\, d' \leq d.\overline{Dim}(Neg(x_1), d)$ ottenendo che esiste una formula aritmetica ψ tale che

$$Q \vdash \psi \longleftrightarrow \left(\forall\, d.\overline{Dim}\left(\overline{\ulcorner\psi\urcorner}, d\right) \to \exists\, d' \leq d.\overline{Dim}\left(Neg(\overline{\ulcorner\psi\urcorner}), d'\right)\right)$$

e vediamo che T non può essere completa in quanto non può dimostrare ψ.

- Se per assurdo $T \vdash \psi$ allora per definizione del predicato di dimostrabilità (10.3.2)

  $$\mathbb{N} \vDash \exists\, d.Dim_T\left(d, \ulcorner\psi\urcorner\right)$$

  e quindi esiste $n \in \mathbb{N}$ tale che $\mathbb{N} \vDash Dim_T\left(\overline{n}, \overline{\ulcorner\psi\urcorner}\right)$ ovvero esiste $m \in \mathbb{N}$ tale che $\mathbb{N} \vDash \overline{Dim}\left(\overline{\ulcorner\psi\urcorner}, \overline{m}\right)$ e quindi Q dimostra questa formula, però vale anche

  $$\mathbb{N} \vDash \neg\exists\, d' \leq \overline{m}.\overline{Dim}\left(Neg(\overline{\ulcorner\psi\urcorner}), d'\right)$$

  (altrimenti sarebbe vero $\mathbb{N} \vDash \exists\, d.Dim_T\left(Neg(\overline{\ulcorner\psi\urcorner}), d\right)$ da cui per definizione seguirebbe che T dimostra $\neg\psi$ e quindi T sarebbe deduttivamente incoerente) ed essendo questa una formula chiusa Δ_0^0 vale

  $$Q \vdash \neg\exists\, d' \leq \overline{m}.\overline{Dim}\left(Neg(\overline{\ulcorner\psi\urcorner}), d'\right)$$

[9] Dove $Neg(x)$ è una abbreviazione per $\langle \#\to, x, \ulcorner\bot\urcorner\rangle$

ed anche $\overline{Dim}\left(\overline{\ulcorner\psi\urcorner}, \overline{m}\right)$ è una formula chiusa Δ_0^0 quindi vale

$$Q \vdash \neg\forall\, d.\overline{Dim}\left(\overline{\ulcorner\psi\urcorner}, d\right) \to \exists\, d' \leq d.\overline{Dim}\left(Neg(\overline{\ulcorner\psi\urcorner}), d'\right)$$

ovvero per costruzione di ψ vale $Q \vdash \neg\psi$ ma questo è assurdo perché $T \vdash Q, \psi$ e T è deduttivamente coerente.

- Se, ancora una volta per assurdo, $T \vdash \neg\psi$ allora esiste $d' \in \mathbb{N}$ tale che $\mathbb{N} \vDash Dim_T\left(d', \ulcorner\neg\psi\urcorner\right)$ e quindi esiste $n \in \mathbb{N}$ tale che $\mathbb{N} \vDash \overline{Dim}\left(\ulcorner\neg\psi\urcorner, \overline{n}\right)$ ed ovviamente $\overline{\ulcorner\neg\psi\urcorner} = \overline{Neg\left(\overline{\ulcorner\psi\urcorner}\right)}$ quindi

$$Q \vdash \overline{Dim}\left(\overline{Neg\left(\overline{\ulcorner\psi\urcorner}\right)}, \overline{n}\right)$$

Supponiamo per assurdo che $Q \nvdash \psi$, allora esiste $M \vDash Q, \neg\psi$, quindi per costruzione di M vale

$$M \vDash \neg\left(\forall\, d.\overline{Dim}\left(\overline{\ulcorner\psi\urcorner}, d\right) \to \exists\, d' \leq d.\overline{Dim}\left(Neg(\overline{\ulcorner\psi\urcorner}), d'\right)\right)$$

cioè per la semantica di Tarski deve esistere $\alpha \in M$ tale che

$$M \vDash \overline{Dim}\left(\overline{\ulcorner\psi\urcorner}, \alpha\right) \qquad \text{e} \qquad M \vDash \neg\exists\, d' \leq \alpha.\overline{Dim}\left(Neg(\overline{\ulcorner\psi\urcorner}), d'\right)$$

necessariamente tale α deve essere standard perché se α fosse non-standard sarebbe vero $M \vDash \overline{m} < \alpha$ per il lemma 9.2.8 e quindi $M \vDash \exists\, d' \leq \alpha.\overline{Dim}\left(Neg(\overline{\ulcorner\psi\urcorner}), d'\right)$, quindi esiste $k \in \mathbb{N}$ tale che $M \vDash \overline{Dim}\left(\overline{\ulcorner\psi\urcorner}, \overline{k}\right)$ ed essendo questa una formula Δ_0^0 chiusa Q decide tale formula (9.2.9) da cui necessariamente $Q \vdash \overline{Dim}\left(\overline{\ulcorner\psi\urcorner}, \overline{k}\right)$ perché $M \vDash Q$, ma anche $\mathbb{N} \vDash Q$ quindi $\mathbb{N} \vDash \overline{Dim}\left(\overline{\ulcorner\psi\urcorner}, \overline{k}\right)$ da cui per costruzione di $\overline{Dim}$ segue che

$$\mathbb{N} \vDash Dim_T\left(\overline{\ulcorner\psi\urcorner}, car\left(\overline{k}\right)\right)$$

da cui per definizione di Dim_T segue che $T \vdash \psi$, ma dato che $T \vdash \neg\psi$ questo contraddice la coerenza deduttiva di T.

□

Proposizione 10.3.5

data una teoria dell'aritmetica T decidibile (ovvero se l'insieme delle formule aritmetiche che seguono da T è un insieme decidibile) se T è coerente allora esiste T' completa e decidibile che estende T.

Dimostrazione. L'idea della dimostrazione è di esibire un algoritmo che enumera le conseguenze di T', da cui T' è ricorsivamente enumerabile (quindi T' è semidecidibile); essendo T' completa da questo segue che è decidibile infatti data una qualunque formula φ posso cercarla nella sua enumerazione e per completezza prima o poi troverò o φ o $\neg\varphi$.

Per enumerare le conseguenze di T' procediamo come segue: al passo n-esimo avendo enumerato $\varphi_0, \ldots, \varphi_{n-1}$ tutte conseguenze di T' consideriamo la formula ψ tale che $\ulcorner\psi\urcorner = n$, per decidibilità di T possiamo separare due sottocasi:

- se $T, \varphi_0, \ldots, \varphi_{n-1} \vdash \neg\psi$ allora definiamo $\varphi_n \doteq 0 = 0$;
- altrimenti $T, \varphi_0, \ldots, \varphi_{n-1} \nvdash \neg\psi$, quindi esiste un modello M di $T \cup \{\varphi_0, \ldots, \varphi_{n-1}, \psi\}$ e definiamo $\varphi_n \doteq \psi$.

Per costruzione la teoria $T \cup \{\varphi_i\}_{i\in\mathbb{N}}$ è finitamente coerente, quindi è coerente (3.2.1) ed è completa in quanto per costruzione decide tutte le formule aritmetiche. quindi è la teoria T' cercata. □

Corollario 10.3.5.1

La teoria Q di Robinson e la teoria dell'aritmetica di Peano PA non sono decidibili.

Dimostrazione. Se Q fosse decidibile allora per la proposizione precedente (10.3.5) esisterebbe un suo completamento Q' decidibile, ma questo contraddice il primo teorema di incompletezza di Gödel (10.3.3) in quanto se Q' fosse decidibile allora sarebbe ricorsivamente enumerabile.

Analogamente dato che PA estende Q un completamento decidibile di PA sarebbe anche un completamento decidibile di Q. □

Corollario 10.3.5.2

L'insieme

$$\{\ulcorner\varphi\urcorner \mid \mathbb{N} \vDash \varphi\}$$

non è ricorsivamente enumerabile (e quindi non è ricorsivo).

Corollario 10.3.5.3

La teoria vuota nel linguaggio dell'aritmetica non è decidibile.

Dimostrazione. Dato che la teoria Q di Robinson ha un numero finito di assiomi data una qualunque formula aritmetica vale

$$Q \vdash \varphi \quad \iff \quad \vdash Q_1 \wedge \cdots \wedge Q_7 \to \varphi$$

quindi dato un qualunque algoritmo che decide la teoria vuota potremmo costruire un algoritmo che decide la Q di Robinson. □

10.4 Il secondo teorema di incompletezza

Come conseguenza del primo teorema di incompletezza di Gödel si può dimostrare un altro risultato riguardo l'aritmetica di Peano al primo ordine, che è il secondo teorema di incompletezza. Per questo teorema introduciamo la notazione

$$\Box\varphi \quad \doteq \quad \exists d.Dim_{\mathrm{PA}}(d, \ulcorner\varphi\urcorner)$$

dove φ è una formula chiusa.

Osservazione 10.4.1 Prima di introdurre il teorema facciamo tre osservazioni che saranno utili nella sua dimostrazione:

1. Per il lemma 10.3.2 se $\mathrm{PA} \vdash \varphi$ allora $\mathrm{PA} \vdash \Box\varphi$.
2. Data una formula chiusa φ
$$\mathrm{PA} \vdash \Box\varphi \to \Box(\Box\varphi)$$
cioè l'implicazione del punto precedente può essere formalizzata nell'aritmetica di Peano. (non dimostreremo questo fatto, l'idea è di formalizzare dentro l'aritmetica di Peano tutti i ragionamenti fatti per dimostrare il punto precedente)
3. L'aritmetica di Peano 'capisce' il *modus ponens* ovvero date due formule chiuse φ e ψ
$$\mathrm{PA} \vdash (\Box\varphi \wedge \Box(\varphi \to \psi)) \to \Box\psi$$
(non dimostreremo questo fatto)

Teorema 10.4.1: *Secondo teorema di incompletezza di Gödel*

La teoria dell'aritmetica di Peano al primo ordine non dimostra la sua stessa coerenza, ovvero

$$PA \nvdash \neg$$

Dimostrazione. Per dimostrare il teorema cercheremo di vedere che la γ di Gödel (10.3) equivale in PA a $\neg\Box\bot$ ovvero che

$$\mathrm{PA} \vdash \gamma \leftrightarrow \neg\Box\bot$$

Per costruzione dato che $\mathrm{PA} \vdash Q$ vale per definizione di $\Box\gamma$ che

$$\mathrm{PA} \vdash \gamma \leftrightarrow \neg\Box\gamma$$

e verifichiamo le due implicazioni:

($\longrightarrow$) per dimostrare che $\mathrm{PA} \vdash \gamma \to \neg\Box\bot$ iniziamo notando che in qualunque teoria da $\bot$ segue qualunque cosa; in particolare $\mathrm{PA} \vdash \bot \to \gamma$, quindi per il primo punto dell'osservazione 10.4.1 vale $\mathrm{PA} \vdash \Box(\bot \to \gamma)$ da cui per il terzo punto della stessa osservazione $\mathrm{PA} \vdash \Box\bot \to \Box\gamma$, da cui vale anche la contronominanle

$$\mathrm{PA} \vdash \neg\Box\gamma \to \neg\Box\bot$$

e si conclude in quanto per costruzione $\mathrm{PA} \vdash \gamma \leftrightarrow \neg\Box\gamma$.

($\longleftarrow$) Per l'altra implicazione dimostriamo la contronominale $\mathrm{PA} \vdash \neg\gamma \to \Box\bot$; per costruzione sappiamo che $\mathrm{PA} \vdash \Box\gamma \to \neg\gamma$ e sfruttando i punti dell'osservazione precedente da questo si ottiene che:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathrm{PA} \vdash \Box\gamma \to \neg\gamma}\,10.4.1.1}{\mathrm{PA} \vdash \Box(\Box\gamma \to \neg\gamma)}\,10.4.1.3}{\mathrm{PA} \vdash \Box\Box\gamma \to \Box\neg\gamma} \qquad \dfrac{}{\mathrm{PA} \vdash \Box\gamma \to \Box\Box\gamma}\,10.4.1.2}{\mathrm{PA} \vdash \Box\gamma \to \Box\neg\gamma} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \gamma \leftrightarrow \neg\neg\gamma}}{\mathrm{PA} \vdash \gamma \to (\neg\gamma \to \bot)}\,10.4.1.1}{\mathrm{PA} \vdash \Box(\gamma \to (\neg\gamma \to \bot))}\,10.4.1.3}{\mathrm{PA} \vdash \Box\gamma \to \Box(\neg\gamma \to \bot)}\,10.4.1.3}{\mathrm{PA} \vdash \Box\gamma \to (\Box\neg\gamma \to \Box\bot)}$$

$$\mathrm{PA} \vdash \Box\gamma \to \Box\bot$$

infine per definizione di γ vale $\mathrm{PA} \vdash \neg\gamma \leftrightarrow \Box\gamma$ quindi $\mathrm{PA} \vdash \neg\gamma \to \Box\bot$.

Per la dimostrazione del primo teorema di incompletezza (10.3.3) vale che $\mathrm{PA} \nvdash \gamma$, quindi necessariamente $\mathrm{PA} \nvdash \neg\Box\bot$. □

Capitolo 11

Il decimo problema di Hilbert

Questo capitolo è quello scritto peggio, con più omissioni e con più cose che non ho capito di tutti gli appunti, in quanto non ho avuto il tempo o la voglia di soffermarmi attentamente sui vari passaggi mentre seguivo la lezione e non ci ho più messo mano per provare a correggerli.

L'ultimo dei dieci problemi 'del secolo' esposti da David Hilbert nel 1900 era di mostrare se esiste un algoritmo che risolve le equazioni diofantee, cioè che risolve

$$\exists x_1, \dots, x_k \in \mathbb{N}. p(x_1, \dots, x_k) = 0$$

dove $p \in \mathbb{Z}[x_1, \dots, x_k]$.

Vediamo che tale algoritmo non esiste mostrando come questo problema è collegato ai teoremi di Gödel.

Definizione 11.0.1: *Insieme diofanteo*

Diciamo che un insieme $X \subseteq \mathbb{N}^k$ è diofanteo se esiste $p \in \mathbb{Z}[x_1, \dots, x_k, y_1, \dots, y_h]$ tale che

$$X = \{(x_1, \dots, x_k) \mid \exists y_1, \dots, y_h \in \mathbb{N}. p(x_1, \dots, x_k, y_1, \dots, y_h) = 0\}$$

Osservazione 11.0.1 Gli insiemi diofantei sono tutti ricorsivamente enumerabili; infatti per la proposizione 8.2.2 dato l'insieme X determinato dal polinomio $p(x_1, \dots, x_k, y_1, \dots, y_h)$ data la k-upla $(x_1, \dots, x_k)$ posso elencare tutte le h-uple $(y_1, \dots, y_h)$ fino a quando ne trovo una tale che $p(x_1, \dots, x_k, y_1, \dots, y_h) = 0$, cioè X è semidecidibile.

Il teorema chiave per dimostrare che il decimo problema di Hilbert non ha soluzione è il 11.0.7, per il quale gli insiemi diofantei sono esattamente quelli ricorsivamente enumerabili.

Esempio 11.0.2: *Esempi di insiemi diofantei* I seguenti insiemi sono diofantei:

- l'insieme vuoto $\varnothing$ e l'insieme dei numeri naturali $\mathbb{N}$;
- l'insieme $\{(x_1, x_2) \mid x_1 < x_2\}$ è diofanteo in quanto è definito da

  $$\exists x_3. x_3 + x_1 + 1 - x_2 = 0$$

  e da ora in avanti indicheremo questo dicendo che *la relazione* $x_1 < x_2$ *è diofantea*;
- la relazione $x_1 \leq x_2$ è diofantea, in maniera esattamente analoga alla precedente;
- la relazione $x_1 = x_2$ è diofantea (basta porre $p(x_1, x_2) \doteq x_1 - x_2$);
- la relazione $x_1 \neq x_2$ è diofantea infatti basta porre $0 < (x_1 - x_2)^2$ ed abbiamo già visto che il $<$ è diofanteo;
- la relazione $x \equiv y \mod z$ è diofantea in quanto possiamo descrivala come

  $$\exists t_1, t_2. x + zt_1 = y + zt_2$$

Lemma 11.0.2

Gli insiemi diofantei sono chiusi sotto unione, intersezione, proiezioni e prodotti cartesiani.

Dimostrazione. Dati $X \subseteq \mathbb{N}^k$ ed $Y \subseteq \mathbb{N}^h$ sottoinsiemi descritti rispettivamente come

$$\begin{aligned} \overline{x} \in X &\iff \exists \overline{y}.p(\overline{x},\overline{y}) = 0 \\ \overline{x} \in Y &\iff \exists \overline{z}.p(\overline{x},\overline{z}) = 0 \end{aligned}$$

allora:

- Con $k = h$ l'unione $X \cup Y$ è descritta dal prodotto $p(\overline{x},\overline{y}) \cdot q(\overline{xz})$.
- Con $k = h$ l'intersezione $X \cap Y$ è descritta dalla somma dei quadrati

$$(p(\overline{x},\overline{y}))^2 + (q(\overline{xz}))^2$$

- La proiezione $\pi^k_{\overline{i}}$ sul multi-indice $\overline{i} \subseteq k$ (di $h \leq k$ elementi) dell'insieme X è diofantea infatti è descritta come l'insieme diofanteo

$$\pi^k_{\overline{i}}(X) = \left\{ x_{\overline{i}} \in \mathbb{N}^h \;\middle|\; \exists\, x_{k \setminus \overline{i}}, \overline{y}.p(x_{\overline{i}}, x_{k\setminus\overline{i}}, \overline{y}) \right\}$$

  a meno di rinominare le variabili nel polinomio p per 'aggiustarne' l'ordinamento.

- Il prodotto cartesiano $X \times Y$ si può costruire come l'intersezione

$$X \times Y \equiv X \times \mathbb{N}^h \cap \mathbb{N}^k \times Y$$

  e l'insieme $X \times \mathbb{N}^h$ è descritto in maniera diofantea come

$$X \times \mathbb{N}^h = \left\{ (\overline{x},\overline{z}) \in \mathbb{N}^{k+h} \;\middle|\; \exists y.p(\overline{x},\overline{y},\overline{z}) = 0 \right\}$$

  dove tutte le potenze di tutte le variabili $\overline{z}$ nel polinomio p hanno coefficiente nullo; ed allo stesso modo si descrive $\mathbb{N}^k \times Y$.

□

Esempio 11.0.3: *La divisione euclidea è diofantea* Le relazioni

$$x = y \bmod z \qquad \text{e} \qquad x = y \operatorname{div} z$$

sono diofantee (dove la prima non è la congruenza ma l'uguaglianza, cioè x è esattamente il resto della divisione euclidea $y \operatorname{div} x$); infatti la prima può essere descritta come $x = y \bmod z$ se e solo se

$$x \equiv y \mod z \wedge x < z$$

per il lemma precedente (11.0.2) è un predicato diofanteo.
Per la seconda $x = y \operatorname{div} z$ se e solo se

$$xz + y \bmod z = y$$

Osservazione 11.0.4 Se il teorema 11.0.7 è vero allora gli insiemi diofantei non sono chiusi per complemento, quindi è inutile cercare di dimostrarlo.

Per dimostrare il teorema 11.0.7 inizieremo prima mostrando che la relazione dell'esponenziale $x^y = z$ è diofantea, il che faremo con una grande quantità di lemmi al termini dei quali risulta che $x^y = z$ senza capire effettivamente se c'è un'idea fondamentale dietro e quale.

Definizione 11.0.3: *Equazione di Pell*

Definiamo l'insieme delle soluzioni dell'*equazione di Pell con parametro* $a > 1$ come

$$P_a = \left\{(x, y) \in \mathbb{Z}^2 \;\middle|\; x^2 - (a^2 - 1)y^2 = 1\right\}$$ [1]

[1] Notiamo che fino ad ora abbiamo usato gli insiemi diofantei come sottoinsiemi di $\mathbb{N}^k$ invece che $\mathbb{Z}^k$, ma questo è stato soltanto perché ci tornava meglio al livello di notazione; in questo caso la notazione viene meglio con $\mathbb{Z}$ ma se volessimo trasformarlo in un insieme diofanteo come sottoinsieme di $\mathbb{N}^2$ potremmo 'spezzarlo' nei quattro quadranti assegnando il segno ad x ed y nell'equazione e facendone l'unione (in questo caso essendo x ed y sempre al quadrato l'insieme chiaramente sarà simmetrico nei quattro quadranti ma il procedimento si può sempre fare indipendentemente da questo)

Notiamo che per ogni a le coppie $(1, 0)$ ed $(a, 1)$ appartengono a P_a e se indichiamo la coppia $(x, y) \doteq x + y\sqrt{a^2 - 1}$ allora se $x_1 + y_1\sqrt{a^2 - 1}$ ed $x_2 + y_2\sqrt{a^2 - 1}$ sono elementi di P_a allora anche

$$\left(x_1 + y_1\sqrt{a^2 - 1}\right)\left(x_2 + y_2\sqrt{a^2 - 1}\right) = x_1x_2 + y_1y_2\left(a^2 - 1\right) + (x_1y_2 + x_2y_1)\sqrt{a^2 - 1} \in P_a$$

e questo induce una struttura di gruppo, dove l'inverso è cambiare segno alla seconda componente

$$\left(x + y\sqrt{a^2 - 1}\right)\left(x - y\sqrt{a^2 - 1}\right) = x^2 - y^2\left(a^2 - 1\right) = 1$$

infatti 1 corrisponde nella notazione ad $(1, 0)$ che è l'elemento neutro del gruppo.

Esercizio 11.1 Con la struttura di gruppo descritta in precedenza $P_a \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ con $(a, 1) \doteq a + \sqrt{a^2 + 1}$ uno dei due generatori ed in particolare se definiamo la sequenza di coppie

$$x_n(a) + y_n(a)\sqrt{a^2 + 1} \doteq (a + \sqrt{a^2 + 1})^n$$

allora $(x, y) \in P_a \cap \mathbb{N}^2$ se e solo se esiste $n \in \mathbb{N}$ tale che $(x, y) = (x_n, y_n)$.
(Suggerimento: verificare che x_n ed y_n sono crescenti, se per assurdo ci fosse un'altra soluzione positiva (x', y') oltre a quelle moltiplicandola per l'inverso dell'ultima della lista più piccola di (x', y') verificare che si ottiene un elemento compreso tra $(1, 0)$ ed $(a, 1)$ e che nel gruppo non ci sono altri elementi strettamente compresi tra questi due)

Usando la definizione del prodotto

$$x_{m+n}(a) = x_m(a)x_n(a) + y_m(a)y_n(a)(a^2 - 1) \qquad \text{e} \qquad y_{m+n}(a) = x_m(a)y_n(a) + x_n(a)y_m(a) \tag{11.1}$$

quindi fissando $n = 1$ otteniamo

$$x_{m+1}(a) = a\,x_m(a) + y_m(a)(a^2 - 1) \qquad \text{e} \qquad y_{m+1}(a) = x_m(a) + a\,y_m(a) \tag{11.2}$$

che è una formula ricorsiva per elencale tutti gli elementi positivi di P_a, infatti la possiamo interpretare come:

$$f(a, 0) = (1, 0) f(a, n + 1) = (a\,car(f(a, n)) + cdr(f(a, n))(a^2 - 1), a\,cdr(f(a, n)) + car(f(a, n)))$$

inoltre

$$x_{m-1}(a) = a\,x_m(a) - y_m(a)(a^2 - 1) \qquad \text{e} \qquad y_{m-1}(a) = x_m(a) - a\,y_m(a)$$

dalla quale otteniamo un'altra formula ricorsiva per gli elementi positivi di P_a come

$$x_{m+1}(a) = 2a\,x_m(a) - x_{m-1}(a) \qquad \text{e} \qquad y_{m+1}(a) = 2a\,y_m(a) - y_{m-1}(a) \tag{11.3}$$

Elenchiamo diversi lemmi che ci serviranno per dimostrare che l'esponenziale è diofanteo i quali si dimostrano con le ricorsioni viste fino ad ora e diamo un'idea delle loro dimostrazioni.

Lemma 11.0.4

Valgono le seguenti:

1. le successioni $x_n(a)$ ed $y_n(a)$ sono strettamente crescenti in n;

2. per ogni $m > 0$ vale $a^m \leq x_m(a) \leq (2a)^m$;
3. $(x_m(a), y_m(a)) = 1$ ovvero i due numeri sono coprimi;
4. $y_n(a) \mid y_m(a)$ se e solo se $n \mid m$;
5. $y_{n\,k}(a) \equiv k(x_n(a))^{k-1} y_n(a) \mod (y_n(a))^3$;
6. $(y_n(a))^2 \mid y_{n\,y_n(a)}(a)$;
7. se $(y_n(a))^2 \mid y_t(a)$ allora $y_n(a) \mid t$;
8. $y_n(a) \equiv n \mod (a-1)$ ed $y_n(a) \equiv n \mod (2)$;
9. se $a \equiv b \mod c$ allora valgono sia $x_n(a) \equiv x_n(b) \mod c$ che $y_n(a) \equiv y_n(b) \mod c$;
10. $x_n(a) - y_n(a)(a - z) \equiv z^n \mod (2\,a\,z - z^2 - 1)$;
11. $x_{2n\pm k}(a) \equiv -x_k(a) \mod (x_n(a))$;
12. dati i, j tali che $0 \leq i, j \leq 2n$ se $x_i(a) \equiv x_j(a) \mod (x_n(a))$ allora $i = j$(ovvero la funzione che mappa i in $x_i(a) \bmod (x_n(a))$ è iniettiva fra 0 e $2n$) eccetto se $a = 2$, $n = 1$, $i, j = 0, 2$;
13. dato i tale che $0 < i \leq n$ se $x_i(a) \equiv x_j(a) \mod (x_n(a))$ allora $j \equiv \pm i \mod 4n$

Dimostrazione. 1. Segue immediatamente dalla formula (11.2).

2. Per la costruzione di x_{m+1} nella (11.2) vale $x_{m+1}(a) \geq a\,x_m(a)$ ed $x_1(a) = a$, quindi $x_{m+1}(a) \geq a^{m+1}$ mentre dalla (11.3) vale $x_{m+1}(a) \leq 2a\,x_m(a)$ quindi $x_{m+1}(a) \leq (2a)^{m+1}$, ovvero $x_m(a)$ cresce esattamente in maniera esponenziale.
3. Si verifica per induzione a partire dalle formule ricorsive.
4. Se $m \mid n$ vediamo per induzione che y_m divide y_k per ogni multiplo di m, infatti per la (11.2) per ogni k vale $y_{k+m} = y_k\,x_m + y_m\,x_k$ quindi se come ipotesi induttiva y_k è un multiplo di y_m allora anche y_{k+m} è un multiplo di y_m, in particolare quindi $y_m \mid y_n$.

   Per l'altra implicazione se $y_m \mid y_n$ supponiamo per assurdo che $m \nmid n$, ovvero $n \bmod m = n_0 \neq 0$; per la relazione $y_{k+m} = y_k\,x_m + y_m\,y_k$ se $y_m \mid y_{k+m}$ allora $y_m \mid y_k\,x_m$ e per il punto 3. $(y_m, x_m) = 1$ quindi $y_m \mid y_k$, quindi impostando un ragionamento per induzione su $n \operatorname{div} m$ si ottiene che $y_m \mid y_{n_0}$ ma questo è assurdo perché $n_0 < m$.
5. Fissiamo a per alleggerire la notazione; dato che $x_{n\,k} + y_{n\,k}\sqrt{\cdot} = \left(x_n + y_n\sqrt{\cdot}\right)^k$ espandendo la formula per la potenza del binomio:

   $$x_{n\,k} + y_{n\,k}\sqrt{\cdot} = x_n^k + k\,x_n^{k-1}\,y_n\sqrt{\cdot} + \dots$$

   dove tutti i termini pari successivi a $k\,x_n^{k-1}\,y_n\sqrt{\cdot}$ contengono una potenza di y_n maggiore o uguale a 3 quindi sono congrui a zero modulo y_n^3 mentre per i termini dispari la potenza a cui è elevato $y_n\sqrt{\cdot}$ è pari, quindi si elimina la radice ovvero la loro somma è la componente $x_{n\,k}$ ovvero isolando $y_{n\,k}$ nella congruenza l'unico termine che rimane è esattamente quello che cerchiamo.
6. Se nella congruenza al punto 5. impostiamo $k = y_n(a)$ si ottiene che

   $$y_{n\,y_n(a)}(a) \equiv (x_n(a))^{y_n(a)-1}(y_n(a))^2 \mod (y_n(a))^3$$

   quindi $y_{n\,y_n(a)}(a) \equiv 0 \mod (y_n(a))^2$ [2]
7. Se $(y_n(a))^2 \mid y_t(a)$ allora $y_n(a) \mid y_t(a)$ e quindi $n \mid t$ ovvero esiste k tale che $t = k\,n$, quindi per la congruenza al punto 5.

   $$y_t(a) \equiv k(x_n(a))^{k-1} y_n(a) \mod (y_n(a))^3$$

   ???non vedo come procedere???

[2] Usando la proprietà che se $a \equiv b \mod (kn)$ allora $a \equiv b \mod n$; infatti per definizione se $a \equiv b \mod (kn)$ allora esiste h tale che $a - b = h\,k\,n = (h\,k)n$

8. ?segue dalle formule (11.3)?

9. ?segue dalle formule (11.3)?

10. Per le formule (11.3) se indichiamo $t_n = x_n(a) - y_n(a)(a - z)$ allora t_n soddisfa la relazione di ricorrenza
$$t_{n+1} = 2a\, t_n - t_{n-1}$$
e quindi in particolare vale la congruenza modulo $2\,a\,z - z^2 - 1$; inoltre
$$z^{n+1} \equiv 2a\, z^n - z_{n-1} \mod (2\,a\,z - z^2 - 1)$$
in quanto $z^{n-1}(z^2 - 2\,a\,z - 1) \equiv 0 \mod (2\,a\,z - z^2 - 1)$, quindi basta verificare che la congruenza è vera per $n = 0$ ed $n = 1$; con $n = 0$ la congruenza diventa $1 \equiv 1 \mod (\dots)$ e con $n = 1$ diventa $z \equiv z \mod (\dots)$ entrambe vere.

11. Ancora una volta fissiamo a per alleggerire la notazione;separando $2n \pm k = n + (n \pm k)$ ed usando la formula (11.1)
$$x_{n+n\pm k} \equiv y_{n\pm k}\, y_n(a^2 - 1) \mod x_n$$
in quanto $x_n \equiv 0 \mod x_n$ e

- nel caso del $+$ facendo la stessa cosa con y_{n+k}
$$x_{n+n+k} \equiv x_k\, y_n^2(a^2 - 1) \mod x_n$$
e per definizione x_n ed y_n sono soluzioni dell'equazione di Pell, quindi $y_n^2(a^2 - 1) = x_n^2 - 1$ da cui
$$x_{n+n+k} \equiv x_k\, x_n^2 - x_k \equiv x_k \mod x_n$$
- invece nel caso del $-$???

12. chiaramente se $i, j < n$ allora
$$x_i(a) \equiv x_j(a) \mod (x_n(a)) \quad \to \quad i = j$$
in quanto la funzione è strettamente crescente; l'idea sta nel vedere che
$$x_{2n} \equiv -x_0, x_{2n-1} \equiv -x_1, \dots, x_{n+1} \equiv -x_{n-1} \mod (x_n)$$
infatti eccetto nel caso particolare vale $x_{n-1} < \frac{x_n}{2}$ in quanto per la (11.2) $x_n = a\, x_{n-1} + (a^2 - 1)y_{n-1}$ da cui $x_{n-1} \le \frac{x_n}{a}$ ed eccetto nel caso particolare in cui $a = 2$ ed $n = 1$ vale la disuguaglianza stretta, ottenendo così che per $0 \le i \le n - 1$ vale $0 < x_i < \frac{x_n}{2}$ mentre per $n + 1 \le i \le 2n$ vale $\frac{x_n}{2} < (x_i \bmod x_n) < x_n$ e quindi la funzione è iniettiva;

13.
> **Esercizio 11.2** Dimostrare il punto 13.
> (Suggerimento: sfruttando il punto 12. basterà verificare due casi)

□

Lemma 11.0.5

Dati k, x se $k > 0$ ed $x > 1$ allora $x = x_k(a)$ se e solo se il seguente sistema di equazioni diofantee ha soluzione:

$$(x, y) \in P_a \qquad (u, v) \in P_a \qquad (s, t) \in P_b \tag{11.4}$$
$$b \equiv a \mod u \qquad s \equiv x \mod u \tag{11.5}$$
$$y^2 \mid v \tag{11.6}$$
$$b \equiv 1 \mod 4y \qquad t \equiv k \mod 4y \tag{11.7}$$
$$k \le y \qquad 1 < a < b \qquad 1 \le v \qquad x \le u \tag{11.8}$$

Dimostrazione. Diamo un'idea della dimostrazione di questo lemma:

- Dalle formule (11.4) esistono i, n, j tali che

$$\begin{aligned} x &= x_i(a) & y &= y_i(a) \\ u &= x_n(a) & v &= y_n(a) \\ s &= x_j(b) & t &= y_j(b) \end{aligned}$$

  per mostrare che $x = x_k(a)$ bisogna quindi verificare che $i = k$.

- Sostituendo quanto appena ricavato nelle congruenze (11.5) si ottiene che

$$b \equiv a \mod (x_n(a)) \qquad x_j(b) \equiv x_i(a) \mod (x_n(a))$$

  e per il lemma 11.0.4.9 dalla prima di queste due segue che $x_j(b) \equiv x_j(a) \mod (x_n(a))$ quindi per transitività $x_i(a) \equiv x_j(a) \mod (x_n(a))$ e per la (11.8) vale $x_i(a) = x \leq u = x_n(a)$ quindi per monotonia $i \leq n$ ovvero possiamo usare il lemma 11.0.4.13 ottenendo che $j \equiv \pm i \mod 4n$.

- Possiamo scrivere la formula (11.6) come $(y_i(a))^2 \mid y_n(a)$ quindi per il lemma 11.0.4.7 $y_i(a) \mid n$ da cui la congruenza del punto precedente vale anche modulo $4y_i(a)$ ovvero $j \equiv \pm i \mod (4y_i(a))$

- Possiamo scrivere la prima congruenza di (11.7) come $b \equiv 1 \mod (4y_i(a))$ ovvero $b - 1$ è un multiplo di $4y_i(a)$ e per il lemma 11.0.4.9 vale $y_j(b) \equiv j \mod (b-1)$ quindi per le proprietà delle congruenze

$$k \equiv y_j(b) \equiv j \mod (4y_i(a))$$

  in quanto $k \equiv y_j(b) \mod (4y_i(a))$ per la seconda congruenza di (11.7); quindi siamo arrivati a dire che

$$k \equiv \pm i \mod (4y_i(a))$$

- per la prima disequazione di (11.8) $k \leq y_i(a)$ e per monotonia vale $i \leq y_i(a)$ quindi l'unico numero congruente a $\pm i$ modulo $4y_i(a)$ che sia maggiore di 0 e minore o uguale ad y_i è esattamente i, ovvero $k = i$.

Rimane da vedere che se $x = x_k(a)$ allora il sistema ha soluzione.
Fissando $n = 2\,k\,y_k(a)$ poniamo

$$\begin{aligned} x &= x_k(a) & u &= x_n(a) & s &= x_k(b) \\ y &= y_k(a) & v &= y_n(a) & t &= y_k(b) \end{aligned}$$

dove scegliamo b come soluzione abbastanza grande del sistema di congruenze

$$\begin{cases} b \equiv a \mod u \\ b \equiv 1 \mod 4y \end{cases}$$

> **Esercizio 11.3** Verificare usando i lemmi 11.0.4 che u e $4y$ sono coprimi (quindi esiste b) e che le variabili scelte come sopra effettivamente risolvono il sistema.

□

Lemma 11.0.6

Dato $z > 0$ vale $m = z^k$ se e solo se il seguente sistema di equazioni ha soluzione:

$$x = x_k(a) \qquad y = y_k^a \tag{11.9}$$
$$x - y(a - z) \equiv m \mod (2az - z^2 - 1) \tag{11.10}$$
$$a^2 - (w^2 - 1)(w - 1)^2 t^2 = 1 \tag{11.11}$$
$$m < 2az - z^2 - 1 \qquad z < w \qquad k < w \tag{11.12}$$

Dimostrazione. Dimostriamo l'implicazione $\leftarrow$, quindi supponiamo che il sistema abbia soluzione. Per il lemma 11.0.4.10 vale

$$x_n(a) - y_n(a)(a - z) \equiv z^n \mod (2\,a\,z - z^2 - 1)$$

quindi dalla (11.10) segue che

$$m \equiv z^n \mod (2\,a\,z - z^2 - 1) \tag{11.13}$$

Per la (11.11) $(a, (w-1)t)$ è una soluzione dell'equazione di Pell con parametro w; quindi esiste j tale che $a = x_j(w)$ e $(w-1)t = y_j(w)$. Per il lemma 11.0.4.8

$$0 \equiv (w-1)t \equiv y_j(w) \equiv j \mod (w-1)$$

quindi $w - 1 \leq j$[3].

Notiamo adesso che $z^k < w^{w-1}$ in quanto per la (11.12) $z < w$ e $k \leq w - 1$, inoltre per il lemma 11.0.4.2 $x_j(w) > w^j$ quindi

$$z^k < w^{w-1} \leq w^j < x_j(w) = a \leq az + az - z^2 - 1 = 2az - z^2 - 1$$

Dato che per (11.12) anche $m < 2az - z^2 - 1$ allora la congruenza (11.13) è necessariamente una uguaglianza.

> **Esercizio 11.4** Completare la dimostrazione verificando che se $m = z^k$ allora il sistema ha soluzione.

□

Dato che il sistema di questo ultimo lemma (11.0.6) è composto da formule e relazioni diofantee allora effettivamente l'esponenziale è diofanteo.

Teorema 11.0.7

Un insieme $X \subseteq \mathbb{N}^k$ è diofanteo se e solo se è ricorsivamente enumerabile.

Dimostrazione. Per l'osservazione precedente (11.0.1) rimane solo da dimostrare che ogni insieme ricorsivamente enumerabile è diofanteo.

Possiamo separare la dimostrazione in tre parti:

1. prima costruiremo una codifica delle sequenze di bit;
2. poi dimostreremo che determinate operazioni sulle sequenze sono diofantee;
3. poi usando il punto 2. dimostreremo che la computabilità è diofantea, cioè rappresenteremo con un polinomio la relazione 'la macchina di Turing con codice x sull'input y produce l'output z'.

Indicando l'insieme $\mathrm{bit} = \{0, 1\}$ diciamo che la sequenza $(b_1, \ldots, b_n) \in \mathrm{bit}^n$ è codificata da

$$b_1, \ldots, b_n = (1\,b_n\,\ldots\,b_1)_2 = 2^n + b_n 2^{n-1} + \cdots + b_1 2^0$$

cioè il numero corrispondente al codice binario $1\,b_n\,\ldots\,b_1$.

Vediamo che le seguenti relazioni sulle sequenze sono diofantee:

1. La relazione $\sigma = \overbrace{0\ldots0}^{n}$ è diofantea in quanto equivale a dire che $\sigma = 2^n$ ed abbiamo visto che l'esponenziale è diofanteo.
2. La lunghezza di una sequenza $n = len(\sigma)$ è diofantea in quanto equivale a dire $2^n \leq \sigma < 2^{n+1}$.
3. La concatenazione di due sequenze $\tau = \sigma_1 \oplus \sigma_2$ è diofantea in quanto equivale a dire che $\tau = \sigma_1 + (\sigma_2 - 1)2^{len(\sigma_1)}$ (il -1 serve per levare l'uno in testa a σ_1).
4. gli shift a sinistra $\tau = \sigma \ll n$ e a destra $\tau = \sigma \gg n$[4] sono diofantei infatti corrispondono a divisioni euclidee e moltiplicazioni:

$$\sigma \ll n = \sigma \div 2^n \qquad\qquad \sigma \gg n = \sigma \cdot 2^n$$

[3] Perché non potrebbe essere $a = 1$ e $j = 0$ e w qualunque?

[4] con questa notazione vogliamo dire che $\sigma_1\,\ldots\,\sigma_m \ll n \doteq \sigma_{n+1}\,\ldots\,\sigma_m$ e che $\sigma_1\,\ldots\,\sigma_m \ll n \doteq \overbrace{0\,\ldots\,0}^{n}\sigma_1\,\ldots\,\sigma_m$

Lemma 11.0.8

la relazione *disgiunto* definita come

$$dis(\sigma, \tau) \doteq \neg\exists\, i.\sigma_i = \tau_i = 1$$

è diofantea.

Dimostrazione. Per definizione della codifica delle sequenze date le codifiche σ e τ di due sequenze vale $dis(\sigma, \tau)$ se e solo se i due numeri $m = \sigma - 2^{len(\sigma)}$ ed $n = \tau - 2^{len(t)}$ non hanno 'uni incolonnati' e questo avviene se e solo se sommando m ed n in colonna in binario non ci sono riporti.

Verifichiamo che il numero dei riporti nella somma $m+n$ è uguale a $v_2\binom{m+n}{m}$[5] e che il binomiale $\binom{m+n}{m}$ è diofanteo.

Verifichiamo che $v_2(n!) = n - \#_1(n)$ dove $\#_1(n)$ è il numero di uni nella rappresentazione binaria del numero n. Infatti vale

$$v_2(n!) = v_2(1 \cdot 2 \cdot 3 \cdots n) = v_2(2 \cdot 4 \cdots 2(n \operatorname{div} 2)) = v_2(2^{n \operatorname{div} 2} 1 \cdot 2 \cdot 3 \cdots (n \operatorname{div} 2)) = n \operatorname{div} 2 + v2((n \operatorname{div} 2)!)$$

e da questo possiamo procedere per induzione:

- per il passo base se $n = 1$ allora $v_2(1!) = 0 = 1 - 1 = 1 - \#_1(1)$;
- se come ipotesi induttiva la tesi vale per ogni numero minore di n in particolare vale per $n \operatorname{div} 2$, quindi
$$v_2(n!) = (n \operatorname{div} 2) + v2((n \operatorname{div} 2)!) = (n \operatorname{div} 2) + (n \operatorname{div} 2) - \#_1(n \operatorname{div} 2)$$
allora separiamo i casi in cui n è:

  pari allora $(n \operatorname{div} 2) + (n \operatorname{div} 2) = n$ ed in notazione binaria n è uguale ad $(n \operatorname{div} 2)$ aggiungendo uno zero all'inizio, quindi $\#_1(n) = \#_1(n \operatorname{div} 2)$ ovvero $v_2(n!) = n - \#_1(n)$

  dispari allora $(n \operatorname{div} 2) + (n \operatorname{div} 2) = n - 1$ mentre $\#_1(n) = \#_1(n \operatorname{div} 2) + 1$ in quanto partendo dalla notazione binaria di $(n \operatorname{div} 2)$ si ottiene quella di n aggiungendo un uno all'inizio, quindi
$$v_2(n!) = (n-1) - (\#_1(n) - 1) = n - \#_1(n)$$

Adesso possiamo calcolare

$$v_2\binom{m+n}{m} = v_2\left(\frac{(m+n)!}{(m!)(n!)}\right) = v_2((m+n)!) - v_2(m!) - v_2(n!) =$$
$$m + n - \#_1(m+n) - m + \#_1(m) - n + \#_1(n) = \#_1(m) + \#_1(n) - \#_1(m+n)$$

e $\#_1(m) + \#_1(n) - \#_1(m+n)$ è proprio il numero di riporti nella somma $m + n$.

Esercizio 11.5 Dimostrare che il binomiale è diofanteo verificando che

$$((2^y + 1)^y \operatorname{div} 2^{yz}) \bmod 2^y = \binom{y}{z}$$

□

Definizione 11.0.9

Data una funzione $f : \text{bit}^n \to \text{bit}$ ovvero dalle sequenze di bit in $\{0, 1\}$ definiamo la funzione $[f]$ (formalmente da $\mathbb{N}^k$ in $\mathbb{N}$, ma ci interessa soltanto come una funzione dalle k-uple di sequenze di bit della stessa lunghezza nelle sequenze di bit) tale che data la k-upla $(\sigma_1, \ldots, \sigma_k)$ dove $\sigma_1 \ldots \sigma_k$ come sequenze hanno la stessa lunghezza allora

$$([f](\sigma_1, \ldots, \sigma_k))_i = f((\sigma_1)_1 \ldots (\sigma_k)_i)$$

dove $(x)_i$ è l'elemento in posizione i-esima della sequenza i. Cioè l'elemento i-esimo della sequenza

[5] dove $v_2(x)$ è la *valutazione diadica* di x, ovvero il numero di potenze di due che divide x, ad esempio $v_2(1000) = 3$ e $v_2(1002) = 1$

$[f](\sigma_1 \dots \sigma_k)$ è il bit che si ottiene applicando f alla sequenza $(\sigma_{1,i} \dots \sigma_{k,i})$ dove $\sigma_{a,b}$ è l'elemento b-esimo di σ_a.

Lemma 11.0.10

Fissato k e data $f : \mathrm{bit}^k \to \mathrm{bit}$ la funzione $[f]$ è diofantea.

Questo lemma ci dice che se abbiamo k sequenze possiamo applicare in maniera diofantea una qualunque operazione *component-wise*.

Dimostrazione. Iniziamo notando che ogni funzione da bit^k in bit può essere scritta come composizione di $not : \mathrm{bit} \to \mathrm{bit}$ ed $and : \mathrm{bit}^2 \to \mathrm{bit}$ in quanto ogni relazione logica si scrive come composizione di $\neg$ e $\wedge$.

Detto questo basta vedere che $[not] : \mathbb{N} \to \mathbb{N}$ e $[and] : \mathbb{N}^2 \to \mathbb{N}$ sono diofantee ottenendo per composizione che per ogni f anche $[f]$ è diofantea:

- Verifichiamo che $\sigma = not(\tau)$ è diofantea. Notiamo che se $\sigma = not(\tau)$ se e solo se sommando σ a τ senza considerare l'uno iniziale si ottiene esattamente $2^{len(\sigma)} - 1$ (ovvero il numero la cui interpretazione binariaè composta esattamente da $len(\sigma)$ uni), ovvero se e solo se

  $$\sigma - 2^{len(\sigma)} + \tau - 2^{len(\sigma)} = 2^{len(\sigma)} - 1$$

  ovvero se e solo se $\sigma = 3 \cdot 2^{len(\sigma)} - 1 - \tau$ che è una relazione diofantea.

- Verifichiamo che $\sigma = and(\tau_1, \tau_2)$ è diofantea. Vale $\sigma = and(\tau_1, \tau_2)$ se e solo se esistono due sequenze ε_1 ed ε_2 della stessa lunghezza di σ, τ_1, τ_2 entrambe disgiunte da σ e disgiunte l'una dall'altra tali che

  $$\sigma + \varepsilon_1 = \tau_1 - 2^{len(\sigma)} \qquad \sigma + \varepsilon_2 = \tau_2 - 2^{len(\sigma)}$$

  infatti:

  - se $\sigma = and(\tau_1, \tau_2)$ allora gli uni di σ sono tutti e soli gli uni in comune tra τ_1 e τ_2 quindi possiamo prendere ε_1 come $\tau_1 - \sigma + 2^{len(\sigma)}$ ed $\varepsilon_2 = \tau_2 - \sigma + 2^{len(\sigma)}$ rispettando tutte le condizioni richieste;
  - se invece esistono tali ε_1 ed ε_2 allora tutti gli uni di σ sono presenti sia in τ_1 che in τ_2; mentre gli zeri di σ corrispondono necessariamente o ad elementi dove sia τ_1 che τ_2 sono zero, o ad elementi dove almeno una tra ε_1 ed ε_2 sono uguali ad uno ma, essendo queste ultime due disgiunte, non possono entrambe corrispondere ad un uno contemporaneamente ovvero ad ogni zero di σ corrisponde uno zero in almeno in una tra τ_1 e τ_2, cioè $\sigma = and(\tau_1, \tau_2)$.

  e questa condizione è diofantea, quindi anche $\sigma = and(\tau_1, \tau_2)$ è diofantea.

□

Adesso codifichiamo le macchine di Turing. Per fare questo iniziamo lavorando soltanto con macchine di Turing che hanno un nastro di lunghezza finita.

Fissiamo una macchina M con al più 2^m stati ed al più 2^n simboli ed iniziamo codificando una configurazione (S, P, N) della macchina; dove S è lo stato (tra 0 e $2^n - 1$), N è il nastro (di lunghezza l) e P è la posizione (tra 0 ed $l - 1$).

Per fissare la lunghezza del nastro consideriamo la sequenza *format* fmt di lunghezza $l + 2$ composta da un uno 'in testa' al nastro, tanti zeri quante sono le celle l del nastro N ed un altro uno 'in coda', in quanto successivamente vorremo potere dire quando il nastro inizia o finisce.

Per rappresentare il nastro vero e proprio della macchina di Turing useremo n sequenze $tp_1, \dots, tp_n$ anch'esse di lunghezza $l + 2$, con uno zero in testa (posizione 0) ed uno in coda (posizione $l + 1$) e dove se in posizione i del nastro N c'è il simbolo j allora $(tp_{1,i+1} \dots tp_{n,i+1})$ è la rappresentazione binaria di j.

Per rappresentare la posizione della macchina useremo un'altra sequenza pos sempre di lunghezza $l + 2$ con un 1 nella posizione $P + 1$ della configurazione ed uno zero altrove.

Per rappresentare lo stato attuale S della macchina useremo m sequenze $st_1, \dots, st_m$ di lunghezza $l + 2$ composte interamente da zeri eccetto nella posizione $P + 1$ dove $(st_{1,P+1} \dots st_{m,P+1})$ è la codifica in binario di S.

Con queste $n+m+2 \doteq k$ sequenze effettivamente stiamo rappresentando interamente la configurazione (S,P,N), per alleggerire la notazione chiameremo queste sequenze anche come $\sigma_1,\dots,\sigma_k$ ordinate esattamente come le abbiamo definite.

Consideriamo k funzioni $step_1,\dots,step_k : \mathbb{N}^k \to \mathbb{N}$ tali che

$$\begin{aligned} step_1(\sigma_1,\dots,\sigma_k) &= \sigma_1' \\ &\vdots \\ step_k(\sigma_1,\dots,\sigma_k) &= \sigma_k' \end{aligned}$$

dove $(\sigma_1,\dots,\sigma_k)\vec{M}(\sigma_1',\dots,\sigma_k')$ e vediamo che queste sono diofantee; dove per usare una notazione più compatta indichiamo $\overline{step}(\overline{\sigma}) = \overline{\sigma}'$ raggruppando tutte le funzioni e le sequenze.

Lemma 11.0.11

La funzione $\overline{step}$ è diofantea.

Dimostrazione. Per definizione delle macchine di Turing l'elemento in posizione j-esima dell'output σ_i dipende soltanto dai valori del nastro in posizione $j-1$, j e $j+1$, cioè possiamo scrivere

$$(step_i(\overline{\sigma}))_j = f\begin{pmatrix} (\sigma_1)_{j-1} & \dots & (\sigma_k)_{j-1} \\ (\sigma_1)_j & \dots & (\sigma_k)_j \\ (\sigma_1)_{j+1} & \dots & (\sigma_k)_{j+1} \end{pmatrix} = f\begin{pmatrix} (\sigma_1 \gg 1)_j & \dots & (\sigma_k \gg 1)_j \\ (\sigma_1)_j & \dots & (\sigma_k)_j \\ (\sigma_1 \ll 1)_j & \dots & (\sigma_k \ll 1)_j \end{pmatrix}$$

allora possiamo usare il lemma precedente (11.0.10) ottenendo che su tutta la lunghezza del nastro

$$step_i(\overline{\sigma}) = [f]\begin{pmatrix} (\sigma_1 \gg 1) & \dots & (\sigma_k \gg 1) \\ (\sigma_1) & \dots & (\sigma_k) \\ (\sigma_1 \ll 1)_j & \dots & (\sigma_k \ll 1) \end{pmatrix}$$

e questa è una funzione diofantea[6]. □

Quindi possiamo calcolare un passo della macchina di Turing è diofantea, adesso vorremmo riuscire a calcolare n passi.

Lemma 11.0.12

La relazione $\overline{\sigma} \overset{M^\star}{\to} \overline{\tau}$ è diofantea.

Dimostrazione. Notiamo che date n configurazioni $\overline{\sigma}_1,\dots,\overline{\sigma}_n$ se applichiamo $\overline{step}$ alla loro concatenazione otteniamo per definizione che

$$\overline{step}(\overline{\sigma}_1 \oplus \dots \oplus \overline{\sigma}_n) = \overline{step}(\overline{\sigma}_1) \oplus \dots \oplus \overline{step}(\overline{\sigma}_n)$$

cerchiamo di usare questo per ottenere la tesi.

Per dire che $\overline{\sigma} \overset{M^\star}{\to} \overline{\tau}$ vorremmo poter dire che

$$\exists n.\exists \overline{\sigma}_1,\dots,\exists \overline{\sigma}_n.\begin{cases} \overline{step}(\overline{\sigma}) = \overline{\sigma}_1 \\ \overline{step}(\overline{\sigma}_1) = \overline{\sigma}_2 \\ \quad\vdots \\ \overline{step}(\overline{\sigma}_n) = \overline{\tau} \end{cases}$$

ed usando quanto appena osservato questo equivale a dire che

$$\exists n.\exists \overline{\sigma}_1,\dots,\exists \overline{\sigma}_n.\overline{step}(\overline{\sigma} \oplus \overline{\sigma}_1 \oplus \dots \oplus \overline{\sigma}_n) = \overline{\sigma}_1 \oplus \dots \oplus \overline{\sigma}_n \oplus \overline{\tau}$$

[6] al netto di un dettaglio che andrebbe corretto: quando abbiamo definito f e quindi $[f]$ con gli shift a destra ed a sinistra queste due operazioni cambiano la lunghezza della sequenza ma nella costruzione di $[\cdot]$ le sequenze dovevano avere tutte la stessa lunghezza; dovremmo invece mostrare che è diofante anche una variazione shift a destra ed a sinistra che rimuove o aggiunge degli zeri per fare in modo che la lunghezza non cambi

dove abbiamo ridotto il numero di volte che applichiamo $\overline{step}$ ad una volta sola; però chiaramente questa ancora non è una formula accettabile per colpa di quell'n che fa variare il numero di quantificatori, però possiamo chiamare $\alpha \doteq \overline{\sigma}_1 \oplus \cdots \oplus \overline{\sigma}_n$ e questo quindi equivale a dire che

$$\exists\, \alpha.\overline{step}(\overline{\sigma} \oplus \alpha) = \alpha \oplus \overline{\tau}$$

e questa formula è diofantea[7]. □

In questo modo abbiamo quasi dimostrato il teorema, il problema è che ci siamo ridotti al caso di macchine di Turing con nastri di lunghezza finita. Cerchiamo adesso di concludere dimostrando che questo funziona per tutte le macchine di Turing (e quindi che tutti gli insiemi ricorsivamente enumerabili sono diofantei).

Se X è ricorsivamente enumerabile allora esiste una macchina di Turing M tale che dando in input $\overbrace{1\ldots1}^{n}$ ad M l'esecuzione di M termina (ovvero M arriva nello stato 0) se e solo se $n \in X$.

Quindi possiamo dire che

$$n \in X \iff \exists\, m.\exists\, N.(1, 0, \overbrace{1\ldots1}^{n}\overbrace{0\ldots0}^{m}) \overset{M^\star}{\to} (0, 0, N)$$

dove N è un nastro valido, infatti se $n \in X$ allora nell'esecuzione di M a partire da un qualunque nastro composto da n uni in testa e zero nelle successive posizioni per finitezza del numero di passi eseguiti da M esisterà una massima posizione delle celle visitate da M.

Perché questo si verifichi in maniera diofantea basta eventualmente alterare $\overline{step}$ in modo tale che se si raggiunge la fine del nastro la macchina non fa niente e va in loop; infatti è diofanteo costruire la configurazione iniziale $(1, 0, \overbrace{1\ldots1}^{n}\overbrace{0\ldots0}^{m})$ e quindi si conclude applicando il lemma 11.0.12. □

Corollario 11.0.12.1

Il decimo problema di Hilbert non ha soluzione.

Dimostrazione. Consideriamo l'insieme della fermata H_1 che è ricorsivamente enumerabile (8.3), quindi per il teorema 11.0.7 l'insieme H_1 è diofanteo; se per assurdo il decimo problema di Hilbert avesse soluzione allora esisterebbe un algoritmo che risolve il problema della fermata, che è assurdo in quanto H_1 non è decidibile (8.2.5). □

[7] al netto di un dettaglio: per fare si che sia vera l'equivalenza dovremmo anche aggiungere una verifica che tale α è una concatenazione di codifiche valide di configurazioni per la stessa macchina di Turing

Indice analitico