ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea in Matematica

LOGICA MODALE DELLA DIMOSTRABILITÀ

Tesi di Laurea in Logica

Relatore:
Chiar.ma Prof.ssa
Giovanna Corsi

Presentata da:
Carlotta Dainesi

I Sessione
Anno Accademico 2011/12

.....

Introduzione

Le basi concettuali della *logica modale* nascono in epoca greca con l'analisi delle proposizioni contenenti le espressioni ''necessario'' e '' possibile'' fatta da Aristotele. Essa studia le ''modalità'' in cui una proposizione può essere proferità: modalità positiva, negativa, necessaria, possibile, impossibile...
In questo nostro lavoro non vedremo come queste basi sono progredite nel corso della storia, nel mondo antico come nel medioevo, ma partiremo dagli sviluppi della logica modale moderna ottenuti nella seconda metà del secolo scorso. In particolare ci concentreremo sui risultati raggiunti da Kripke (1959) grazie all'introduzione di modelli matematici, i *Modelli Kripkiani.* In essi gli enunciati sono veri o falsi in un mondo non solo a seconda del valore di verità/falsità che assumono in quel preciso mondo, ma anche in funzione del valore assunto in tutti gli altri mondi accessibili, relati al primo. Kripke riprende così la teoria di Leibnitz, per il quale un enunciato necessario è vero se risulta tale in tutti i mondi possibili, con la differenza che, per Kripke, i mondi possibili da considerare sono solo quelli relati al mondo in considerazione; quindi utilizzando la formalizzazione dell'idea intuitiva di ''mondo possibile'' di Leibnitz, Kripke interpreta la necessità come verità in tutti i mondi accessibili rispetto a quello dato.

Un modello Kripkiano non è altro che una tripla $< \mathcal{W}, \mathcal{R}, \mathcal{I} >$ costituita da un insieme $\mathcal{W}$ non vuoto detto *universo*, una relazione binaria $\mathcal{R}$ su $\mathcal{W}$ detta *relazione di accessibilità* e una relazione $\mathcal{I}$ tra mondi e lettere proposizionali che specifica quali di queste sono vere e in quali mondi. Pertanto, ad esempio, l'enunciato $\Box A$ da leggersi come ''è necessario che A'' è vero in w appartenente a $\mathcal{W}$ se e solo se A è vera in tutti i mondi x relati con w, wRx, analogamente $\Diamond A$ tradotto come ''è possibile che A'' è vero in $w \in \mathcal{W}$ se e solo se $\exists x \in \mathcal{W}$ tale che $w\mathcal{R}x$

Un enunciato del tipo $\Box A$ o $\Diamond A$ può però ammettere diverse letture a seconda di come viene interpretao e tradotto il simbolo logico in esse contenuto, rispettivamente $\Box$ e $\Diamond$. Ad esempio $\Box$ può essere letto come ''sempre in futuro", ''sempre in passato", ''è obbligatorio", ''dopo ogni esecuzione di un dato programma". Per quanto ci riguarda siamo interessati a leggere $\Box$ come ''è dimostrabile in PA che'' e il nostro obiettivo sarà quello di mettere in relazione i teoremi della logica modale GL (da Gödel e Löb) con quelli dell'Aritmetica di Peano (PA). Gödel,''Eine interpretation des intuitionistichen Aussagenkalküls'' (1933).
Questo rapporto verrà precisato dal *Teorema di Solovay* il quale sancisce definitivamente il legame presente tra teorematicità in GL e teorematicità in PA. Da qui, la logica GL viene anche detta *Logica della dimostrabilità*

Questa tesi si articola in tre capitoli.
Nel primo di questi si analizzano le logiche modali K e GL. Il linguaggio di queste due logiche è lo stesso, si tratta di un linguaggio proposizionale classico arricchito con l'operatore $\Box$ a cui, in un primo momento, non attribuiamo alcuna interpretazione specifica.
Siamo partiti dalle nozioni fondamentali della logica modale definendo la sua sintassi (alfabeto, simboli logici, formule ben formate,..) e la sua semantica. Qui abbiamo introdotto la nozione di mondo possibile, di relazione di accessibilità e di funzione di interpretazione quale funzione che dichiara quali sono i mondi in cui una variabile enunciativa è vera; abbiamo cioè illustrato i modelli che nel 1959 furono introdotti da Kripke proprio nello studio della logica modale (''A completeness theorem in modal logic"). Abbiamo poi de-

finito i concetti di verità in un punto, verità in un modello e validità su una struttura.
Come vedremo, l'insieme degli enunciati validi su una struttura è una logica modale normale e la logica K si lascia descrivere come l'intersezione di tutte le logiche modali normali. Non solo, una tale logica è anche assiomatizzabile, ovvero descrivibile attraverso un insieme finito di schemi di assiomi e di regole di inferenza.
La logica GL non è altro che un'estensione della prima ottenuta aggiungendo a K un altro assioma, l'assioma G. Di entrambe abbiamo dimostrato validità e completezza.

Nel secondo capitolo abbiamo introdotto l'Aritmetica di Peano (PA) e considerato alcune sue proprietà metateoriche. Risulta fondamentale, in questo capitolo, tener bene presente che abbiamo ''lavorato'' su tre piani distinti: il primo costituito da PA, con il suo linguaggio e le sue regole, il secondo costituito dalla metateoria e il terzo ottenuto mediante l'aritmetizzazione. In altre parole per studiare PA dentro PA stesso abbiamo tradotto ogni proposizione di PA in un numero e ogni relazione logica tra proposizioni in una relazione aritmetiche tra numeri; per fare questo utilizziamo la tecnica di gödelizzazione.
Nello specifico applicando tale tecnica abbiamo associato un numero ad ogni formula in modo da poter eseguire univocamente anche il passaggio inverso, risalire cioè dalla formula al numero senza ambiguità, poi abbiamo tradotto in relazioni aritmetiche le relazioni originarie tra segni in PA utilizzando le funzioni ricorsive. Sappiamo infatti, per un noto teorema, che queste funzioni sono fortemente rappresentabili in PA.
A questo punto abbiamo tradotto l'asserto metateorico ''essere dimostrazione di'' in asserto aritmetico attraverso la definizione del predicato aritmetico $D(x, y)$ verificato solo quando la sequenza di formule con gödeliano x è dimostrazione della formula con gödeliano y. Essendo questo predicato ricorsivo per definizione, risulta fortemente rappresentabile in PA e quindi abbiamo

definito $Dim(x, y)$ la formula nel linguaggio di PA che traduce D. Siamo così giunti a definire, grazie a *Dim*, la formula *Teor* di PA che traduce formalmente la proprietà di "essere dimostrabile", e ne abbiamo illustrato le proprietà.

Il terzo capitolo risulta il fulcro di questo nostro lavoro; in esso abbiamo confrontato il sitema GL con la teoria PA e siamo giunti alla corrispondenza enunciata all'inizio di questa introduzione. Stabilendo un'opportuna traduzione da GL a PA il teorema di Solovay sancisce una sorta di relazione biunivoca tra il simobolo $\Box$ e la proprietà di "essere dimostrabile".

Indice

Capitolo 1

LA LOGICA MODALE

In questo capitolo studieremo la logica modale e in particolare la Logica K e la Logia GL.

1.1 Sintassi

Definizione 1.1. L'*Alfabeto* di un linguaggio enunciativo modale $\mathcal{L}^\Phi$ è costituito da:

- un insieme Φ al massimo numerabile di variabili enunciative: $p, q, r \ldots$
- la costante logica zero-aria $\perp$
- la costante logica unaria $\Box$
- la costante logica binaria $\rightarrow$
- le parentesi $(,)$.

Definizione 1.2. L'insieme $\mathcal{F}m^\Phi$ delle formule ben formate, fbf, di $\mathcal{L}^\Phi$ è il piu piccolo insieme X tale che:

- $\phi \subseteq X$
- $\perp \in X$

- se $A \in X$, allora $\Box A \in X$
- se $A \in X$, allora $(A \to B) \in X$.

Le prime due condizioni stabiliscono quali sono gli elementi iniziali di $\mathcal{F}m^{\Phi}$, le restanti stabiliscono le operazioni con le quali otteniamo nuovi elementi a partire da elementi già in X. Un insieme così costruito si dice definito per *induzione*.

Definizione 1.3. Alcuni simboli logici definiti:

$$\begin{aligned} \top &\triangleq (\bot \to \bot) \\ \neg A &\triangleq (A \to \bot) \\ \Diamond A &\triangleq \neg\Box\neg A \\ (A \land B) &\triangleq \neg(A \to \neg B) \\ (A \lor B) &\triangleq (\neg A \to B) \\ (A \leftrightarrow B) &\triangleq ((A \to B) \land (B \to A)) \end{aligned}$$

Definizione 1.4. Sia p una lettera enunciativa e A una formula. Definiamo per ricorsione sulla costruzione della formula A, l'operazione di *sostituzione uniforme* di A per p in una proposizione F, $F_p(A)$:

- se $F = p$ allora $F_p(A) = A$
- se $F = q$ con q variabile proposizionale tale che $p \neq q$ allora $F_p(A) = q$
- se $F = \bot$ allora $F_p(A) = \bot$
- $(F \to G)_p(A) = (F_P(A) \to G_P(A))$
- $\Box(F)_p(A) = \Box(F_p(A))$

$F_{p_1}(A_1)\ldots_{p_k}(A_k)$ denota una formula ottenuta a partire da F sostituendo *simultaneamente* ogni occorrenza di p_1 con A_1, ..., ogni occorrenza di p_k con A_k.

1.2 Semantica

La semantica di un linguaggio Modale utilizza la nozione di *mondo possibile*. Se abbiamo a che fare con i concetti di possibilità e necessità siamo intuitivamente portati a stabilire confronti con mondi diversi da quello attuale per stabilire validità o meno di enunciati contenenti quei concetti. Dire ad esempio che la radice quadrata di 9 è 3, significa affermare che in ogni mondo possibile rispetto a quello all'attuale quella relazione aritmetica sussiste. Viceversa la possibilità si configurerà come la verità in almeno uno tra tutti i mondi possibili.
Ora, come precedentemente accennato, per Leibnitz la verità di un enunciato, ad esempio $\Box A$, dipende dalla verità che possiede in tutti i mondi prossibili, invece, per Kripke occorre introdurre una relazione binaria (*relazione di accessibilità*) per ridurre questa dipendenza ai soli mondi relati al mondo attuale.
Introdotta questa relazione arriviamo così a definire:

Definizione 1.5. *Frame* una coppia :

$$\mathcal{F} =< \mathcal{W}, \mathcal{R} >$$

dove:

- $\mathcal{W}$ è un insieme non vuoto detto *Universo* e i cui elementi son detti *mondi*
- $\mathcal{R} \subseteq \mathcal{W} \times \mathcal{W}$ è una relazione binaria detta *Relazione di accessibilità* .

Definizione 1.6. Data una struttura relazionale $\mathcal{F} =< \mathcal{W}, \mathcal{R} >$, definiamo *modello* basato su $\mathcal{F}$ una tripla:

$$\mathcal{M} =< \mathcal{W}, \mathcal{R}, \mathcal{I} >$$

dove $\mathcal{I}$ è una funzione di *interpretazione* che associa ad ogni variabile enunciativa un sottinsieme di $\mathcal{W}$:

$$\mathcal{I} : \Phi \rightarrow \mathcal{P}(\mathcal{W})$$

$$\mathcal{I}(p) \subseteq \mathcal{W}$$

Intuitivamente la funzione di interpretazione ci dice quali sono i mondi in cui una variabile enunciativa è vera.

1.2.1 Verità e validità

Definizione 1.7. verità in un mondo
Dato un modello $\mathcal{M} =< \mathcal{W}, \mathcal{R}, \mathcal{I} >$, definiamo per induzione sulla costruzione delle formule quand'è che una fbf è *vera in un mondo* w di $\mathcal{M}$, $\mathcal{M} \models A$:

- $\mathcal{M} \models_w p$ sse $w \in \mathcal{I}(p)$
- $\mathcal{M} \not\models_w \bot$
- $\mathcal{M} \models_w B_1 \rightarrow B_2$ sse $\mathcal{M} \not\models_w B_1$ oppure $\mathcal{M} \models_w B_2$
- $\mathcal{M} \models_w \Box B$ sse per ogni $v \in \mathcal{W}$: se $w\mathcal{R}v$ allora $\mathcal{M} \models_v B$

Definizione 1.8. verità in un modello
Diciamo che una formula A è *vera in un modello* $\mathcal{M}$, $\mathcal{M} \models A$, se e solo se essa è vera in ogni mondo del modello. Formalmente:

$$\mathcal{M} \models A \quad \text{sse} \quad \text{per ogni} \quad w \in \mathcal{W} : \mathcal{M} \models_w A$$

Definizione 1.9. validità su una struttura
Una formula A è *valida su una struttura* $\mathcal{F}$, $\mathcal{F} \models A$, se e solo se essa è vera in ogni modello costituito dalla srtuttura. Formalmente:

$$\mathcal{F} \models A \quad \text{sse} \quad \text{per ogni} \quad \mathcal{M} \text{ basato su } \quad \mathcal{F} : \mathcal{M} \models_w A$$

Definizione 1.10. validità
Una formula è *valida* se e solo se essa è valida su ogni struttura. Formalmente:

$$\models A \quad \text{sse per ogni} \quad \mathcal{F} : \mathcal{F} \models A$$

1.2.2 Regole

Introduciamo a questo punto le regole base della logica modale che ci serviranno per mostrare cos'è la logica modale; è facile vedere come tali regole conservano la validità su una struttura.

- *Modus Ponens*
$$\frac{A \qquad A \to B}{B} \qquad \text{MP}$$

- *Necessitazione*
$$\frac{A}{\Box A} \qquad \text{N}$$

- *Sostituzione Uniforme*
$$\frac{A}{A_p(B)} \qquad \text{SU}$$

1.2.3 Definizione insiemistica di alcune logiche

Caratterizziamo alcuni tipi di logiche:

Definizione 1.11. Una *Logica Classica* è un insieme $X \subseteq \mathcal{F}m^{\Phi}$ tale che:

1. contiene gli schemi:
   - $A \to (B \to A)$
   - $A(B \to C) \to (A \to B) \to (A \to C))$
   - $((A \to \bot) \to \bot) \to A$
2. è chiuso sotto *MP*
3. è chiuso sotto *SU*

Definizione 1.12. Una *Logica Modale* è una logica classica contenente lo schema:

- $\Box(A \to B) \to (\Box A \to \Box B)$

Definizione 1.13. Una *Logica Modale Normale* è una logica modale che:

- e chiusa sotto N

Definizione 1.14. Gli elementi di una logica modale normale L sono chiamati *Teoremi* e li indicheremo con:

$$L \vdash A$$

Definizione 1.15. Sia $\mathcal{C}$ una classe di strutture.
Una logica L è *valida* rispetto a $\mathcal{C}$ se per ogni $A \in \mathcal{F}m^{\Phi}$:

$$L \vdash A \Rightarrow \mathcal{C} \models A$$

Una logica L è *completa* rispetto a $\mathcal{C}$ se per ogni A:

$$\mathcal{C} \models A \Rightarrow L \vdash A$$

1.3 La Logica K

Consideriamo il sistema il cui insieme di teoremi è formato da tutte le tautologie, dalle proposizioni della forma $\Box(A \to B) \to (\Box A \to \Box B)$, ed è chiuso rispetto alla necessitazione e al modus ponens; otteniamo la logica modale K o sistema Kripkiano, che costituisce la più piccola logica normale. Vediamo ora dei teoremi di K che si riveleranno utili in seguito:

Teorema 1.3.1. *Supponiamo $K \vdash A \to B$.*
Allora $K \vdash \Box A \to \Box B$.

Dimostrazione.
Applicando la Regola di Necessitazione sappiamo che: $K \vdash \Box(A \to B)$
Da cio segue:
$K \vdash \Box(A \to B) \to (\Box A \to \Box B)$ poichè K è logica modale
$K \vdash \Box A \to \Box B$ per MP.

$\Box$

Teorema 1.3.2. *Supponiamo $K \vdash A \leftrightarrow B$.*
Allora $K \vdash \Box A \leftrightarrow \Box B$.

Dimostrazione.
Dalle Ipotesi segue che: $K \vdash A \to B$ e $K \vdash B \to A$
Ora, per il teorema (1.3.1):
$K \vdash \Box A \to \Box B$
$K \vdash \Box B \to \Box A$.
La tesi segue dalla verità di entrambe. □

Teorema 1.3.3.
$K \vdash \Box(A \wedge B) \leftrightarrow (\Box A \wedge \Box B)$

Dimostrazione.
Noi sappiamo che: $K \vdash (A \wedge B) \to A$ e $K \vdash (A \wedge B) \to B$ per logica proposizionale, da cui per il teorema (1.3.1):
$K \vdash \Box(A \wedge B) \to \Box A$
$K \vdash \Box(A \wedge B) \to \Box B$
Sempre per logica proposizionale sappiamo che: $K \vdash A \to (B \to (A \wedge B))$ da cui per il teorema (1.3.1):
$K \vdash \Box A \to \Box(B \to (A \wedge B))$
$K \vdash \Box(B \to (A \wedge B)) \to (\Box B \to \Box(A \wedge B))$ per assioma distribuzione e MP.
La tesi segue dalla validità delle affermazioni fatte. □

Teorema 1.3.4.
$K \vdash \Box(A_1 \wedge \cdots \wedge A_n) \leftrightarrow (\Box A_1 \wedge \cdots \wedge \Box A_n)$

Dimostrazione.
Il teorema è valido se $n = 0$, poichè la congiunzione vuota è identificata con $\top$, e $K \vdash \Box\top$.
Il teorema è banale se $n = 1$ ed è già stato provato per $n = 2$.
Se $n > 2$ allora:

$$\begin{aligned} K \vdash \Box(A_1 \wedge A_2 \wedge \cdots \wedge A_n) &\leftrightarrow \Box(A_1 \wedge (A_2 \wedge \cdots \wedge A_n)) \\ &\leftrightarrow \Box A_1 \wedge \Box(A_2 \wedge \cdots \wedge A_n) \\ &\leftrightarrow (\Box A_1 \wedge \Box A_2 \wedge \cdots \wedge \Box A_n) \end{aligned}$$

La prima di queste equivalenze segue dal teorema (1.3.2), la seconda dal teorema (1.3.3) e la terza dall'ipotesi induttiva. $\square$

Teorema 1.3.5. ***Primo teorema di sostituzione***
Supponiamo che $K \vdash A \leftrightarrow B$.
Allora $F_p(A) \leftrightarrow F_p(B)$

Dimostrazione.
Procediamo per induzione sulla complessità di F.
Se $F = p$ la proposizione in conclusione risulta essere un teorema di K solo se lo è $A \leftrightarrow B$;
se $F = q$, è $q \leftrightarrow q$;
se $F = \bot$, risulta $\bot \leftrightarrow \bot$, entrambi teoremi di K.
Se $F = (G \rightarrow H)$ e la conclusione del teorema è valida per G e H, allora essa è valida per F per la logica proposizionale e la definizione di sostituzione.
Infine, se $F = \square(G)$ e $K \vdash G_p(A) \leftrightarrow G_p(B)$, allora per il teorema (1.3.2):
$K \vdash \square(G_p(A)) \leftrightarrow \square(G_p(B))$ cioè
$K \vdash \square(G)_p(A) \leftrightarrow \square(G)_p(B)$ cioè
$K \vdash F_p(A) \leftrightarrow F_p(B)$ $\square$

Introduciamo ora il simbolo '$\Diamond$' come abbreviazione di '$\neg\square\neg$'. Si dimostra che valgono le seguenti relazioni:

- se $K \vdash A \rightarrow B$ allora $K \vdash \Diamond A \rightarrow \Diamond B$
- se $K \vdash A \leftrightarrow$ B allora $K \vdash \Diamond A \leftrightarrow \Diamond B$
- $K \vdash \Diamond A \wedge \square B \rightarrow \Diamond(A \wedge B)$

1.4 La Logica GL

La logica GL è un sistema della logica modale che deve il suo nome a Gödel e Löb.
GL è un sistema normale e pertanto, come già detto, l'insieme dei suoi teoremi contiene tutte le tautologie del calcolo proposizionale, tutte le proposizioni modali della forma $\Box(A \to B) \to (\Box A \to \Box B)$ ed è chiuso rispetto alle regole di Modus Ponens, Sostituzione e Necessitazione.
A tutti questi assiomi e regole si aggiunge l'assioma caratterizzante di GL, detto *Assioma G*:

$$\Box(\Box A \to A) \to \Box A.$$

E' ovvio che ogni teorema di K risulta essere teorema anche di GL e quindi nelle dimostrazioni in GL faremo ampio uso dei teoremi di K dandoli per assodati.

Teorema 1.4.1.
$GL \vdash \Box A \to \Box\Box A$

Dimostrazione.
Per la logica proposizionale abbiamo: $GL \vdash A \to ((\Box\Box A \wedge \Box A) \to (\Box A \wedge A))$
da cui segue:
$GL \vdash A \to (\Box(\Box A \wedge A) \to (\Box A \wedge A))$ per teo.di K
$GL \vdash \Box A \to \Box(\Box(\Box A \wedge A) \to (\Box A \wedge A))$ ancora per teo.di K .
Ma, ponendo $B = (\Box A \wedge A)$: $\Box(\Box B \to B) \to \Box B$ è assioma di GL
quindi:
$GL \vdash \Box(\Box(\Box A \wedge A) \to (\Box A \wedge A)) \to \Box(\Box A \wedge A)$.
$GL \vdash \Box A \to \Box(\Box A \wedge A)$ verità funzionale
$Gl \vdash \Box(\Box A \wedge A) \to \Box\Box A$ per teo.di K .
Da queste ultima affermazioni segue che:
$GL \vdash \Box A \to \Box\Box A$. □

Teorema 1.4.2.

$$GL \vdash \Box(\Box A \to A) \quad \leftrightarrow \quad \Box A \tag{1.1}$$

$$GL \vdash \Box(\Box A \to A) \quad \leftrightarrow \quad \Box(\Box A \wedge A) \tag{1.2}$$

Dimostrazione. (1.1)
$(\to)$
sempre verificato in quanto assioma G.
$(\leftarrow)$
Sappiamo che: $GL \vdash A \to (\Box A \to A)$
da cui segue:
$GL \vdash \Box(A \to (\Box A \to A))$ per N
$GL \vdash \Box A \to \Box(\Box A \to A)$ per distribuzione. $\Box$

Dimostrazione. (1.2)
$(\leftarrow)$
Sappiamo che: $GL \vdash \Box A \wedge A \to (\Box A \to A)$ per tautologia
da cui:
$GL \vdash \Box(\Box A \wedge A) \to \Box(\Box A \to A)$ per N e distribuzione.
$(\to)$
E' noto che: $GL \vdash ((\Box A \to A) \wedge \Box A) \to A$ per tautologia
da cui segue:
$GL \vdash ((\Box A \to A) \wedge \Box A) \to \Box A$ sempre per tautologia
$GL \vdash ((\Box A \to A) \wedge \Box A) \to \Box A \wedge A$
$GL \vdash \Box((\Box A \to A) \wedge \Box A) \to \Box(\Box A \wedge A)$ per proprietà di $\Box$
$GL \vdash \Box(\Box A \to A) \wedge \Box\Box A \to \Box(\Box A \wedge A)$ per distribuzione
$GL \vdash \Box(\Box A \to A) \wedge \Box A \to \Box(\Box A \wedge A)$ per proprietà di $\Box$
Ora, essendo i due termini della congiunzione equivalenti per il punto (1.1) appena dimostrato:
$GL \vdash \Box(\Box A \to A) \to \Box(A \wedge \Box A)$. $\Box$

Teorema 1.4.3. *Se* $GL \vdash (\Box A_1 \wedge A_1 \wedge \cdots \wedge \Box A_n \wedge A_n \wedge \Box B) \rightarrow B$ *allora* $GL \vdash (\Box A_1 \wedge \cdots \wedge \Box A_n) \rightarrow \Box B$.

Dimostrazione.
Dall'ipotesi segue che:
$GL \vdash \Box A_1 \wedge A_1 \wedge \cdots \wedge \Box A_n \wedge A_n \rightarrow (\Box B \rightarrow B)$
$GL \vdash \Box(\Box A_1 \wedge A_1) \wedge \cdots \wedge \Box(\Box A_n \wedge A_n) \rightarrow \Box(\Box B \rightarrow B)$ per teo.di K
Dall'equivalena del teorema (1.4.2) segue:
$GL \vdash (\Box A_1 \wedge \cdots \wedge \Box A_n) \rightarrow \Box B$. □

Teorema 1.4.4.
$GL \vdash \Box\bot \leftrightarrow \Box\Diamond p$

Dimostrazione.
$(\rightarrow)$
$GL \vdash \bot \rightarrow \Diamond p$ poichè l'antecedente è sempre falso
$GL \vdash \Box\bot \rightarrow \Box\Diamond p$ per teo.di K
$(\leftarrow)$
$GL \vdash p \rightarrow \top$ poichè il conseguente è sempre vero.
$GL \vdash \Diamond p \rightarrow \Diamond\top$ per teo.di K .
Ma sappiamo che:

$$\begin{aligned} \Diamond\top &\leftrightarrow \neg\Box\neg\top \\ &\leftrightarrow \neg\Box\bot \\ &\leftrightarrow (\Box\bot \rightarrow \bot) \end{aligned}$$

da cui:
$GL \vdash \Diamond\top \rightarrow (\Box\bot \rightarrow \bot)$
allora:
$GL \vdash \Diamond p \rightarrow (\Box\bot \rightarrow \bot)$
$GL \vdash \Box\Diamond p \rightarrow \Box(\Box\bot \rightarrow \bot)$ per teo.di K .
Seguono:
$GL \vdash \Box(\Box\bot \rightarrow \bot) \rightarrow \Box\bot$
$GL \vdash \Box\Diamond p \rightarrow \Box\bot$ per assioma G. □

Teorema 1.4.5.
$GL \vdash \Box\Diamond\bot \to \Box\bot$

Dimostrazione.
Segue immediatamente sostituendo $\bot$ al posto di p nel teorema (1.4.4). $\Box$

Abbiamo così fornito una rapida descrizione della forza di GL.
Per il momento non ci siamo preoccupati di dare una definizione precisa e rigorosa dell'operatore modale $\Box$ e del suo *significato*. Questa precisazione la otterremo solo alla fine della nostra analisi su GL e PA, quando dimostreremo il *Teorema di Solovay*.

1.5 Validità di K e GL

Come già accennato nei paragrafi precedenti un mondo possibile è detto *accessibile* da un altro mondo se e solo se è in relazione con esso.
A questo punto viene naturale domandarsi se tale relazione debba godere di certe proprietà oppure se una qualunque relazione binaria risulti accettabile per definire l'accessibilità ad un mondo.
Per esempio, supponiamo la realazione $\mathcal{R}$ sia transitiva; allora tutti i mondi accessibili da altri mondi che sono a loro volta accessibili al mondo attuale risultano essi stessi accessibili dal mondo attuale. Pertanto segue che se l'evento "è necessario che A" è vero, allora A è vero in tutti i mondi x accessibili al mondo attuale e quindi A risulta vero in ogni mondo y accessibile da ciascun mondo x accessibile dal mondo attuale. Da questo risultato otteniamo che l'evento $\Box A$ è vero in ogni mondo x accessibile al mondo attuale e quindi è esso stesso necessario, ovvero $\Box(\Box A)$ è vero nel mondo attuale.
In altre parole, se la relazione di accessibilità è transitiva, data la validità dell'evento "è necessario che A" segue che l'evento "è necessario che A" è anch'esso necessario, o in termini logici:

$$\text{se } \mathcal{R} \text{ transitiva allora} \quad \Box A \to \Box\Box A$$

Possiamo quindi affermare che è la relazione di accessibilità a determinare la natura del modello di cui fa parte e di conseguenza a stabilire in base alle proprie caratteristiche se una logica risulta valida e completa rispetto ad una classe di modelli.
Analizziamo pertanto quali condizioni deve avere $\mathcal{R}$ affinchè la logica K e la logica GL siano valide e complete rispetto alla classe delle strutture in cui $\mathcal{R}$ gode di quelle proprietà.

<u>Consideriamo il sistema K.</u>
Il sistema K risulta valido in tutte le possibili strutture, poichè le tautologie e l'assioma K sono sempre validi. Inoltre l'insieme delle proposizioni valide in un modello è chiuso rispetto alle regole di modus ponens e necessitazione quindi questi risultati non richiedono ad $\mathcal{R}$ di soddisfare particolari condizioni.

Al contrario GL, come altre logiche modali, trova un'interpretazione adeguata solo in alcuni modelli; questo poichè il suo assioma specifico, *assioma G*, richiede che valgano determinate relazioni tra le proposizioni contenenti l'operatore modale.

Teorema 1.5.1.
$\Box p \to \Box\Box p$ è valido in $<\mathcal{W},\mathcal{R}>$ sse $\mathcal{R}$ è transitiva.

Dimostrazione.
$(\to)$
Supponiamo $\Box p \to \Box\Box p$ sia valida su una struttura $<\mathcal{W},\mathcal{R}>$ e facciamo vedere che $\mathcal{R}$ è transitiva.
Supponiamo ora per assurdo $\mathcal{R}$ non sia transitiva ovvero esistano tre mondi $w, x, y \in \mathcal{W}$ tali che:

$$w\mathcal{R}x \quad x\mathcal{R}y \quad w\neg\mathcal{R}y$$

e costruiamo $\mathcal{I}$ tale che:

$$\mathcal{I}(p) = \{z : w\mathcal{R}z\}$$

Ora, per definizione di $\mathcal{R}$ abbiamo che $w \models \Box p$ e per ipotesi $w \models \Box\Box p$.
Pertanto, per definizione di $\models$, $x \models \Box p$ e $y \models p$, da cui $w\mathcal{R}y$. ma tale risultato è un assurdo per le ipotesi fatte quindi una tale terna di mondi non esiste e quindi $\mathcal{R}$ è transitiva.
$(\leftarrow)$
Supponiamo $< \mathcal{W}, \mathcal{R} >$ sia una frame transitiva.
Poniamo che $w \models \Box p$.
Avremo che: $\forall x$ tale che $w\mathcal{R}x$: $x \models p$.
Inoltre, consideriamo tutti gli y tali che $x\mathcal{R}y$.
Data la transitività di $\mathcal{R}$ sarà anche: $w\mathcal{R}y$, per cui, $\forall y \quad y \models p$.
Quindi: $x \models \Box p$, da cui, $w \models \Box\Box p$
Infine: $w \models \Box p \rightarrow \Box\Box p$. $\Box$

Introduciamo ora una definizione importante.

Definizione 1.16. Una relazione $\mathcal{R}$ si dice *inversamente ben fondata* se per ogni insieme non vuoto X, esiste un elemento $\mathcal{R}$-massimale, cioè un $w \in X$ tale che $w\mathcal{R}x$ per nessun x in X.

Se $\mathcal{R}$ è inversamente ben fondata, allora $\mathcal{R}$ è irriflessiva, poichè se $w\mathcal{R}w$ allora $\{w\}$ è un insieme non vuoto senza elementi $\mathcal{R}$-massimali.
Inoltre se $\mathcal{R}$ è una relazione inversamente ben fondata su $\mathcal{W}$, allora per provare che ogni membro di $\mathcal{W}$ ha una certa proprietà ψ, è sufficiente mostrare che un mondo arbitrario w gode di ψ dall'assunzione che tutti i suoi $\mathcal{R}$-successori godono di ψ. (Questa tecnica di dimostrazione è detta *induzione sull'inversione di* $\mathcal{R}$).
Per mostrare questa tecnica, assumiamo che per tutti w, w ha ψ se tutti gli x tali che $w\mathcal{R}x$ hanno ψ, e sia $X = \{w \in \mathcal{W} : w \quad \text{non possiede} \quad \psi\}$. Mostriamo che X non ha nessun elemento $\mathcal{R}$-massimale: supponiamo $w \in X$.

Allora w non ha ψ e dalla nostra assunzione, per qualche x, $w\mathcal{R}x$ e x non ha ψ. Ma $x \in \mathcal{W}$ poichè $\mathcal{R}$ è per definizione una relazione su $\mathcal{W}$, e così $x \in X$. Quindi è proprio vero che X non possiede elementi $\mathcal{R}$-massimali.
Ora, dato che $\mathcal{R}$ è inversamente ben fondata, X deve esser vuoto, ed ogni w in $\mathcal{W}$ possiede la proprietà ψ

Consideriamo ora GL.
Sappiamo che '$\Box A \rightarrow \Box\Box A$' è un suo teorema. E' chiaro quindi che l'insieme dei teoremi di GL sarà un sottinsieme dell'insieme di frame transitive.

Teorema 1.5.2.
$\Box(\Box p \rightarrow p) \rightarrow \Box p)$ *è valida nella frame* $< \mathcal{W}, \mathcal{R} >$ *se e solo se* $\mathcal{R}$ *è transitiva e inversamente ben fondata.*

Dimostrazione.
$(\rightarrow)$
Si $w \models \Box(\Box p \rightarrow p) \rightarrow \Box p$.
Assumiamo per assurdo che $\mathcal{R}$ non sia inversamente ben fondata. Questo significa che esiste un insieme X non vuoto tale che in X non esiste un elemento $\mathcal{R}$-massimale.
Poniamo che $w \in X$ e sia $\mathcal{I}$ l'interpretazione:

$$\mathcal{I}(p) = \{p : a\mathcal{R}p \quad \text{con} \quad a \in \mathcal{W} - X\}$$

Supponiamo $w\mathcal{R}x$ e assumiamo che $x \not\models p$.
Da qui deduciamo che non $x \notin \mathcal{I}(p)$; per cui $x \in X$.
Dato che abbiamo supposto che in X non vi sia un elemento $\mathcal{R}$-massimale, esisterà un $y \in X$ tale che $x\mathcal{R}y$.
Per la definizione di $\mathcal{I}$, $y \not\models p$, per cui $x \not\models \Box p$.
Dato che avevamo assunto che $x \not\models p$, otteniamo che $x \models p$ oppure $x \not\models \Box p$.
Avremo dunque: $x \models \Box p \rightarrow p$
e anche: $w \models \Box(\Box p \rightarrow p)$.
Ora $w \in X$, per cui esisterà uno $z \in X$ tale che $w\mathcal{R}z$.

Quindi avremo non $z \notin \mathcal{I}(p)$, da cui $z \not\models p$.
Da qui possiamo concludere: $w \not\models \Box p$.
Otteniamo così una contraddizione: dato che l'ipotesi del teorema è che $w \models \Box(\Box p \to p) \to \Box p$ non può essere che $w \models \Box(\Box p \to p)$ e $w \not\models \Box p$.
$(\leftarrow)$
Sia $\mathcal{R}$ una relazione transitiva e inversamente ben fondata.
Consideriamo un qualsiasi modello $\mathcal{M} =< \mathcal{W}, \mathcal{R}, \mathcal{I} >$ tale che: $\mathcal{M} \not\models_w \Box p$.
Definiamo ora un insieme $X = \{x \in \mathcal{W} : w\mathcal{R}x \quad \wedge \quad x \not\models p\}$
Dato che $w \not\models \Box p$, esisterà almeno un z tale che $w\mathcal{R}z$ e $z \not\models p$; per cui X non è vuoto.
Dato che $\mathcal{R}$ è inversamente ben fondata, esisterà un elemento x $\mathcal{R}$-massimale appartenente a X tale che $x\mathcal{R}y$ per nessun $y \in X$.
Per cui, assumendo $x\mathcal{R}y$, dato che $\mathcal{R}$ è transitiva, avremo $w\mathcal{R}y$, e dovrà necessariamente essere $y \models p$ (dato che $y \notin X$).
Per definizione di $\models$ avremo dunque: $x \models \Box p$.
Ma dato che $x \not\models p$, avremo $x \not\models \Box p \to p$.
Considerando che $w\mathcal{R}x$ si ottiene: $w \not\models \Box(\Box p \to p)$
Rimane così dimostrato che se $\mathcal{R}$ è transitiva e inversamente ben fondata: $w \models \Box(\Box p \to p) \to \Box p$ □

Possiamo così dimostrare il seguente teorema:

Teorema 1.5.3. ***Teorema di validità per GL***
Se GL $\vdash A$, allora A è valida in tutte le strutture transitive e inversamente ben fondate.

Dimostrazione. Se A è un teorema di GL o è un assioma o è ottenuto da essi tramite le regole di derivazione. Per dimostrare il teorema dovremo quindi dimostrare che esso vale per gli assiomi di GL, e che l'insieme delle proposizioni valide nelle frame è chiuso rispetto alle regole di derivazione dei sistemi modali.
Gli assiomi di GL sono:

- le tautologie: per esse il teorema vale, in quanto le tautologie sono valide in ogni frame, dato che il loro valore non dipende dalle singole valutazioni. Per cui esse sono valide nelle frame transitive e inversamente ben fondate.

- i singoli esempi dell'assioma di distribuzione: ipotizziamo che $w \models \Box(A \to B)$;per ogni x tale che $w\mathcal{R}x, \quad x \models A \to B$. Assumiamo che $w \models \Box A, \quad x \models A$. Per cui $x \models B$. Da cui otteniamo $w \models \Box B$. Data la definizione di $\models$ otteniamo $w \models \Box(A \to B) \to (\Box A \to \Box B)$. Anche questo assioma è valido senza assunzioni su $\mathcal{R}$.

- l'assioma G, per il teorema (1.5.2), è valido in tutte le frame transitive e inversamente ben fondate.

Poniamo ora che Γ si l'insieme delle proposizioni valide nelle frame $< \mathcal{W}, \mathcal{R} >$, senza assunzioni particolari su $\mathcal{R}$.
Assumiamo che: $A \in \Gamma$ e $A \to B \in \Gamma$.
Data la definizione $\vdash$ avremo che $B \in \Gamma$. Γ è quindi chiuso per MP.
Poniamo ora che $A \in \Gamma$. Per definizione di Γ, per ogni $w \in \mathcal{W}$ avremo che $w \models A$.
Per cui tutti gli x tali che $w\mathcal{R}x, x \vdash A$. Da cui segue che: $w \models \Box A$.
Dato che w è stato scelto in maniera arbitraria avremo $\Box A \in \Gamma$. Quindi Γ è chiuso per N.
Da tutto ciò segue la tesi.

$\Box$

Ovviamente questa dimostrazione riguarda anche K anche se, come detto prima, per essa non è necessario richiedere particolari frame perchè sia valido.

1.6 Completezza di K e GL

Abbiamo appena dimostrato che se $GL \vdash A$, allora A è valida in tutte le frame transitive e inversamente ben fondate. Per affermare che GL è pure completa dobbiamo dimostrare che se A è valida in tutte le frame transitive e inversamente ben fondate allora $GL \vdash A$.
E' necessario prima introdurre alcune definizioni e dimostrare alcuni risultati.

Definizione 1.17. Definiamo per induzione una *sotto-formula*:

- A è sotto-formula di A.
- se B→C è una sotto-formula di A, allora anche B e C lo sono.
- se $\Box B$ è sotto-formula di A, allora anche B lo è.

Teorema 1.6.1. *Se* $< \mathcal{W}, \mathcal{R} >$ *è una frame finita e transitiva allora:* $< \mathcal{W}, \mathcal{R} >$ *è irriflessiva se e solo se è inversamente ben fondata.*

Dimostrazione.
(←)
Se $\mathcal{R}$ è inversamente ben fondata è ovviamente irriflessiva, poichè per definizione:

$$\forall X \subseteq W (\exists w \in X \neg \exists x \in X \quad w\mathcal{R}x)$$

per cui non varrà nemmeno $w\mathcal{R}w$.
(→)
Sia $\mathcal{R}$ irriflessiva.
Se $x_1, \ldots, x_n$ è una sequenza di elementi tali che $x_i\mathcal{R}x_{i+1}$, allora $x_i \neq x_j$ per $i < j$, altrimenti per transitività avremmo $x_i\mathcal{R}x_j$ e $x_i = x_j$ contro l'ipotesi di irriflessività.
Assumiamo per assurdo che $\mathcal{R}$ non sia inversamente ben fondata.
Sia X un sottinsieme di $\mathcal{W}$ tale che: $\forall w \in X \exists x \in X \quad w\mathcal{R}x$
Ora chiaramente per ogni n ci sarà una sequenza $x_1, \ldots, x_n$ di elementi di X tali che $x_i\mathcal{R}x_{i+1}$ per tutti gli $i < n$.

Quindi per ogni n esisteranno almeno n elementi di $X \subseteq \mathcal{W}$, per cui $\mathcal{W}$ non può essere finito, contro l'ipotesi. $\square$

Definizione 1.18. Diremo che una relazione $\mathcal{R}$ è *appropriata* ad un particolare sistema L, se L è valido nelle frame $< \mathcal{W}, \mathcal{R} >$ e solo in quelle.

La stessa definizione si applica direttamente alle frame e ai modelli.

Dobbiamo ora dimostrare che se A è valida in tutte le frame $< \mathcal{W}, \mathcal{R} >$ appropriate per L allora A è un teorema di L.
Procederemo dimostrando l'implicazione inversa: assumeremo cioè che A non è teorema di L e dimostreremo che in questo caso esiste almeno una frame appropriata per L in cui A non è valida.
Sia pertanto D una proposizione modale che non sia teorema di L.

Useremo il termine *formula* per indicare le sotto-formule di D e le loro negazioni, e diremo che un insieme X di formule è *L-coerente* se : $L \nvdash \neg \wedge X$ (dove con $\nvdash$ indichiamo la negazione di $\vdash$ e con $\wedge X$ indichiamo la congiunzione di tutti gli elementi di X). Chiameremo un insieme X di formule *L-coerente e massimale* se X è L-coerente e per ogni sotto-formula A di D, A o la sua negazione appartiene a X.
Chiaramente se X è coerente e massimale:
$A_1, \ldots, A_n \in X$, $L \vdash A_1 \wedge \cdots \wedge A_n \to B$ e B è una sotto-proposizione di D allora $B \in X$, infatti altrimenti $\neg B \in X$, $L \vdash \neg(A_1 \wedge \cdots \wedge A_n \wedge \neg B)$, quindi $L \vdash \neg \wedge X$, contro l'ipotesi di coerenza.
Si dimostra che ogni insieme X coerente è incluso in un insieme coerente e massimale.
Per la logica proposizionale, infatti, $\wedge X$ è equivalente a una disgiunzione $E_1 \vee \cdots \vee E_n$ in cui in ogni disgiunto occorre ogni sotto-proposizione di D o la sua negazione, e tutti i membri di X. Ora, almeno un disgiunto E_i sarà L-coerente altrimenti $L \vdash \neg E_1 \wedge \cdots \wedge \neg E_n$ per cui $L \vdash \neg(E_1 \vee \cdots \vee E_n)$ e quindi $L \vdash \neg \wedge X$, contro l'ipotesi.

E_i è dunque coerente e, per definizione contiene tutti gli elementi di X ed è massimale.

Ora cerchiamo di individuare un modello appropriato per L per cui D non sia valida.
Abbiamo supposto che $L \vdash \neg D$, per cui $\{\neg D\}$ sarà L-coerente, quindi incluso in un insieme y coerenete e massimale. Sia W l'insieme di tutti gli insiemi coerenti e massimali, W non è vuoto dato che $y \in W$. Sia ora $w \in \mathcal{W}$ e sia $\mathcal{I}$ l'interpretazione:

$$\mathcal{I}(p) = \{p : p \in w \quad \text{e} \quad p \text{ occorre come sotto-proposizione in } D\}$$

Sia ora $\mathcal{R}$ una relazione con le seguenti caratteristiche:

1. per ogni sotto-formula del tipo $\Box B$ in D e ogni $w \in W \quad \Box B \in w$ se e solo se per ogni x tale che $w\mathcal{R}x, B \in x$.

2. $< \mathcal{W}, \mathcal{R} >$ è appropriata per L, cioè è un tipo di frame per cui vale il teorema di validità per L.

Per un modello $\mathcal{M} =< \mathcal{W}, \mathcal{R}, \mathcal{I} >$ con le caratteristiche descritte vale il seguente lemma:

Lemma 1.6.2. *Per ogni sotto-formula A di D e per ogni $w \in W$:*
$A \in W$ se e solo se $w \models A$

Dimostrazione. Procediamo per induzione su A.
$A = \bot$ implica che $A \notin w$ (dato che $L \vdash \neg\bot$) e contemporaneamente $w \not\models \bot$.
Se $A = p$ (variabile proposizionale) allora $A \in w$ se e solo se $w \in \mathcal{I}(A)$ se e solo se $w \models A$.
Se $A = B \to C$, il lemma vale per ipotesi induttiva per B e per C. Ora sappiamo che $\neg A$ equivale alla congiunzione $(B \wedge \neg C)$, per cui varranno le seguenti espressioni:

$$L \vdash \neg A \to B \qquad L \vdash \neg A \to \neg C$$

Tenendo presente questo possiamo scrivere le seguenti equivalenze:

$$\begin{aligned} A \notin w \quad & sse \quad \neg A \in W \quad \text{per coerenza e massimalità} \\ & sse \quad B \in w \quad \text{e} \quad \neg C \in w \\ & sse \quad w \models B \quad \text{e} \quad w \models \neg C \quad \text{per ipotesi induttiva} \\ & sse \quad w \not\models A \end{aligned}$$

Per cui: $A = B \to C \qquad A \in w$ sse $w \models A$.
Ora supponiamo che $A = \Box B$: $\Box B \in w$ se e solo se, per definizione di $\mathcal{R}$, per tutti gli x tali che $w\mathcal{R}x$ $B \in x$.
Ma per ipotesi induttiva:

$$\begin{aligned} B \in x \quad & sse \quad x \models B \qquad \text{per tutti gli x tali che} \quad w\mathcal{R}x \\ & sse \quad w \models \Box B \end{aligned}$$

$\Box$

Dimostrato questo risultato, per stabilire la completezza di L bisogna solo individuare una relazione $\mathcal{R}$ che soddisfi le condizioni 1 e 2.
E' chiaro che, a seconda del sistema modale con cui avremo a che fare, le caratteristiche di $\mathcal{R}$ saranno differenti.

1.6.1 Completezza di K

Definiamo una $\mathcal{R}$ in maniera tale che $w\mathcal{R}x$ sse per tutte le proposizioni del tipo $\Box B$ che appartengono a w, $B \in x$.
$\mathcal{R}$ è chiaramente adeguata per K, dato che K non richiede alcuna particolare proprietà ad $\mathcal{R}$ affinchè valga il teorema di validità. Quindi la condizione 2 su $\mathcal{R}$ è soddisfatta.
Per quanto riguarda una parte della condizione 1 notiamo che per definizione di $\mathcal{R}$:

$$\text{se} \quad \Box B \in w \quad \text{e} \quad w\mathcal{R}x \quad \text{allora} \quad B \in x$$

Ora dobbiamo dimostrare che vale l'implicazione inversa contenuta all'interno della condizione 1, cioè:
se $B \in x$ per ogni x tale che $w\mathcal{R}x$ allora deve essere $\Box B \in w$.
Ciò equivale a dimostrare che:
se $\Box B \notin w$ allora esiste almeno un $x \in W$ tale che $w\mathcal{R}x$ e $B \notin x$.
Ipotizziamo che $\Box B \notin w$ e definiamo un insieme $X = \{\neg B\} \cup \{C : \Box C \in w\}$.
Supponiamo che X non sia K-coerente:

$$K \vdash \neg \wedge X, \quad \text{cioè} \quad K \vdash \neg(\neg B \wedge C_1 \wedge \cdots \wedge C_n).$$

Quindi sarà:
$K \vdash (C_1 \wedge \cdots \wedge C_n) \rightarrow B$
$K \vdash (\Box C_1 \wedge \cdots \wedge \Box C_n) \rightarrow \Box B$ per normalità
Dato che tutti i $\Box C$ per definizione appartengono a w sarà anche, per il lemma (1.6.2), $\Box B \in w$.
Per cui se $\Box B \notin w$, X deve essere K-coerente. Ma se X è K-coerente allora è contenuto in un x K-coerente e massimale (cioè $x \in W$).
Ora avremo $\neg B \in X \subseteq x$. Per cui $B \notin x$.
In più, dato che per tutte le proposizioni del tipo $\Box C \in w$, $C \in X \subseteq x$, avremo $w\mathcal{R}x$ per definizione di $\mathcal{R}$

1.6.2 Completezza di GL

Definiamo $\mathcal{R}$ in modo tale che $w\mathcal{R}x$ se e solo se per tutte le proposizioni del tipo $\Box B \in w, \Box B \in x \quad \text{e} \quad B \in x$ e per qualche $\Box F \in x \neg \Box F \in w$.
Cominciamo con lo stabilire se $\mathcal{R}$ è adeguata per GL.
Gli elementi di $\mathcal{W}$, essendo insiemi di sotto-proposizioni di D sono tutti finiti.
Inoltre, affinchè $\mathcal{R}$ sia adeguata è sufficiente che $\mathcal{R}$ sia transitiva.
Se $w\mathcal{R}x$ e $x\mathcal{R}z$ avremo che per tutti i $\Box B \in w$, $\Box B \in x$.
Dato che $x\mathcal{R}z$ sarà anche $\Box B \in z$ e $B \in z$, per cui per definizione di $\mathcal{R} : w\mathcal{R}z$
$\mathcal{R}$ è inoltre irriflessiva: se non lo fosse, infatti, avremmo $w\mathcal{R}w$ per tutti i w.
Per la definizione di $\mathcal{R}$ dovrebbe succedere che per qualche $\Box F \in w$, $\neg\Box F \in w$, il che è impossibile dato che w è coerente e massimale per definizione.

$\mathcal{R}$ è quindi finita, transitiva e irriflessiva.
Per il teorema (1.6.1), $\mathcal{R}$ sarà anche inversamente ben fondata, per cui $\mathcal{R}$ è adeguata per GL.
Passiamo ora ad analizzare la condizione 1 richiesta su $\mathcal{R}$; l'implicazione diretta è chiaramente soddisfatta mentre per l'implicazione inversa dobbiamo dimostrare che se vale $B \in x$ per ogni x tale che $w\mathcal{R}x$, allora vale $\Box B \in w$.
Consideriamo un insieme $X = \{\neg B, \Box B\} \cup \{C, \Box C : \Box C \in w\}$.
Supponiamo che X sia GL-incoerente. Avremo $GL \vdash \neg \wedge X$.
Per cui $GL \vdash \neg(\neg B \wedge \Box B \wedge C_1 \wedge \Box C_1 \wedge \cdots \wedge C_n \wedge \Box C_n)$, per tutte le n proposizioni della forma $\Box C$ presenti in X.
Ora: $GL \vdash C_1 \wedge \Box C_1 \wedge \cdots \wedge C_n \wedge \Box C_n \to (\Box B \to B)$
da cui per normalità: $GL \vdash \Box C_1 \wedge \Box\Box C_1 \wedge \cdots \wedge \Box C_n \wedge \Box\Box C_n \to \Box(\Box B \to B)$.
Ma, GL deriva tutte le proposizioni del tipo $\Box N \to \Box\Box N$, in più in GL vale $\Box(\Box N \to N) \to \Box N$.
Otteniamo dunque: $GL \vdash \Box C_1 \wedge \cdots \wedge \Box C_n \to \Box B$.
Da cui ricaviamo che: $\Box B \in w$.
Se ipotizziamo dunque $\Box B \notin w$, X deve essere GL-coerente e dunque deve essere anche incluso in un insieme x GL-coerente e massimale.
Ma $\neg B \in X$, per cui dato che $X \subseteq x$, $B \notin x$.
Ora manca solo da dimostrare che $w\mathcal{R}x$.
Per definizione sappiamo che se $\Box C \in w$ allora $C \in X \subseteq x$ e $\Box C \in X \subseteq x$.
In più, dato che w è coerente e massimale, da $\Box B \notin w$ ricaviamo $\neg\Box B \in w$ e per definizione $\Box B \in X \subseteq x$.
Dunque si ha $w\mathcal{R}x$.
Notiamo che: se consideriamo frame il cui insieme di mondi possibili è finito, $\mathcal{R}$ è irriflessiva, questo significa che in GL nessun mondo è accessibile a se stesso.

Capitolo 2

L'ARITMETICA DI PEANO

Ogni volta che trattiamo di una qualsiasi teoria T dobbiamo ricordarci che essa altro non è che una "struttura" costituita da un insieme di oggetti U di cui la teoria parla e da un linguaggio L con cui vengono descritti gli oggetti e le loro relazioni; $T =< L, U >$. Se ora decidiamo di analizzare T, ovvero di rendere T l'oggetto del nostro studio, altro non facciamo che determinare una nuova teoria T' il cui universo U' è costituito dalle proposizioni di T , quindi $U' = T$, delle quali parleremo attraverso un linguaggio L'; $T' =< L', T >$. T' prende il nome di *metateoria* relativa a T, T vien detta *teoria oggetto* e L' prende il nome di *metalinguaggio*.
Questa precisazione risulta fondamentale per capire cosa faremo in questo capitolo ovvero studiare l'Aritmetica di Peano (che diventa la nostra teoria oggetto) all'interno di una metateoria che però utilizza come metalinguaggio il linguaggio stesso di PA.
Procederemo con l'esposizione del sistema da noi scelto e passeremo ad illustrare il metodo utilizzato da Gödel nel 1931 per studiare PA.

2.1 Sintassi

Introduciamo l'Aritmetica di Peano al primo ordine; tale teoria contenendo in sè oltre la logica dei predicati anche gli *assiomi di Peano* è in grado di formalizzare l'aritmetica.

Definizione 2.1. L'*alfabeto* del linguaggio PA è costituto da:

- i simboli logici: $\bot$,$\rightarrow$,$\forall$,$\exists$
- una successione infinita numerabile di variabili: $x_1, x_2, x_3 \ldots$
- i simboli ausiliari: (,)
- i simboli descrittivi:
  - il predicato binario identità: =
  - la costante individuale: **0**
  - il simbolo funtoriale unario: **s**
  - i simboli fuontoriali binari: +,×

Per convenzione notazionale considereremo:
$x, y, z \ldots$ le metavariabili necessarie per tradurre le variabili del linguaggio di PA
$=, 0, s, +, \times$ i simboli metalinguistici per indicare i simboli descritti del linguaggio di PA.

Definizione 2.2. Definiamo *termine* di PA per via induttiva:

- ogni variabile è un termine.
- **0** è un termine.
- se t è un termine, allora **s**t è un termine.
- se t_1 e t_2 sono termini, allora anche $(t_1{+}t_2)$ e $(t_1{\times}t_2)$ lo sono.

Useremo *st* come variabile metalinguistica per indicare il successivo di t e di ogni variabile che occorre in un termine diremo che *occorre liberamente*.

Definizione 2.3. Definiamo F le *formule* di PA nel seguente modo:

1. se t_1 e t_2 sono termine allora $t_1 = t_2$ è una formula *atomica*

> **1*** ogni variabile occorrente in $t_1 = t_2$ è detta *libera*

2. $\perp$ è una formula

3. se A e B sono formule allora $(A \to B)$ è una fbf

> **3*** una variabile occorre *libera* in $(A \to B)$ se e solo se occorre libera in A oppure occorre libera in B

4. se A è una fbf e x una variabile allora $\forall xA$ e $\exists xA$ sono fbf

> **4*** una variabile y occorre *libera* in $\forall xA$ se e solo se $y \neq x$ e y occorre libera in A mentre x è detta *vincolata* in A. Analogamente vale per y in $\exists xA$.

Definizione 2.4. Una formula si dice *proposizione*, o *formula chiusa*, quando nessuna variabile occorre libera in essa.

Introduciamo anche i simboli $\neg, \wedge, \vee, \to, \leftrightarrow$ ed $\exists$ con il significato usuale, tutti gli assiomi della logica predicativa del primo ordine e infine, le regole di inferenza Modus Ponens, Sostituzione Uniforme e la regola di Generalizzazione di seguito riportata:

$$\frac{B \to A(x)}{B \to \forall x[A(x)]} \qquad \text{GEN}$$

Definizione 2.5. Definiamo *dimostrazione* in PA di una formula F, una sequenza finita di formule di cui ognuna di esse o è un'assioma del primo ordine o è un altro assioma di PA o è ottenuta da formule precedenti mediante una delle regole di inferenza MP,SU,GEN.

Definizione 2.6. Definiamo Σ-*proposizione* una proposizione costituita da formule atomiche e negazione di formule atomiche per mezzo di congiunzioni, disgiunzioni, quantificatori esistenziali, quantificatori universali delimitanti ("per ogni x meno che y"), ma non da quantificatori negativi o universali.

Definizione 2.7. Definiamo *operazione di sostituzione* per termini e formule, e la indichiamo rispettivamente con $t_v(z)$ e $F_v(z)$ la formula che si ottiene sostituendo il termine z al posto della variabile v all'interno della formula F. Partiamo definendo tale operazione per i termini:

- $t_v(z) = \begin{cases} z & t = v \\ v & t \neq v \end{cases}$
- se $t = t_1 + t_2$ oppure $t = t_1 \times t_2$
  allora $t_v(z) = (t_1)_v(z) + (t_2)_v(z)$ oppure $t_v(z) = (t_1)_v(z) \times (t_2)_v(z)$
- se $t = \boldsymbol{s}t_1$
  allora $t_v(z) = \boldsymbol{s}(t_1)_v(z)$

Passiamo ora alle formule:

- se $F = \perp$
  allora $F_v(z) = \perp$
- se $F = (t = t_1)$
  allora $F_v(t = t_1)(z) = (t_v(z) = (t_1)_v(z))$
- se F è della forma $A \rightarrow B$ e A,B sono formule
  allora $F_v(z) = A_v(z) \rightarrow B_v(z)$
- se F è della forma $\forall x A_v(z)$ dove x è una variabile e A è una formula
  allora, se v è libera per x in F, $F_v(z) = \forall x A_v(z)$ e $F_v(z) = F$ altrimenti.

Gli assiomi non logici che caratterizzano la teoria sono gli *assiomi di Peano*:

(1) $\mathbf{0}\neq \mathrm{s}x$

(2) $\mathrm{s}x = \boldsymbol{s}y \rightarrow x = y$

(3) $x+\mathbf{0} = x$

(4) $x +\boldsymbol{s}\, y = \boldsymbol{s}(x + y)$

(5) $x\times\mathbf{0} = \mathbf{0}$

(6) $x \times\boldsymbol{s}\, y = (x \times y) + x.$

e l'*assioma di induzione*:

(7) siano $F(x)$ una fbf e x una variabile, allora
$F(\mathbf{0}) \wedge \forall x(F(x) \rightarrow F(\boldsymbol{s}x)) \rightarrow \forall x F(x)$

L'ultimo assioma è quindi uno schema di assiomi. Esso raccoglie in sè un'infinità di assiomi mentre gli altri assiomi forniscono le definizioni ricorsive di passaggio al successore, somma e prodotto.
Quindi gli assiomi di PA sono gli assiomi logici, gli assiomi ricorsivi per il successore, somma e prodotto e l'assioma di induzione.

2.2 Alcuni teoremi di PA

In PA è possibile dimostrare le consuete leggi aritmetiche, come la proprietà associativa per la somma o quella distributiva del prodotto rispetto la somma; ne vediamo alcune.

(1) $\vdash x = \mathbf{0} \vee \exists y$ tc $x = \boldsymbol{s}y$

Dimostrazione.
Data F la formula $(x = \mathbf{0} \vee \exists y \quad x = \mathbf{s}y)$ segue che:
$\forall x(x = 0 \to F)$ e $\forall x(x = \boldsymbol{s}y \to F)$ sono verità logiche
da cui:
$\vdash \forall x(x = 0 \to F)$ e $\vdash \forall y(\forall x(x = y \to F) \to \forall x(x = \boldsymbol{s}y \to F))$.
Allora per l'assioma di induzione: $\vdash x = \mathbf{0} \vee \exists y \quad x = \mathbf{s}y$ □

(2) $\vdash x + y = y + x$

Dimostrazione.
$\vdash \mathbf{0} + \mathbf{0} = \mathbf{0}$ per l'assioma di Peano n.(3)
$\vdash \mathbf{0}{+}x = x \to \mathbf{0} + \boldsymbol{s}x = \boldsymbol{s}(\mathbf{0}{+}x) = \boldsymbol{s}x$ per l'assioma di Peano n.(4) e per l'antecedente del condizionale.
Quindi per l'assioma di induzione:
$\vdash \mathbf{0}{+}x = x$.
Ora, dato che vale: $\vdash x = x{+}\mathbf{0}$ per l'assioma di Peano n.(3)
segue:
$\vdash \mathbf{0}{+}x = x{+}\mathbf{0}$
$\vdash y{+}\boldsymbol{s}\mathbf{0} = \boldsymbol{s}(y{+}\mathbf{0}) = \boldsymbol{s}y = \boldsymbol{s}y{+}\mathbf{0}$ per l'assioma di Peano n.(4) e (3)
$\vdash y +\boldsymbol{s}\, x = \boldsymbol{s}y + x \to y +\boldsymbol{ss}\, x = \boldsymbol{s}(y +\boldsymbol{s}\, x) = \boldsymbol{s}(\boldsymbol{s}y + x) = \boldsymbol{s}y +\boldsymbol{s}\, x$ per l'assioma di Peano n.(4) e per l'antecedente condizionale.
Allora, per l'assioma di induzione: $y +\boldsymbol{s}\, x = \boldsymbol{s}y + x$.
$\vdash x + y = y + x \to x +\boldsymbol{s}\, y = \boldsymbol{s}(x + y) = \boldsymbol{s}(y + x) = y +\boldsymbol{s}\, x = \boldsymbol{s}y + x$ per l'assioma di Peano n.(4), l'antecedente condizionale e per quanto detto nelo passaggio precedente.
Dunque, sempre per l'assioma di induzione otteniamo: $\vdash x + y = y + x$. □

(3) $\vdash x + (y + z) = (x + y) + z$

(4) $\vdash x \times (y + z) = (x \times y) + (x \times z)$

(5) $\vdash x \times (y \times z) = (x \times y) \times z$

(6) $\vdash x \times y = y \times x$

Illustriamo ora il Metodo di Gödel prima citato.

2.3 Metodo di Gödel

Nel 1931 Gödel, per dimostrare il teorema di incompletezza, sviluppò un metodo per esprimere alcuni enunciati metateorici con il medesimo linguaggio della teoria stessa. Procediamo illustrando tale metodo.
Fissiamo come teoria di riferimento l'aritmetica di Peano PA.
Poichè il sistema PA considerato astrattamente è, come detto all'inizio del capitolo, un sistema di oggetti, la descrizione di questo insieme di oggetti, delle operazioni che su di essi si possono compiere e delle proprietà a loro attribuite, è tutta operata entro la metateoria di PA.
Presentando in tal modo PA notiamo che non ha più alcuna importanza quali segni noi utilizziamo per formulare PA e pertanto possiamo ad esempio sostituire al posto dei segni elementari di PA delle cifre; in tal modo, tutte le asserzioni metateoriche riguardanti i segni di PA avranno il loro corrispettivo in asserti riferiti ai numeri ad essi associati e viceversa tutte le asserzioni metateoriche verranno tradotte in proposizioni aritmetiche.
Osserviamo che il nostro scopo è quello di costruire un metodo che permetta non solo di associare ad ogni proposizione un numero ma, ci consenta anche, di risalire in modo univoco dal numero alla proposizione.
Mediante il processo di *aritmetizzazione* di Gödel saremo in grado di stabilire questa relazione biunivoca tra proposizioni e numeri, poi, per ritenersi completa la rappresentazione della metateoria nella teoria, dovremo riuscire a formulare in funzioni aritmetiche tra numeri, le relazioni logiche presenti tra le proposizioni.
Per risolvere questo secondo passaggio dovremo far uso delle *relazioni ricorsive.*

2.3.1 L'aritmetizzazione

All'interno di una teoria formale, formule e dimostrazioni non sono altro che sequenze finite di simboli fondamentali, pertanto associando un numero ad ogni simbolo fondamentale possiamo avere un numero relativo ad ogni

formula e ad ogni dimostrazione.
A tutti i simboli della sintassi di PA attribuiamo un numero dispari da 3 a 33

$$g(\neg) = 3 \qquad g(\wedge) = 5 \qquad g(\vee) = 7 \qquad g(\rightarrow) = 9 \qquad g(\forall) = 11$$
$$g(\exists) = 13 \qquad g(=) = 15 \qquad g(() = 17 \qquad g()) = 19 \qquad g(\mathbf{0}) = 21$$
$$g(+) = 23 \qquad g(\times) = 25 \qquad g(\mathbf{s}) = 27 \qquad g(,) = 29 \qquad g(\perp) = 31$$
$$g(\vdash) = 33$$

e a tutte le sue variabili del linguaggio un numero, sempre dispari, da 35 in poi:

$$g(x_1) = 35 \qquad g(x_2) = 37 \qquad g(x_3) = 39 \ldots\ldots$$

Così facendo la k-esima variabile sarà in corrispondenza con il k-esimo numero primo successivo di 33.
Questi numeri sono detti *numeri di Gödel* o *gödeliani* dei simboli di Pa.
Consideriamo ora una formula di PA ad esempio:

$$x = sy$$

Traduciamo ogni simbolo di questa formula con un numero come indicato in precedenza; ovviamente così facendo non abbiamo ancora attribuito alla formula un unico numero. Per fare ciò Gödel stabilì come convenzione di fissare come unico numero associato ad una formula quello che si ottiene moltiplicando tanti primi in ordine di grandezza quanti sono i segni della formula ciascuno elevato al numero di Gödel del segno corrispondente.
Quindi se $t_1 t_2 \ldots t_r$ sono i segni presenti nella formula, definiamo il suo numero di Gödel come:

$$g(t_1 t_2 \ldots t_r) = 2^{g(t_1)} 3^{g(t_2)} \ldots p_{r-1}^{g(t_r)}$$

dove p_i è l'i-esimo primo e $p_0 = 2$.
E in modo analogo si calcola il gödeliano di una sequenza di formule quando si conosce il numero di Gödel di ciascuna formula.

Notiamo che essendo ogni numero naturale scomponibile in maniera unica nel prodotto di potenze di numeri primi allora tale tecnica è univocamente determinata una volta fissate le regole con cui essa avviene.
Ovviamente a questo punto vale anche il discorso contrario, ovvero dato un numero di Gödel n siamo in grado di risalire alla formula o sequenza di formule che esso traduce; basterà scomporre il numero in fattori primi, disporli in ordine crescente dalla potenza di 2 e vedere se gli esponenti delle potenze sono i gödeliani di segni di PA oppure no, nel primo caso il nostro numero n sarà il gödeliano di una formula mentre nel secondo sarà il coordinato di una sequenza di formule.
Ad esempio il numero 180 risulta:

$$180 = 2^3 \times 3^3 \times 5$$

che per quanto detto fin'ora è il numero gödeliano dell'espressione "$ss0$" ovvero del numero 2; ricordiamo che una cifra n nel metalinguaggio si traduce come l'n-esimo successore di 0.
Pertanto g è una funzione biunivoca dall'insieme dei simboli di PA, espressioni di PA e dalle sequenze di espressioni di PA, all'insieme dei numeri naturali; il codominio non coincide con l'insieme $\mathbb{N}$.
Concludiamo notando che l'assegnazione da noi fornita dei numeri di Gödel non è assolutamente univocamente determinata e stabiliamo che nel nostro lavoro utilizzeremo in PA gli apici angolati $\ulcorner S \urcorner$ per indicare il numero di Gödel di S invece che la notazione $g(S)$.

2.3.2 Osservazioni sulla ricorsività

Ora che ogni espressione di PA è associata ad un numero e che le proposizioni metaaritmetiche che hanno per oggetto queste espressioni di PA vengono tradotte in proposizioni riguardanti i loro numeri gödeliani abbiamo bisogno di capire quale relazione aritmetica corrisponde alle relazioni originarie tra segni di PA. Abbiamo bisogno di definire una classe di funzioni aritmetiche che, applicata a numeri, ci permetta di ottenere un altro numero in modo che, quando il suo argomento è costituito da gödeliani, anche il suo valore sia un gödeliano; precisamente sia il gödeliano dell'espressione ottenuta dalla combinazione di simboli ai cui gödeliani la funzione è stata applicata. Raggiunto questo obiettivo potremo far corrispondere a certe proprietà metateoriche di espressioni di PA le relative proprietà aritmetiche dei numeri gödeliani. Questo secondo passo si può raggiungere grazie alle funzioni ricorsive.

In questo lavoro noi non riproporremo la vasta teoria riguardante le funzioni ricorsive, definiremo le *funzioni fortemente rappresentabili* e mostreremo la connessione tra queste e le funzioni ricorsive mediante il *teorema di rappresentazione*. Tale teorema sarà la chiave per concludere la spiegazione del Metodo di Gödel.

Definizione 2.8. Una funzione f si dice *debolmente rappresentabile* in PA se:

- esiste una formula ben formata $\phi(y, x)$ con 2 variabili libere che esprime la relazione $y = f(x)$;
- per ogni coppia di numeri naturali n e m si ha che:
  - se $n = f(m)$ allora $\phi(S^n(0), S^m(0))$ è dimostrabile in T
  - se $n \neq f(m)$ allora $\neg\phi(S^n(0), S^m(0))$ è dimostrabile in T.

con $S^n(0)$ il termine $S(S(S(...S(S(0)))...)))$ in cui il simbolo S compare n volte.

Definizione 2.9. Una funzione f si dice *fortemente rappresentabile* in PA se valgono entrambi le seguenti condizioni:

- f è debolmente rappresentabile
- per ogni numero naturale m è dimostrabile in PA che:

$$\exists y(\phi(y, s^m(0)) \wedge \forall z(\phi(y, S^m(0)) \rightarrow (z = y)))$$

La seconda condizione assicura che, dato l'elemento m del dominio esiste un unico elemento y del codominio che è in relazione con m.

Teorema 2.3.1. ***teorema di rappresentazione***
Ogni funzione ricorsiva è fortemente rappresentabile in PA.

Concludendo, le funzioni ricorsive per la proprietà appena enuncita dal teorema sono proprio le funzioni che ci permettono di tradurre espressioni riguardanti numeri in espressioni di PA.

2.4 "Teor" e le sue proprietà

Ora che abbiamo introdotto PA, quale sistema in grado di formalizzare l'aritmetica, abbiamo visto un complesso metodo per far corrispondere un numero ad ogni espressione di PA e abbiamo, grazie all'aritmetica ricorsiva, riprodotto le considerazioni metateoriche fatte sull'espressioni di PA in relazioni aritmetiche ricorsive sui loro gödeliani possiamo concludere che la metateoria di PA che ci occorre viene formalizzata entro il sistema stesso PA.
Diamo un semplice esempio di come avviene la traduzione da asserto metateorico relativo ad espressioni di PA e alle loro relazioni logiche, ad asserto relativo a numeri e alle loro relazioni numeriche.
Sia dato: $\neg(x = y) \vee (sx = sy)$. Chiamiamo la prima espressione 'parte iniziale' dell'assioma.
Traduciamo tale assioma assegnando i numeri gödeliani alle due espressioni:

$\neg(x = y) = 2^3 \times 3^{17} \times 5^{35} \times 7^{15} \times 11^{37} \times 13^{19} = l$
$\neg(x = y) \vee (sx = sy) = 2^3 \times 3^{17} \times 5^{35} \times 7^{15} \times 11^{37} \times 13^{19} \times 17^7 \times 19^{27} \times 23^{35} \times 29^{15} \times 31^{27} \times 37^{37} \times 41^{19} = k$

Notiamo immediatamente che "k è divisibile per l" e questa è proprio una relazione logica di PA che viene rappresentata in una relazione aritmetica tra i loro gödeliani k e l. Inoltre, il predicato è ricorsivo e pure la sua funzione rappresentativa lo è. Ciò significa che la proprietà di "essere divisibile per" si può esprimere con il formalismo di PA.

Definizione 2.10. Date k ed l due variabili si dice che k *è divisibile* per l se:

$$k/l = \exists_{z=0}^{k} z(k = l \times z)$$

Ricordiamo che, nella sintassi di PA, avevamo definito *dimostrazione* una sequenza ordinata di assiomi o di formule ottenute dalle precedenti grazie a MP,SU e GEN. Vogliamo ora tradurre l'asserto metateorico "essere dimostrazione di" in asserto aritmetico come nell'esempio precedente, ovvero vogliamo definire un predicato aritmetico $D(x, y)$ verificato solo quando la sequenza di formule con gödeliano x è una dimostrazione della fomula di gödeliano y.

Definizione 2.11. Definiamo x *dimostrazione di* y mediante la formula:

$$D(x, y) \qquad \text{sse} \qquad Dv(x) \wedge [l(x)]Glx = y$$

In altre parole, x è dimostrazione di y se x è una *derivazione* e se il termine della sequenza numerica coordinata ad x che occupa il posto di indice $l(x)$, cioè l'ultimo numero della sequenza, è il numero gödeliano y.
Notiamo che tutti i predicati usati nella definizione sono ricorsivi primitivi e pertanto per proprietà della congiunzione risulta tale anche $D(x, y)$. Inoltre essendo D fortemente rappresentabile, se è vero che $D(x, y)$ allora deve esistere una formula nel linguaggio di PA che traduca D; chiamiamo Dim tale fomula di PA contenente due variabili libere.
Ora che abbiamo definito la relazione D e la sua traduzione Dim in PA possiamo affermare che se tra due numeri gödeliani sussiste Dim allora la sequenza di formule associate al primo è una dimostrazione della formula associata

al secondo, ovvero, siamo in grado di rappresentare dentro l'aritmetica la proprietà di essere "dimostrabile" in PA.

Definizione 2.12. Data x una variabile diciamo che è *dimostrabile* in PA attraverso la seguente formula:

$$Teor(x) \qquad \text{sse} \qquad \exists y(Dim(y,x))$$

Sia ora S una proposizione di PA e sia $Teor(\ulcorner S \urcorner)$ il risultato ottenuto sostituendo $\ulcorner S \urcorner$ al posto della variabile x in $Teor(x)$. Allora, presa T un'altra proposizione di PA valgono le seguenti proprietà:

1. se $\vdash S$, allora $\vdash Teor(\ulcorner S \urcorner)$
2. $\vdash Teor(\ulcorner (S \to T) \urcorner) \to (Teor(\ulcorner S \urcorner) \to Teor(\ulcorner T \urcorner))$
3. $\vdash Teor(\ulcorner S \urcorner) \to Teor(\ulcorner Teor(\ulcorner S \urcorner) \urcorner)$
4. $Teor(\ulcorner S \urcorner)$ è una Σ-proposizione
5. se S è una Σ-proposzione, allora $\vdash S \to Teor(\ulcorner S \urcorner)$

Capitolo 3

Il "Box" come "Teor"

In questo capitolo confronteremo il sistema GL con la teoria PA e giungeremo a stabilire un importante risultato di corrispondenza. Stabilendo un'opportuna traduzione dal lingiaggio di GL a quello di PA dimostreremo che ogni formula di GL risulta teorema di GL se e solo se la sua corrispondente traduzione in PA è teorema di PA; questo è il *Teorema di Solovay.* Prima di procedere con la dimostrazione di tale teorema mostreremo qualche risultato interessante, tra cui il *Teorema di Löb.*

Definizione 3.1. Un' *interpretazione* è una funzione ρ che assegna ad ogni variabile proposizionale una proposizione del linguaggio dell'Aritmetica di Peano.

Definizione 3.2. Una *traduzione* A^* di una proposizione modale A sotto una realizzazione ρ è definita induttivamente nel seguente modo:

1. $\perp^* = \perp$
2. $p^* = \rho(p)$ con p variabile proposizionale
3. $(A \to B)^* = (A^* \to B^*)$
4. $\Box(A^*) = Teor[A^*]$ con $Teor[A^*] = Teor(\ulcorner A^* \urcorner)$

Le prime tre condizioni garantiscono che la combinazione vero-funzionale di proposizioni è la combinazione vero-funzionale della traduzione sotto $*$ di quelle proposizioni. La condizione 4 assicura che se la traduzione di A è S, allora la traduzione di $\Box A$ è $Teor(\ulcorner S \urcorner)$, ovvero una proposizione dimostrabile nell'Aritmetica di Peano se S è dimostrabile in PA.

Ora vogliamo stabilire quali principi della Logica Modale si mantengono validi quando il simbolo $\Box$, fino ad ora letto come "è necessario che", viene interpretato come "è dimostrabile in PA che".

3.1 Teorema di Löb

Il *Teorema di Löb* afferma che se PA dimostra che la derivabilità di una proposizione S implica S, allora PA dimostra S stessa. Tale risultato che può sembrare scontato non è affatto banale e per la sua dimostrazione dovremo ricorrere al *lemma di diagonalizzazione*.
Questo lemma sostiene a sua volta che per ogni proprietà esprimibile in PA attraverso una formula con un'unica variabile libera, è sempre possibile trovare una proposizione che afferma di godere di quella proprietà.
Vediamoli ora entrambi nello specifico.

Lemma 3.1.1. ***Lemma di diagonalizzazione***
Sia $P(y)$ una formula del linguaggio di PA in cui non compaiono variabili libere diverse da y.
Allora esiste una proposizione S di PA tale che:

$$PA \vdash S \leftrightarrow P(\ulcorner S \urcorner)$$

Dimostrazione.
Definiamo $sost(n, m)$ la funzione che vale sse n è il gödeliano di una formula con una variabile libera $A(x)$ e $m = \ulcorner A(\ulcorner A(x) \urcorner) \urcorner$ e definiamo $prova(n, m)$ la funzione che vale sse n è il gödeliano di una dimostrazione di una formula che ha gödeliano m.

Allora sappiamo che:

OSS.1 esiste un formula da PA con due variabili libere, $\Delta(x, y)$ tale che per ogni $n, m \in \mathbb{N}$:
se vale $sost(n, m)$ allora $PA \vdash \Delta(\ulcorner n \urcorner, \ulcorner m \urcorner)$
se non vale $sost(n, m)$ allora $PA \vdash \neg\Delta(\ulcorner n \urcorner, \ulcorner m \urcorner)$

OSS. $PA \vdash \Delta(\ulcorner A(x) \urcorner, y) \leftrightarrow y = \ulcorner A(\ulcorner A(x) \urcorner) \urcorner$
per ogni fbf $A(x)$ con una sola variabile libera.

Per approfondimenti si veda "Mendelson, Introduzione alla logica matematica".

Ora, sia data $P(y)$. Poniamo:

$$C(x) := \forall y(\Delta(x, y) \to P(y)) \qquad \text{e} \qquad S := C(\ulcorner C(x) \urcorner)$$

Allora:
$PA \vdash S \leftrightarrow C(\ulcorner C(x) \urcorner)$ per definizione di S
$PA \vdash S \leftrightarrow \forall y(\Delta(\ulcorner C(x) \urcorner, y) \to P(y))$ per sostituzione di x con $\ulcorner C(x) \urcorner$ nella definizione di $C(x)$.
$PA \vdash \Delta(\ulcorner C(x) \urcorner, y) \leftrightarrow y = \ulcorner C(\ulcorner C(x) \urcorner) \urcorner$ per **OSS.2**
$PA \vdash S \leftrightarrow \forall y(y = (\ulcorner C(\ulcorner C(x) \urcorner) \urcorner) \to P(y))$
$PA \vdash S \leftrightarrow P(\ulcorner C(\ulcorner C(x) \urcorner) \urcorner)$ per logica dell'identità
$PA \vdash S \leftrightarrow P(\ulcorner S \urcorner)$ per definizione di S □

Teorema 3.1.2. ***Teorema di Löb***
Se $PA \vdash Teor(\ulcorner S \urcorner) \to S$
allora $PA \vdash S$

Dimostrazione.
Definiamo $Q(x) =_{def} (Teor(x) \to S)$.
L'ipotesi del nostro teorema diventa pertanto: $PA \vdash Q(x)$.

Per il lemma (3.1.1) esiste una proposizione I di PA tale che:

$$PA \vdash I \leftrightarrow Q(\ulcorner I \urcorner).$$

cioè:$PA \vdash I \leftrightarrow (Teor(\ulcorner I \urcorner) \rightarrow S)$.
Quindi:

1 $PA \vdash I \leftrightarrow (Teor(\ulcorner I \urcorner) \rightarrow S)$ per lemma (3.1.1)

2 $PA \vdash I \rightarrow (Teor(\ulcorner I \urcorner) \rightarrow S)$ da **1**.

3 $PA \vdash Teor(\ulcorner (I \rightarrow (Teor(\ulcorner I \urcorner) \rightarrow S)) \urcorner)$ per proprietà 1 di Teor.

4 $PA \vdash Teor(\ulcorner (I \rightarrow (Teor(\ulcorner I \urcorner) \rightarrow S)) \urcorner) \rightarrow (Teor(\ulcorner I \urcorner) \rightarrow Teor(\ulcorner (Teor(\ulcorner I \urcorner) \rightarrow S) \urcorner)$ per proprietà 2 di Teor.

5 $PA \vdash Teor(\ulcorner I \urcorner) \rightarrow Teor(\ulcorner (Teor(\ulcorner I \urcorner) \rightarrow S) \urcorner)$ per MP da **3** e **4**.

6 $PA \vdash Teor(\ulcorner (Teor(\ulcorner I \urcorner) \rightarrow S) \urcorner) \rightarrow (Teor(\ulcorner Teor(\ulcorner I \urcorner) \urcorner) \rightarrow Teor(\ulcorner S \urcorner)$ istanza della proprietà 2 di Teor

7 $PA \vdash Teor(\ulcorner I \urcorner) \rightarrow (Teor(\ulcorner Teor(\ulcorner I \urcorner) \urcorner) \rightarrow Teor(\ulcorner S \urcorner))$ per transitività.

8 $PA \vdash Teor(\ulcorner I \urcorner) \rightarrow Teor(\ulcorner Teor(\ulcorner I \urcorner) \urcorner)$ istanza della proprietà 3 di Teor.

9 $PA \vdash Teor(\ulcorner I \urcorner) \rightarrow Teor(\ulcorner S \urcorner)$ per transitività.

10 $PA \vdash Teor(\ulcorner S \urcorner) \rightarrow S$ per ipotesi

11 $PA \vdash Teor(\ulcorner I \urcorner) \rightarrow S$ per transitività.

12 $PA \vdash I$ per **1** e **11**.

13 $PA \vdash Teor(\ulcorner I \urcorner)$ per proprietà 1 di Teor.

14 $PA \vdash S$ per **11** e **13**.

$\square$

Dal Teorema di Löb si ottiene immediatamente il seguente teorema.

Teorema 3.1.3. ***Secondo teorema di incompletezza di PA***
Se PA è consistente
allora $PA \nvdash \neg Teor(\ulcorner \perp \urcorner)$

Dimostrazione.
Procediamo per contrapposizione.
Supponiamo: $PA \vdash \neg Teor(\ulcorner \perp \urcorner)$
segue che:
$PA \vdash Teor(\ulcorner \perp \urcorner) \rightarrow \perp$
$PA \vdash \perp$ per teorema (3.1.2)
pertanto PA è inconsistente; assurdo per HP. □

3.2 Teorema di Solovay

Il *Teorema di Solovay* afferma che i teoremi di GL sono le proposizioni della logica modale dimostrabili nell'Aritmetica di Peano una volta 'trasformate' attraverso tutte le possibili traduzioni *. Tale teorema riguarda quindi il concetto di dimostrabilità all'interno di un sistema formale e la tecnica usata da Solovay nella dimostrazione è diventata un fondamentale metodo di studio per la dimostrabilità e le relative nozioni; la dimostrazione utilizza la semantica di Kripke.

Teorema 3.2.1. ***Teorema di validità di GL su PA***
Se $GL \vdash A$
allora per ogni traduzione *, $PA \vdash A^*$.

Teorema 3.2.2. ***Teorema di Solovay***
Se per ogni traduzione *, $PA \vdash A^*$
allora $GL \vdash A$.

Nella dimostrazione daremo prima una sorta di quadro generale del procedimento per poi porre la nostra attenzione sui punti lasciati sospesi.

Dimostrazione.
<u>1.traccia della dimostrazione</u>

La dimostrazione procede per contrapposizione:

$$GL \nvdash A \qquad \text{allora} \qquad PA \nvdash A^*.$$

Supponiamo quindi: $GL \nvdash A$.
Significa che dato un modello $\mathcal{M} =< \mathcal{W}, \mathcal{R}, \mathcal{I} >$ finito, transitivo, inversamente ben fondato:

$$\exists w \in \mathcal{W} \quad \text{tc} \quad \mathcal{M} \not\models_w A$$

Costruiamo una realizzazione * tale che: $PA \nvdash A^*$.
Ci sarà d'aiuto identificare i "mondi possibili" con l'insieme $\mathbb{N}$ dei numeri naturali, e così, poichè per costruzione $\mathcal{W}$ è finito, possiamo scrivere:

$$\mathcal{W} = \{1, 2, \ldots, n\}$$

Poniamo $w = 1$, da cui segue $\mathcal{M} \not\models_1 A$, e definiamo $\mathcal{R}$ tale che:

$$1\mathcal{R}i \quad \text{sse} \quad 1 < i \leq n$$

Definiremo delle proposizioni $S_0, S_1, \ldots, S_n$ in PA per le quali, presa p^* per ogni variabile proposizionale p la disgiunzione di tutte le proposizioni S_i con $i \in \mathcal{I}(p)$, varrà il seguente lemma:

Lemma 3.2.3. *Per tutti gli i tali che $1 \leq i \leq n$, e per tutte le sottoformule B di una formula data A vale che:*

- *se $\mathcal{M} \models_i B$ allora $PA \vdash S_i \rightarrow B^*$*
- *se $\mathcal{M} \not\models_i B$ allora $PA \vdash S_i \rightarrow \neg B^*$*

Ora, essendo A una sottoformula di se stessa e $1 \in \mathcal{W} : \mathcal{M} \not\models_1 A$, applicando il lemma (3.2.3) otterremo:

1 $PA \vdash S_1 \rightarrow \neg A^*$.

2 $PA \vdash A^* \rightarrow \neg S_1$ per contrapposizione.

3 $PA \vdash Teor(\ulcorner(A^* \rightarrow \neg S_1)\urcorner)$ per proprietà 1 di Teor.

4 $PA \vdash Teor(\ulcorner A^* \urcorner) \rightarrow Teor(\ulcorner \neg S_1 \urcorner)$ per proprietà 2 di Teor.

5 $PA \vdash \neg Teor(\ulcorner \neg S_1 \urcorner) \rightarrow \neg Teor(\ulcorner \neg A^* \urcorner)$ per contrapposizione.

Mostreremo che: $PA \vdash S_0 \rightarrow \neg Teor(\ulcorner \neg S_1 \urcorner)$ (proprietà che per comodità indichiamo con $\triangle$) e che S_0 è vera.
Da ciò seguirà:

6 $PA \vdash S_0 \rightarrow \neg Teor(\ulcorner A^* \urcorner)$ per transitività.

Ora, poichè:

$$S_0 \rightarrow \neg Teor(\ulcorner A^* \urcorner) \quad \text{è vera} \quad \text{e} \quad S_0 \quad \text{è vera}$$

otterremo che: $\neg Teor(\ulcorner A^* \urcorner)$ è vera, ovvero:

$$PA \nvdash A^*$$

cioè la tesi del teorema.
Procederemo quindi costruendo le proposizioni $S_0, S_1, \ldots, S_n$, illustrando le loro proprietà, tra cui ($\triangle$), e termineremo con la dimostrazione del lemma sopracitato da cui come abbiamo visto segue immediatamente la tesi di Solovay.

2.Costruzione delle proposizioni di Solovay

Consideriamo un'estensione del modello $\mathcal{M}$:

$$\mathcal{M}' =< \mathcal{W}', \mathcal{R}', \mathcal{I}' >$$

con:

- $\mathcal{W}' = \mathcal{W} \cup 0 = \{0, 1, \ldots, n\}$

- $\mathcal{R}' = \mathcal{R} \cup \{< 0, i >: 1 \leq i \leq n\}$, quindi come $\mathcal{R}$ sarà transitiva e inversamente ben fondata.
- $\mathcal{I}'$ tale che $0 \in \mathcal{I}'(p)$ sse $1 \in \mathcal{I}(p)$ e $i \in \mathcal{I}'(p)$ sse $i \in \mathcal{I}(p)$.

Così il nostro nuovo modello contiene il mondo 0 relato a tutti gli altri mondi dell'universo tramite $\mathcal{R}'$, e 0 si comporta con le variabili proposizionali come 1.

Per ogni j la proposizione S_j sarà tale da affermare che il limite di una certa funzione h è j.

Tale funzione h, che andremo a definire, avrà le seguenti caratteristiche:

- h è una funzione di dominio $\mathbb{N}$ e codominio $\mathcal{W}'$.
- $h(0) = 0$
- $h(m{+}1) = \begin{cases} h(m) & \text{se} \quad \forall k(h(m)\mathcal{R}'k \to m \neq \text{ gödeliano della dimostrazione di} \neg S_k) \\ j & \text{se} \quad h(m)\mathcal{R}'j \wedge m = \text{ gödeliano della dimostrazione di} \neg S_j \end{cases}$

Le proposizioni $\neg S_k$ e $\neg S_j$ affermano rispettivamente che il limite di h non è k e j.

Quindi la funzione h che costruiremo non è altro che una funzione a gradini che parte da 0 e assume costante il valore 0 fino a che non esiste, nel proprio dominio, un naturale $m + 1$ molto molto grande il cui antecedente m risulta essere il gödeliano della dimostrazione di $\neg S_j$, con $0\mathcal{R}'j$. In tal caso la funzione h a partire dal punto $m + 1$ assume il valore j. Ancora, h manterrà il valore j fino a che non incontrerà un naturale $k+1$ tale che k sia il gödeliano della dimostrazione di $\neg S_l$ e in tal caso a partire da $k + 1$, la funzione h assumerà valore l, per un l tale che $j\mathcal{R}'l$, e così via.

Definizione 3.3. Diciamo che j è *limite* di h se:

$$\exists m(h(m) = j \wedge \forall m'(m' > m \to h(m') = j))$$

Vedremo che:

- il limite di h esiste.

Siamo ora finiti in una sorta di circolo; la nostra funzione h è definita nei termini della dimostrazione di $\neg S_j$, ma S_j afferma che il limite di h è un numero stabilito j. L'uscita da questa situazione ce la fornirà il *lemma di diagonalizzazione*.
Notiamo che nella dimostrazione del suo teorema Solovay decide di considerare una tale funzione h proprio per ottenere, mediante diagonalizzazione, una formula che parli di se stessa (come effettivamente risulterà h).

Vogliamo ora dare una definizione formale di h. h può essere rappresentata da un insieme di coppie, il suo grafo, e quindi da una fbf $H(a,b)$.
Se $H(a,b)$ è la formula di PA definita dalla relazione binaria:

$$\{< a, b >: h(a) = b\}$$

allora potremmo definire, e lo faremo, la proposizione S_j come la formula:

$$\exists c \forall a (a \geq c \rightarrow \exists b (b = \mathbf{j} \wedge H(a,b)))$$

[Così S_j affermerebbe proprio che il limite di h è j]
Cerchiamo quindi di giungere a questa definizione formale di S_j.

Partiamo con qualche considerazioni su $h(a) = b$.
Informalmente, tale formula, è vera se e solo se esiste una sequenza finita $h(0), h(1), \ldots, h(a)$ di lunghezza $a + 1$ tale che:

- $h(0) = 0$

- $h(a) = b$

- $\forall m, m < a$:

$$h(m+1) = \begin{cases} h(m) & \text{se} \quad \forall k(h(m)\mathcal{R}'k \rightarrow m \neq \text{gödeliano della dimostrazione di} \neg S_k) \\ j & \text{se} \quad h(m)\mathcal{R}'j \wedge m = \text{gödeliano della dimostrazione di} \neg S_j \end{cases}$$

Formalizziamo questa descrizione euristica di h definendo propriamente $H(a, b)$. Ricordiamo che una volta fatto questo l'espressione di PA:

$$\exists c \forall a(a \geq c \rightarrow \exists b(b = \mathbf{j} \wedge H(a, b)))$$

sarà anche corretta formalmente oltre ad avere il significato da noi desiderato, e quindi potremo identificarla con S_j.

A questo punto passiamo alla definizione di $H(a, b)$.

- Sia $F_m = F(a, b)$ una formula con numero di Gödel m la quale definisce una funzione f.

- Sia $nonlim(x_1, x_2)$ un Σ-termine il cui valore per ogni (m, j) è il gödeliano della formula:

  $$\neg\exists c \forall a(a \geq c \rightarrow \exists b(b = \mathbf{j} \wedge F_m)).$$

  Quindi se una formula F_m con numero di Gödel m definisce una funzione, allora $nonlim(\mathbf{m}, \mathbf{j})$ indica il gödeliano della negazione della proposizione che afferma che j è il limite della funzione definita da F_m.

- Sia $B(y, a, b)$ la formula:

$$\exists s(FinSeq(s) \wedge lh(s) = a+\mathbf{1} \wedge s_0 = \mathbf{0} \wedge s_a = b \wedge \forall x < a$$

$$\bigwedge_{0 \leq i \leq n} [s_x = \mathbf{i} \rightarrow \left\{ \bigwedge_{i\mathcal{R}'j} [Dim(x, nolim(y, \mathbf{j})) \rightarrow s_{x+\mathbf{1}} = \mathbf{j}] \right.$$

$$\wedge [\left\{ \bigwedge_{i\mathcal{R}'j} \neg Dim(x, nonlim(y, \mathbf{j})) \right\} \rightarrow s_{x+\mathbf{1}} = s_x]])$$

Cioè se y è il gödeliano della formula F che definisce una funzione f, allora $B(y,a,b)$ afferma che esiste una sequenza finita di lunghezza $a+1$ il cui primo elemento è 0, l'ultimo è b, e tale che per ogni valore $x < a$, se $s_x = i$, allora $s_{x+1} = j$ con $i\mathcal{R}'j$ e con x numero di Gödel della dimostrazione della negazione della proposizione:

$$\neg\exists c\forall a(a \geq c \rightarrow \exists b(b = \mathbf{j} \wedge F))$$

nel senso che j non è il limite di y e in caso contrario allora l'$x+1$-esimo elemento della successione rimane i.

- Per il *lemma di diagonalizzazione*, poichè $B(y,a,b)$ possiede una sola variabile libera y, esiste una formula $H(a,b)$ tale che:

$$PA \vdash H(a,b) \leftrightarrow B(\ulcorner H(a,b) \urcorner, a, b)$$

- Sia m il numero di Gödel di $H(a,b)$. Così, per la definizione sopra riportata sarà: $H(a,b) = F_m$ e $f = h$.

- Per ogni j, $0 \leq j \leq n$, poniamo ora S_j la proposizione:

$$\exists c\forall a(a \geq c \rightarrow \exists b(b = \mathbf{j} \wedge H(a,b)))$$

che afferma che il limite di h è j.

Ci siamo messi, essendo $y = m$, nella condizione in cui la sequenza s di cui parlavamo nella definizione di $B(y,a,b)$ esiste sempre e con tutte le proprietà che volevamo; di conseguenza abbiamo definito rigorosamente $H(a,b)$e una proposizione che afferma che j è proprio il limite della funzione h definita da $H(a,b)$.

Pertanto:
Grazie alla definizione di $F(a,b), nonlim(m,j), B(y,a,b)$ siamo riusciti a dare la definizione di $H(a,b)$ in termini aritmetici e così l'enunciato:

$$\exists c\forall a(a \geq c \rightarrow \exists b(b = j \wedge H(a,b)))$$

è un enunciato di PA che afferma che il limite di h è proprio j.
Abbiamo concluso ponendo:

$$S_j =_{def} \exists c \forall a(a \geq c \to \exists b(b = j \wedge H(a, b)))$$

Costruite le proposizioni di Solovay dimostriamo alcune loro proprietà; per verificarle risulteranno fondamentali tutte quelle condizioni che abbiamo imposto alla h.
Terminata la presentazione delle proprietà dimostreremo il lemma enunciato all'inizio della traccia; da questo seguirà:

$$PA \vdash S_0 \to \neg Teor(\ulcorner S_1 \urcorner)$$

lasciata in sospeso all'inizio (vedi traccia dimostrazione) e quindi potremo terminare la dimostrazione del teorema.

3.Proprietà delle S_j

Ora sappiamo che: $PA \vdash nonlim(\ulcorner H(a, b) \urcorner, \mathbf{j})$.
Ma:

$$\begin{aligned} nonlim(\ulcorner H(a,b) \urcorner, \mathbf{j}) &= nonlim(\mathbf{m}, \mathbf{j}) \\ &= \ulcorner \neg \exists c \forall a(a \geq c \to \exists b(b = \mathbf{j} \wedge H(a, b)) \urcorner) \\ &= \ulcorner \neg S_j \urcorner \end{aligned}$$

A questo punto, ricordando la definizione di $B(y, a, b)$ e di $H(a, b)$ otteniamo:

(1)

$$PA \vdash H(a,b) \leftrightarrow \exists h(Finseq(h) \wedge lh(h) = a{+}\mathbf{1} \wedge h(0) = \mathbf{0} \wedge h(a) = b$$

$$\wedge \forall m < a \bigwedge_{0 \leq i \leq n} [h(m) = \mathbf{i} \to \left\{ \bigwedge_{i\mathcal{R}'j} [Dim(m, \ulcorner \neg S_j \urcorner) \to h(m+1) = \mathbf{j}] \right.$$

$$\wedge [\{\wedge_{i\mathcal{R}'j} \neg Dim(m, \ulcorner \neg S_j \urcorner)\} \to h(m+1) = h(m)]])$$

Da questa proprietà si può notare che la formula $H(a, b)$ definisce una funzione h che soddisfa tutte le caratteristiche che volevamo attribuirle e quindi siamo in grado di mostrare come PA provi diversi fatti riguardo le proposizioni S_j costruite a partire da $H(a, b)$.

Vedremo ora che:

- h ha un unico limite minore o ugule a n (punti successivi (2),(3), (4))
- se $i\mathcal{R}'j$ in PA si dimostra: $S_i \rightarrow$ "S_j è consistente" (punto (5))
- se $i \geq 1$ in PA si dimostra: $S_i \rightarrow$ "S_i è confutabile" (punto (6))
- se $i \geq 1$ in PA si dimostra: $S_i \rightarrow$ "il limite di h è un qualche j, $i\mathcal{R}'j$" (punto (7))

Dato che $PA \vdash \exists! bH(a, b)$, come possiamo facilmente vedere per induzione su a, abbiamo che:

(2) $PA \vdash \neg(S_i \wedge S_j) \qquad \text{se} \quad 0 \leq i < j \leq n$

Ricordiamo che $< \mathcal{W}', \mathcal{R}' >$ è una frame finita, transitiva, inversamente ben fondata per ipotesi. Ora mostriamo per induzione sull'inversione di $\mathcal{R}'$ che:

(3) $PA \vdash H(a, \mathbf{i}) \rightarrow (S_i \vee \bigvee_{i\mathcal{R}'j} S_j)$

Dimostrazione.
Procediamo per induzione a ritroso.
Possiamo assumere che per ogni j, $i\mathcal{R}'j$:
$PA \vdash H(a, \mathbf{j}) \rightarrow (S_j \vee \bigvee_{j\mathcal{R}'k} S_k)$
$PA \vdash H(a, \mathbf{i}) \rightarrow \forall c(c \geq a \rightarrow [H(c, \mathbf{i}) \vee \bigvee_{i\mathcal{R}'j} H(c, \mathbf{j})])$ per (**1**)
che, unita all'ipotesi induttiva:
$PA \vdash H(a, \mathbf{i}) \rightarrow \forall c(c \geq a \rightarrow [H(c, \mathbf{i}) \vee \bigvee_{i\mathcal{R}'j}(S_j \vee \bigvee_{j\mathcal{R}'k} S_k)])$

quindi:
$PA \vdash H(a, \mathbf{i}) \to (\forall c(c \geq a \to H(c, \mathbf{i})) \vee \bigvee_{i\mathcal{R}'j}(S_j \vee \bigvee_{j\mathcal{R}'k} S_k))$
cioè:
$PA \vdash H(a, \mathbf{i}) \to (S_i \vee \bigvee_{i\mathcal{R}'j}(S_i \vee \bigvee_{j\mathcal{R}'k} S_k))$.
Quindi, per la transitività $\mathcal{R}'$, vale (**3**). $\square$

Segue da (**3**) che:
$PA \vdash H(a, \mathbf{0}) \to (S_0 \vee S_1 \vee \cdots \vee S_n)$
e dato che $PA \vdash H(0, 0)$, ovvero $h(0) = 0$, otteniamo:

(4) $PA \vdash (S_0 \vee S_1 \vee \cdots \vee S_n)$

Ora ricordiamo che:

- Abbiamo definito $h : \mathbb{N} \to \mathcal{W}'$ come una sequenza di lunghezza $a + 1$ tale che:
  - $h(0) = 0$
  - $h(a) = b$
  - $\forall m, m < a$:
  $$h(m{+}1) = \begin{cases} h(m) & \text{se} \quad \forall k(h(m)\mathcal{R}'k \to m \neq \text{gödeliano della dimostrazione di} \neg S_k) \\ j & \text{se} \quad h(m)\mathcal{R}'j \wedge m = \text{gödeliano della dimostrazione di} \neg S_j \end{cases}$$
- per ogni proposizione S:
  $$PA \vdash Teor(\ulcorner S \urcorner) \leftrightarrow \exists y(Dim(y, \ulcorner S \urcorner))$$
  cioè S è un teorema di PA se e solo se esiste un y che risulta essere il gödeliano di una sequenza di formule che risulta essere a sua volta la dimostrazione della formula con gödeliano $\ulcorner S \urcorner$.

Adesso consideriamo $i\mathcal{R}'j$.
Supponiamo il limite di h sia i.
Allora per definizione di limite:

$$\exists m \in \mathbb{N} \quad \text{tc} \quad \forall r \geq m, h(r) = h(m) = i$$

Supponiamo $\neg S_j$ sia teorema di PA.
Allora per definizione di teorema di PA:

$$\exists k > m \quad \text{tc} \quad Dim(k, \ulcorner \neg S_j \urcorner)$$

da cui per definizione di h: $h(k+1) = j \neq i$ il che è una contraddizione.
Quindi dobbiamo supporre $\neg S_j$ non sia teorema di PA.
Formalizzando questa ipotesi avremo:

(5) se $i\mathcal{R}'j$, allora $PA \vdash S_i \rightarrow \neg Teor(\ulcorner \neg S_j \urcorner)$

(6) se $i \geq 1$, allora $PA \vdash S_i \rightarrow Teor(\ulcorner \neg S_i \urcorner)$

Dimostrazione.
Supponiamo $i \geq 1$.
Da (**1**) segue che:
$PA \vdash H(a, \mathbf{i}) \rightarrow \exists x(Dim(x, \ulcorner \neg S_i \urcorner))$.
Ricordiamo:
$PA \vdash \exists x(Dim(x, \ulcorner \neg S_i \urcorner)) \rightarrow Teor(\ulcorner \neg S_i \urcorner)$ per definizione di Teor.
$PA \vdash S_i \rightarrow \exists a H(a, \mathbf{i})$
quindi:
$PA \vdash S_i \rightarrow Teor(\ulcorner \neg S_i \urcorner)$ per transitività. □

(7) se $i \geq 1$, allora $PA \vdash S_i \rightarrow Teor(\ulcorner \bigvee_{i\mathcal{R}'j} S_j \urcorner)$

Dimostrazione.
Da (**3**): $PA \vdash \exists a H(a, \mathbf{i}) \rightarrow (S_i \vee \bigvee_{i\mathcal{R}'j} S_j)$
Quindi:
$PA \vdash Teor(\ulcorner \exists a H(a, \mathbf{i}) \urcorner) \rightarrow Teor(\ulcorner S_i \vee \bigvee_{i\mathcal{R}'j} S_j \urcorner)$ per proprietà 2 di teor.

Ricordiamo:
$PA \vdash S_i \to \exists a H(a,i)$ per definizione di S_i
$PA \vdash \exists a H(a,i) \to Teor(\ulcorner \exists a H(a,i) \urcorner)$ per proprietà 1 di Teor.
Quindi:
$PA \vdash S_i \to Teor(\ulcorner \exists a H(a,i) \urcorner)$ per transitività.
$PA \vdash S_i \to Teor(\ulcorner S_i \vee \bigvee_{i\mathcal{R}'j} S_j \urcorner)$ per transitività.
Ora da (6) essendo $\mathbf{i} \geq 1$:
$PA \vdash S_i \to Teor(\ulcorner \neg S_i \urcorner)$.
Ma: $PA \vdash Teor(\ulcorner \neg S_i \urcorner) \wedge Teor(\ulcorner S_i \vee \bigvee_{i\mathcal{R}'j} S_j \urcorner) \to Teor(\ulcorner \bigvee_{i\mathcal{R}'j} S_j \urcorner)$
Quindi: $PA \vdash S_i \to Teor(\ulcorner \bigvee_{i\mathcal{R}'j} S_j \urcorner)$ □

<u>4.Lemma</u>
Abbiamo ora tutti gli strumenti necessari per dimostrare il lemma già enunciato a inizio paragrafo.
Per ogni lettera proposizionale poniamo:

$$p^* = \bigvee_{i \in \mathcal{I}'(p)} S_i$$

e definiamo così la relazione che ad ogni variabile p di GL associa una proposizione p^* in PA.

Lemma 3.2.4. *Per tutti gli i tali che $1 \leq i \leq n$, e per tutte le sottoformule B della formula A vale che:*

- *se $\mathcal{M} \models_i B$ allora $PA \vdash S_i \to B^*$*
- *se $\mathcal{M} \not\models_i B$ allora $PA \vdash S_i \to \neg B^*$*

Dimostrazione.
Procediamo sulla complessità di B.
Supponiamo $B = p$ variabile proposizionale, allora $B^* = \bigvee_{i:i \in \mathcal{I}'(p)} S_i$.
Se $\mathcal{M} \models_i p$ allora $i \in \mathcal{I}(p)$, da cui $i \in \mathcal{I}'(p)$
Per la definizione di * sarà: $PA \vdash S_i \to p^*$.
Da cui: $PA \vdash S_i \to B^*$.

Se $\mathcal{M} \not\models_i p$ allora $i \notin \mathcal{I}(p)$, per cui, dato che $i \neq 0$, $i \notin \mathcal{I}'(p)$. Quindi per ogni disgiunzione S_j di p^*, S_i è diversa da S_j, e da (**2**): $PA \vdash S_i \to S_j$.
Quindi:
$PA \vdash S_i \to \neg p^*$
cioè: $PA \vdash S_i \to \neg B^*$.
Si dimostra immediatamente che se il lemma vale per B e C, allora esso vale per qualsiasi combinazione vero-funzionale di B e C.
Supponiamo infine $B = \Box C$, quindi $B^* = Teor(\ulcorner C^* \urcorner)$
Se $\mathcal{M} \models_i B$, allora per ogni j tale che $i\mathcal{R}j$, $\mathcal{M} \models_j C$ e quindi, per ipotesi induttiva, per ogni j tale che $i\mathcal{R}j$: $PA \vdash S_j \to C^*$.
Dato che $i \geq 1$, $i\mathcal{R}j$ sse $i\mathcal{R}'j$, e così:
$PA \vdash V_{i\mathcal{R}'j} S_j \to C^*$.
$PA \vdash Teor(\ulcorner V_{i\mathcal{R}'j} S_j \urcorner) \to B^*$
da cui per (**7**): $PA \vdash S_i \to B^*$.
Se $\mathcal{M} \not\models_i B$, allora esiste un j, $j \geq 1$ tale che $i\mathcal{R}j$, da cui segue che $i\mathcal{R}'j$ e $\mathcal{M} \not\models_j C$.
Allora per ipotesi induttiva:
$PA \vdash S_j \to \neg C^*$
$PA \vdash \neg Teor(\ulcorner \neg S_j \urcorner) \to \neg Teor(\ulcorner C^* \urcorner)$
$PA \vdash S_i \to \neg Teor(\ulcorner \neg S_j \urcorner)$ per (**5**)
e quindi: $PA \vdash S_i \to \neg B^*$. $\Box$

Dal lemma (3.2.3), essendo A sottoproposizione di A, segue che:
$PA \vdash S_1 \to \neg A^*$
$PA \vdash A^* \to \neg S_1$ per contrapposizione
$PA \vdash Teor(\ulcorner A^* \urcorner) \to Teor(\ulcorner \neg S_1 \urcorner)$ per prop.2 di Teor
$PA \vdash \neg Teor(\ulcorner \neg S_1 \urcorner) \to \neg Teor(\ulcorner A^* \urcorner)$ per contrapposizione
$PA \vdash S_0 \to \neg Teor(\ulcorner \neg S_1 \urcorner)$ da (**5**)
e quindi:

(**8**) $PA \vdash S_0 \to \neg Teor(\ulcorner A^* \urcorner)$

5.Dimostrazione Teorema Solovay

Ora possiamo terminare la dimostrazione del teorema di completezza di Solovay per GL.

Ogni teorema di PA sappiamo essere vero. Se $i \geq 1$, allora in accordo con (**6**), se S_i è vera allora lo è anche $Teor(\ulcorner \neg S_i \urcorner)$ e quindi $\neg S_i$ è un teorema di PA, e così $\neg S_i$ è vera.

Quindi se $i \geq 1$, S_i non è vera.

In accordo con (**4**) però almeno una tra $S_0, S_1, \ldots, S_n$ è vera, quindi S_0 è vera.

Poichè S_0 è vera, per (**8**), segue che $S_0 \rightarrow \neg Teor(\ulcorner A^* \urcorner)$ è anche vera equindi è tale anche $\neg Teor(\ulcorner A^* \urcorner)$.

Ma allora A^* non è teorema di PA. $\square$

Bibliografia

[1] E.Agazzi, *Introduzione ai problemi dell'assiomatica*, Società editrice Vita e Pensiero, Milano (1961).

[2] G. Boolos, *The Logic of Provability*, Cambridge University Press, Cambridge (1994).

[3] G.Corsi, *Dispense del corso di Logica*, Bologna (2010-2011)

[4] E. Mendelson, *Introduzione alla Logica Matematica*, Serie di Logica Matematica, Bollati Boringhieri, Torino (1972).

[5] R.Rogers, *Logica matematica e teorie formalizzate*, Feltrinelli, Milano (1978).

[6] C.Smorynski, *Self-reference and modal logic*, Springer, New York (1985).