La Logica Modale applicata alla Teoria della Dimostrazione

1 Dalla logica modale alla teoria della dimostrazione

Alla base della logica modale vi sono i concetti di *necessità* e *possibiltà*; l'interesse semantico verso le proposizioni non è limitato a stabilirne le condizioni di verità o falsità, ma cerca di determinare il *modo* in cui una proposizione può essere vera o falsa e quali sianio i rapporti tra questi diversi modi. Questo modo di essere delle proposizioni, questa modalità, è solitamente chiamata *aletica*. Questo campo di ricerca ha impegnato molti illustri ingegni nel corso della storia della logica. Le origini della logica modale risalgono ad Aristotele il quale ha elaborato, sulla base della teoria del sillogismo, una teoria del silllogismo modale, la quale, in epoca recenti ha incontrato le critiche sia di logici che di alcuni tra is uoi commentatori [1]. Lo studio dei concetti di necessità e possibilità è proseguito nel medioevo soprattutto in relazione allo studio teologico della natura divina. In epoca moderna le modalità aletiche sono state un punto fondamentale della riflessione filosofica di un grande pensatore come G. W. Leibniz, il quale ha sviluppato alcune idee che sono state riprese nel secolo scorso da R. Carnap e S. Kripke per dare una caratterizzazione insiemistica delle nozioni di necessità e possibilità. La ricerca svolta sulle modalità aletiche ha aperto la strada allo studio di altri tipi di modalità. Oltre a chiederi se una proposizione è necessariamente o contingentemente vera, possiamo chiederci se rimarrà sempre vera in futuro o se prima o poi sarà vera, un discorso analogo si può fare per il passato; in questi casi si parla di modalità temporali. Inoltre si deve distinguere tra la verità di una proposizione e il ritenerla vera, tra l'attualità di un comportamento ed il fatto che sia permesso o obbligatorio; dall'esigenza di chiarire concettualmente queste distinzioni sono nate le logiche epistemiche e deontiche che si occupano delle modalità corrispondenti. Nelle prossime pagine ci occuperemo di un particolare modo di essere di una proposizione A: il fatto che A sia dimostrabile all'interno di un certo sistema formale S. Useremo tecniche sintattiche e semantiche che sono state originariamente sviluppate per lo studio della logica modale per dimostrare risultati importanti riguardo alla nozione di teorematicità in un sistema formale. Quest'ultimo concetto ha rivestito un ruolo fondamentale nello sviluppo della logica nel secolo scorso, esso è al centro di risultati come il Teorema di Completezza delle teorie del I ordine e i due teoremi di incompletezza di K. Gödel. Cosa può aggiungere di nuovo lo studio modale delle nozioni di dimostrabilità

[1] Secondo J. Łukasiewicz "La teoria aristotelica del sillogismo modale è quasi incomprensibile a causa dei suoi molti difetti e inconsistenze" [8], pg. 133. William e Martha Kneale affermano che tale teoria "è generalmente considerata confusa e insoddisfacente".

e consistenza ad un campo, quello della teoria della dimostrazione, che sembra aver raggiunto la compiutezza con la dimostrazione dei teoremi limitativi? Alla base del lavoro svolto applicando la logica modale alla teoria della dimostrazione vi è l'esigenza di chiarire concettualmente la nozione di *teorema di un sistema formale*, di fornire un punto di vista il più generale possibile di tale nozione. Questo ha reso possibile il reperimento di importanti risultati originali riguardanti la nozione di dimostrabilità; ad uno di questi rivolgeremo in particolare la nostra attenzione: il teorema del punto fisso per il calcolo GL. Boolos: "The symbolism of modal logic turns out to be an exceedingly useful notation for representing the forms of sentences of formal theories that have to do with these foundamental logical notions, and the techniques originally devised to study systems of modal logic disclose facts of great interest about these notions and their strange properties [2].". Fino ad ora abbiamo sempre parlato di dimostrabilità di una proposizione in un sistema formale, senza specificare nessun sistema in particolare. Storicamente l'attenzione si è concentrata sull'*Aritmetica di Peano*, o PA in breve. I risultati raggiunti in teoria della dimostrazione da Gödel, Rosser, Löb, ..., riguardano tutti la dimostrabilità in PA e di conseguenza la logica modale è stata inizialmente utilizzata per rendere conto della nozione di dimostrabilità in questo sistema formale.

Il teorema del punto fisso fornisce informazioni sulle condizioni di verità delle *proposizioni auto-referenziali* dell'aritmetica e di altre teorie formali.

Boolos: "The fixed point theorem may be used to demystify certain "self-referential" characterizations of PA [3].".

Con l'aiuto del teorema del punto fisso possiamo vedere come rimpiazzare certe caratterizzazioni "auto-referenziali" di formule dell'aritmetica con descrizioni equivalenti, che non implicano una tale "auto-referenzialità"pg. xxx. Continua . . . .

2 L'aritmetica di Peano

Condizioni di derivabilità di Hilbert-Bernays-Löb:

1. se $\vdash S$ allora $\vdash Bew(\ulcorner S \urcorner)$,
2. $\vdash Bew(\ulcorner S \to T \urcorner) \to (Bew(\ulcorner S \urcorner) \to Bew(\ulcorner T \urcorner))$,
3. $\vdash Bew(\ulcorner S \urcorner) \to Bew(\ulcorner Bew(\ulcorner S \urcorner) \urcorner)$,

[2] [2], pg. xviii.
[3] [2], pg. xxx.

3 Il predicato 'Bew' come modalità

Una volta che si è stabilito di interpretare il Box $\Box$ come "è dimostrabile che ..." piuttosto che come "è necessario che ...", sorge immediatamente la questione di trovare una calcolo modale che rispecchi il comportamento del predicato *Bew* in PA. La risposta a questa domanda è fornita dal teorema di completezza aritetica per GL di R. Solovay, che costituisce forse il più importante risultato sintattico della logica modale applicata alla teoria della dimostrazione. Tale risultato ci consente di dimostrare fatti importanti riguardanti l'aritmetica di Peano, lavorando esclusivamente con formule modali, senza mai fare riferimento a concetti aritmetici. Il Teorema del punto fisso che dimostreremo nel paragrafo 5 è uno di questi fatti importanti. Non daremo la dimostrazione del teorema di completezza aritmetica per GL, tale dimostrazione estremamente sofisticata richiederebe una ben più profonda trattazione di quella che è possibile dare in poche pagine. Per poter enunciare tale risultato abbiamo bisogno di precisare cosa intendiamo quando affermiamo di interpretare il Box come il predicato *Bew* di PA.

Definizione 3.0.1 Una *realizzazione* è una funzione $\sharp$ dall'insieme V delle variabili proposizionali dell linguaggio di GL all'insieme delle formule chiuse sul linguaggio di PA. La *traduzione* $A\sharp$ di una formula modale A indotta da una realizzazione $\sharp$ è definita induttivamente in modo unico:

1. se A è una variabile proposizionale p allora $p\sharp = \sharp(p)$,
2. se $A = \bot$ allora $\bot\sharp = \bot$,
3. se $A = B \to C$ allora $(B \to C)\sharp = (B\sharp \to C\sharp)$,
4. se $A = \Box B$ allora $(\Box B)\sharp = Bew(\ulcorner A\sharp \urcorner)$.

Osservazioni.

1. Poiché le costanti logiche $\bot$ e $\to$ appaiono anche tra i simboli del linguaggio di PA, ogni traduzione $A\sharp$ di una formula modale A è una formula di PA, indipendentemente dalla scelta della realizzazione $\sharp$.
2. Le clausole (3) e (4) garantiscono che la traduzione di una combinazione vero-funzionale di formule modali corrisponde alla combinazione della traduzione delle formule stesse. La clausola (4) garantisce che se $A\sharp = S$ allora $(\Box A)\sharp = Bew(\ulcorner S\sharp \urcorner)$, cioè il risultato di sostituire la variabile libera x in $Bew(x)$ con il numerale per il numero di G'ödel della formula S. La formula $Bew(\ulcorner S\sharp \urcorner)$ è interpretata in PA come l'asserzione della dimostrabilità di S.

3. La traduzione $A\sharp$ di una formula A è fissata in modo unico dalla realizzazione $\sharp$, ciò significa che se due realizzazioni $\sharp$ e $\star$ coincidono sui valori assegnanti alle variabili proposizionali, allora per ogni formula modale A, $A\sharp = A\star$.

Se siamo interessati a stabilire quali leggi modali sono valide interpretando il Box come "è dimostrabile che…", allora dobbiamo stabilire quali siano le leggi modali A la cui traduzione $A\sharp$ sia dimostrabile in PA indipendentemente dalla traduzione $\sharp$. Una formula modale A con questa caratteristica è detta *sempre dimostrabile*. Il teorema di correttezza aritmetica di GL afferma che se GL dimostra una formula modale A allora A è sempre dimostrabile in PA, la dimostrazione è per induzione sulla lunghezza della dimostrazione di A in GL è non presenta particolari difficoltà. Il teorema di completezza aritmetica di GL, la cui dimostrazione è dovuta a R. Solovay, stabilisce l'altro verso dell'implicazione: se una formula modale A è sempre dimostrabile in PA allora è un teorema di GL. Questo risultato si dimostra per contrapposizione: se $GL \nvdash A$ allora per ogni $p_1, \ldots, p_n$ variabili proposizionali contenute in A si possono trovare delle formule $S_1, \ldots, S_n$ di PA e una realizzazione $\star$ per la quale $\star(p_i) = S_i, 1 \leqslant i \leqslant n$ tali che $PA \nvdash A\star$. Riassumiamo questi risultati nel seguente teorema di adeguatezza aritmetica di GL.

Teorema 3.0.2 (Teorema di adeguatezza aritmetica di GL) *Una formula modale A è dimostrabile in GL sse è sempre dimostrabile in PA*

Questo teorema afferma che il calcolo GL ci fornisce una caratterizzazione delle proprietà del predicato *Bew* nell'aritmetica di Peano. Perciò possiamo dimostrare fatti importanti riguardo alla nozione di "dimostrabilità in PA" all'interno di GL

4 Un calcolo modale per l'aritmetica di Peano: il sistema GL

4.1 La sintassi del calcolo GL

Il sistema che prenderemo in considerazione è solitamente indicato con la sigla GL che sta per Gödel-Löb. Nella letteratura si indica GL anche con altre sigle come PRL[4] e $K4W$[5] In contrasto con quanto avviene solitamente nella letteratura sull'argomento, in questo paragrafo ci concentreremo esclusivamente sul calcolo GL tralasciando gli altri sistemi rilevanti di logica modale. Tale scelta

[4] Cfr. [13]

[5] Tale nome deriva dalle sigle usate per i singoli assiomi

è motivata da una necessità di coincisione che ci consiglia di introdurre solo le nozioni strettamente necessarie alla trattazione del teorema del punto fisso per GL.
Partiamo innazitutto da una serie di definizioni che ci permetteranno di introdurre questo calcolo.

Definizione 4.1.1 (Formule modali) Il *linguaggio* L è una tripla ordinata $\langle V, C, P\rangle$ in cui V è un insieme numerabile di variabili proposizionali $p_1, \ldots, p_n, \ldots$; C è l'insieme formato dalle costanti proposizionali $\bot, \to, \Box$; P è l'insieme che contiene le parentesi (e).
L'insieme F delle $formule\ modali$ ($formule$, in breve) sul linguaggio L è il minimo insieme t. c.:

1. $V \subseteq F$,
2. $\bot \in F$,
3. Se $A \in F$ allora anche $(\Box A) \in F$,
4. Se $A, B \in F$ allora anche $(A \to B) \in F$.

Adottiamo le convenzioni comunemente in uso sulla semplificazione delle parentesi. Inoltre è possibile definiamo la costante proposizionale $\top$ come $\bot \to \bot$ e $\neg A$ come $A \to \bot$; a questo punto possiamo inoltre introdurre $A \wedge B$ come $\neg(A \to \neg B)$, $A \vee B$ come $\neg A \to B$, $A \leftrightarrow B$ come $A \to B$ e $B \to A$ e infine $\Diamond A$ come $\neg\Box\neg A$. Tale modo di introdurre le altre costanti proposizionali rende molto meno pesanti le dimostrazioni per induzione sulla complessità della formula. Di questo fatto forniremo immediatamente due di esempi.

Definizione 4.1.2 (Sottoformula) Sia A una formula modale, definiamo la nozione di sottoformula di A come:

1. A è una sottoformula di se stessa,
2. se $\Box B$ è una sottoformula di A, allora B è una sottoformula di A,
3. se $B \to C$ è una sottoformula di A, allora B e C sono sottoformule di A.

Una formula modale B *occorre in* A sse B è una sottoformula di A. Sia A una formula, definiamo per induzione sulla complessità di A il risultato $A_p(B)$ di sostituire in A le occorrenze della variabile proposizionale p con la formula B:

Definizione 4.1.3 (Sostituzione) 1. se $A = p$ allora $A_p(B) = B$,

2. se A è una variabile proposizionale $q \neq p$ allora $A_p(B) = q$,
3. se $A = \bot$ allora $A_p(B) = \bot$,
4. se $A = C \to D$ allora $A_p(B) = C_p(B) \to D_p(B)$,
5. se $A = \Box C$ allora $A_p(B) = \Box(C_p(B))$.

Per precisare le nozioni di *dimostrazione in un sistema formale* e di *teorema* faremo riferimento a definizioni comunemente accettate per le quali si intende la prima come una successione finita di formule, ciascuna delle quali è un assioma o è stata ottenuta tramite l'applicazione di una regola di inferenza da formule che appaiono prima nella sequenza; la seconda come la formula che appare al termine una tale sequenza. Indicheremo con $S \vdash A$ il fatto che A è un teorema del calcolo S. Introduciamo ora il calcolo GL

Definizione 4.1.4 Il calcolo logico GL contiene tutti gli schemi di assiomi della logica classica K, inoltre contiene tutti gli schemi di assiomi della forma:

1. $\Box(A \to B) \to (\Box A \to \Box B)$ (assioma di distribuzione)
2. $\Box(\Box A \to A) \to \Box A$ (assioma di Löb) Le regole del calcolo sono
3. se $GL \vdash A \to B$ e $GL \vdash A$ allora $GL \vdash B$ (modus ponens)
4. se $GL \vdash A$ allora $GL \vdash \Box A$ (regola di necessitazione)

Il calcolo GL è un calcolo *normale*, come alcuni tra i più studiati sistemi di logica modale: T, D, B, $S4$ e $S5$; contiene cioè tutte le leggi logiche classiche, l'assioma di distribuzione ed è chiuso sotto le regole di necessitazione, modus ponens. Inoltre GL è chiuso sotto la regola di sostituzione, cioé se $GL \vdash A$ allora $GL \vdash A_p(B)$; infatti se la sequenza $C^1, \ldots, C^n$ è una dimostrazione in GL di $A = C^n$, allora la sequenza $C^1_p(B), \ldots, C^n_p(B)$ sarà una dimostrazione di $A_p(B) = C^n_p(B)$.
Per brevità non prenderemo in considerazioni i rapporti sussistenti tra il calcolo GL e gli altri sistemi normali di logica modale, anche se vi sono importanti risultati in questo campo come l'impossibilità di un'estensione normale e consistente comune a GL e a T. Presenteremo ora alcuni risultati sintattici che riguardano diversi calcoli normali in generale e il calcolo GL in particolare. Non forniremo la dimostrazione di questi lemmi preliminari per non appesantire troppo l'esposizione e in quanto si tratta di dimotrazioni di *routine* sulla complessità della formula. In quanto segue indicheremo con $\boxdot A$ la formula $\Box A \wedge A$.

Primo lemma di sostituzione 4.1.5 *Se* $GL \vdash (A \leftrightarrow B)$ *allora* $GL \vdash (F_p(A) \leftrightarrow F_p(B))$

Dimostrazione. Per induzione sulla complessità di F

Un altro importante risultato sintattico che riguarda GL è la dimostrabilità dell'assioma caratteristico del sistema $S4$: $\Box A \rightarrow \Box\Box A$. Come osserva G. Boolos se $\Box A \rightarrow \Box\Box A$ non fosse stato un teorema di GL allora si sarebbe presa in considerazione l'estrensione minima di GL che comprende anche tale formula, infatti la traduzione di questa formula nell'aritentica di Peano esprime una delle caratteristiche fondamentali del predicato Bew. INoltre la dimostrabilità di questo teorema in GL permette di dimostrare una seconda versione del lemma di sostituzine.

Secondo lemma di sostituzione 4.1.6

$$GL \vdash \boxdot(A \leftrightarrow B) \rightarrow (F_p(A) \leftrightarrow F_p(B))$$

Dimostrazione. Per induzione sulla complessità di F

Il Lemma 1 è una diretta conseguenza del Secondo lemma di sostituzione.

Lemma 4.1.7

$$GL \vdash \boxdot(A \leftrightarrow B) \rightarrow \boxdot(F_p(A) \leftrightarrow F_p(B))$$

Inserisci i più importanti risultati sintattici ottenuti per GL: il teorema di correttezza e il teorema di completezza algebrica per GL

4.2 La semantica del calcolo GL

In questo paragrafo introdurremo una semantica di tipo kripkeano per il calcolo GL e daremo i risultati di correttezza e completezza di GL rispetto a questa semantica. Non forniremo le dimostrazioni complete di questi risultati in quanto il nostro interesse non è rivolto tanto ad essi quanto alla possibilità di introdurre tecniche semantiche nella dimostrazioni di risultati sintattici. La semantica di tipo kripkeano ha il vantaggio, rispetto all'approccio puramente sintattico, di rendere molto più intellegibili le nozioni modali e più chiare e comprensibili le dimostrazioni. Tale vantaggio risulterà evidente proprio nella dimostrazione del Teorema del punto fisso. Le semantiche introdotte da S. Kripke in [6] riprendono un'idea esposta per la prima volta da G. L. Leibniz secondo la quale oltre al mondo attuale, esistono altri mondi possibili, più o meno diversi da quello abitato da noi. A questo punto è necessario ciò che è vero in ogni mondo possibile, mentre è possibile ciò che è vero in almeno un mondo. Kripke ha ripreso questa concezione leibniziana delle nozioni di possibilità e necessità, modificandola per dotare alcuni tra i più studiati sistemi di logica modale di una utile semantica. Il contributo certamente più importante dato da Kripke consiste nell'introduzione di una relazione di accessibilità tra mondi; in questo modo si relativizzano i concetti di possibili e necessario, per noi non è più necessario ciò che è vero in ogni mondo possibile ma solo ciò che è vero nei mondi possibili accessibili dal nostro. Questa relativizzazione permette di trattare non solo diverse concezioni delle modalità aletiche, ma anche mdalità differenti (deontiche, temporali, ecc...). Passiamo ora alla precisazione concettuale di queste intuizioni; per svolgere questo compito abbiamo bisogno di una serie di definizioni.

Definizione 4.2.1 R è una relazione su W sse per ogni x, y, se xRy allora $x, y \in W$.
R è una relazione $irriflessiva$ su W sse non esiste $x \in W$ t. c. xRx.
R è una relazione $transitiva$ su W sse per ogni $x, y, z \in W$, se xRy e yRz allora xRz.
R è una relazione $benfondataalcontrario(?)$ su W sse per ogni sottoinsieme non vuoto X di W, esiste un elemento R-massimo in X, cioè un elemento x di X t. c. per ogni $y \in W$ non xRy.

Si noti che se R è ben fondata al contrario allora R è anche irriflessiva, infatti se valesse xRx allora $\{x\}$ sarebbe un sottoinsieme non vuoto di W senza un elemento R-massimo.

Definizione 4.2.2 (struttura) Una *struttura* è una coppia ordinata $\langle W, R \rangle$ in cui W è un insieme non vuoto, detto $dominiodellastruttura$, mentre R è una relazione binaria su W, detta *relazione di accessibilità*.

La struttura $\langle W, R \rangle$ è finita sse lo è W. Intuitivamente si può considerare il dominio W come l'insieme dei mondi possibili; la relazione di accessibilità R stabilisce quali mondi sono accessibili a partire da altri. Con una abuso di linguaggio stabiliamo di attribuire direttamente alla struttura $\langle W, R \rangle$ le proprietà della relazione R. Introduciamo ora la nozione di $valutazione$ di una formula in un mondo possibile.

Definizione 4.2.3 (valutazione) Sia v' una funzione dall'insieme di coppie ordinate $W \times V$ all'insieme $\{V, F\}$ composto dai due valori di verità t. c. $v'(w, \bot) = F$ per ogni $w \in W$. Definiamo una valutazione v delle formule nei mondi possibili come la funzione che estende in modo unico v' t. c.:

1. se $A = p, \bot$ allora $v(w, p) = v'(w, p)$,

2. se $A = B \to C$ allora $v(w, A) = V$ sse $v(w, B) = F$ o $v(w, C) = V$,

3. se $A = \Box B$ allora $v(w, A) = V$ sse per ogni x, se wRx allora $v(x, B) = V$.

In quanto segue useremo $w \vDash A$ per indicare che $(w, A) = V$, di conseguenza $w \nvDash A$ starà per $(w, A) = F$. Nel primo caso diremo che la formula A è *vera* nel mondo possibile w, secondo caso diremo che essa è $falsa$ in w.

Definizione 4.2.4 (modello) Un *modello* M è una tripla ordinata $\langle W, R, v\rangle$ t. c. $\langle W, R\rangle$ è una struttura e v è una valutazione delle formule modali nei mondi possibili. Il modello M è basato sulla struttura $\langle W, R\rangle$.

Se $M = \langle W, R, v\rangle$ per qualche v, allora si dice che M è il modello basato sulla struttura $\langle W, R\rangle$. Con un altro abuso di linguaggio stabiliamo di attribuire direttamente al modello $\langle W, R\rangle$ le proprietà della relazione R. A questo punto possiamo introdurre le nozioni di validità in un modello e in un frame.

Definizione 4.2.5 (validità) Una formula A è *valida* in un modello $M = \langle W, R, v\rangle$, in simboli $M \vDash A$, sse per ogni $x \in W$, $x \vDash A$.
Una formula A è *valida* in una struttura $\mathcal{F} = \langle W, R\rangle$, in simboli $\mathcal{F} \vDash A$, sse per ogni M basato su $\langle W, R\rangle$ si ha $M \vDash A$.

In quanto segue diremo che una formula A è *soddisfacibile in un modello* $M = \langle W, R, v\rangle$ sse esiste $X \in W$ t. c. $x \vDash A$. In modo simile una formula A è *soddisfacibile in una struttura* $\mathcal{F} = \langle W, R\rangle$ sse esiste un modelo M basato su $\mathcal{F}$ e $M \vDash A$. Ora abbiamo tutti gli strumenti necessari per dimostrare i risultati di correttezza e completezza del calcolo GL rispetto alle strutture appena introdotte. Come è già stato anticipato non forniremo questi risultati nei dettagli, soprattutto per quanto riguarda il teorema di completeza, in quanto l'interesse di questi teoremi è limitato all'uso che ne faremo nella dimostrazione del Teorema del punto fisso.

Teorema 4.2.6 (correttezza di GL) *Per ogni formula modale A, se A è dimostrabile in GL allora A è valida in ogni struttura transitiva e ben fondata al contrario*

Dimostrazione. La dimostrazione procede per induzione sulla lunghezza della dimostrazione di A. Innanzitutto notiamo che le tautologie della logica classica e l'assioma di distribuzione sono validi in unastruttura $\mathcal{F}$ qualsiasi. Le regole di modus ponens, necessitazione e sostituzione mantengono la validità nella struttura. Rimane da verificare che il postulato caratteristico di GL, l'assioma di Löb, sia valido in ogni struttura transitiva e ben fondata al contrario, cioè, che per qualsiasi $x \in W$, per qualsiasi valutazione v, $w \models \Box(\Box A \to A) \to \Box A$. Supponiamo per assurdo che esista $x \in W$ t. c. $x \models \Box(\Box A \to A)$ e $x \not\models \Box A$. Questo significa che esiste $y \in W$ e xRy, $y \models \Box A \to A$, $y \not\models A$. Per poter soddisfare l'implicazione è necessario che $y \not\models \Box A$, quindi esiste $z \in W$ t. c. yRz, $z \not\models A$. Per transitività di R si ha inoltre che xRz e perciò $z \models \Box A \to A$. Ci troviamo in z nella stessa situazione in cui eravamo in y, siamo quindi costretti a introdurre un insieme infinito $\{x_1, \dots, x_n, \dots\}$ di mondi possibili, e per ciascuno dei x_i si ha xRx_i, $x_i \models \Box A \to A$, $x_i \not\models A$. Se consideriamo ora l'insieme $X = \{w \in W | xRw \wedge w \not\models A\}$ si vede chiaramente che è infinito, perciò non esiste in X un elemento R-massimo e quindi R non è ben fondata al contrario.

Teorema 4.2.7 (completezza di GL**)** *Per ogni formula modale A, se A è valida in ogni struttura transitiva e ben fondata al contrario allora A è dimostrabile in GL*

Dimostrazione. La dimostrazione del tereoma di completezza avviene per contrapposizione. Si dimostra che se A non è un teorema di GL allora esiste una struttura transitiva e ben fondata al contrario e un modello su questa struttura t. c. $M \not\models A$. Tale struttura è composta dall'insieme W di insiemi consistenti e massimali contenenti sottoformule di A. Una formula B viene valutata vera inun mondo w sse $B \in w$. Poiché $GL \nvdash A$, $\neg A$ appartiene a qualche insieme consistente massimale $w \in W$, per consistenza $A \notin w$ e quindi $wnvDashA$.

Unendo assieme i due risultati appena dimostrati otteniamo l'adeguatezza del calcolo GL rispetto alle strutture transitive e ben fondate al contrario. Registriamo questo risultato nel prossimo teorema.

Teorema 4.2.8 (adeguatezza di GL**)** *Per ogni formula modale A, A è valida in ogni struttura transitiva e ben fondata al contrario sse A è dimostrabile in GL*

Questo risultato può essere rafforzato in due sensi. Per prima cosa si può dimostrare che non occorre prendere in considerazione tutte le strutture transitive e ben fondate al contrario, basta limitarsi a considerare quelle in cui l'insieme W dei mondi possibili è finito; l'insieme delle strutture transistive, ben fondate al contrario e finite è, cioè, adeguato per il calcolo GL. Da ciò segue che GL ha la proprietà del modello finito e quindi è un calcolo decidibile. Un ulteriore rafforzamento del risultato di adeguatezza è costituito dalla possibilità di limitarsi a considerare le strutture transitive, irriflessive, finite. Si è già dimostrato dopo la definizione 4.2 che una struttura ben fondata al contrario è anche irriflessiva; l'implicazione inversa non è sempre vera, ma lo è nel caso in cui la struttura $\mathcal{F}$ sia transitiva e finita. Infatti, sia $x_1, \dots, x_n$ una successione di elementi di W t. c. per ogni $i < n$, $x_i R x_{i+1}$. Si osservi che se $i < j$ allora $x_i \neq x_j$, altrimenti per transitività si avrebbe $x_i R x_j$ contro l'irriflesività. Assumiamo ora che $\mathcal{F}$ non sia ben fondato al contrario. Sia X un sottoinsieme non vuoto di W t. c. per ogni $w \in X$ esiste $x \in X$ e wRx. Si dimostra per induzione che per ogni n naturale positivo esiste una successione $x_1, \dots, x_n$ di elementi di X t. c. per ogni $i < n$, $x_i R x_{i+1}$. Quindi per ogni n, ci sono almeno n elementi in $X \subseteq W$, perciò W è infinito contro l'ipotesi. Quanto appena dimostrato ci consente di dare una nuova formulazione del teorema di adegauteza per GL.

Teorema 4.2.9 (adeguatezza di GL) *Per ogni formula modale A, A è valida in ogni struttura transitiva, irriflessiva, finita sse A è dimostrabile in GL*

Una delle conseguenze immediate di questo teorema, tra le più utili, è la possibilità di dimostrare risultati sintattici attraverso ragionamenti i tipo semantico. Per concludere che GL dimostra una certa formula A basterà far vedere che A è soddisfatta da un mondo arbitrario w per una assegnazione arbitraria v di valori alle variabili proposizionali, per poi applicare il teorema di adeguatezza. Tale modo di procedere è in efetti molto più comodo quando si devono trattare formule con molte modalità incassate le une con le altre.

Osservazione: 1) la buona fondatezza al contrario non è caratterizzabile on una formula del primo ordine. 2) Non esiste formula modale che sia valida esattamente nelle strutture transitive e ben fondate al contrario.

Il secondo teorema di incompletezza di Gödel (per PA) afferma che se l'aritmetica è consistente, allora la consistenza dell'aritmetica non è dimostrabile nell'aritmetica stessa. Poiché $\neg\Box\bot \rightarrow \neg\Box\neg\Box\bot$ è un teorema di GL, per una qualsiasi traduzione $\sharp$ $PA \vdash (\neg\Box\bot \rightarrow \neg\Box\neg\Box\bot)\sharp$, cioè $PA \vdash \neg Bew\ulcorner\bot\urcorner \rightarrow \neg Bew\ulcorner\neg Bew\ulcorner\bot\urcorner\urcorner$, ma questo teorema di PA è l'aritmetizzazione dell'asserzione che se'aritmetica è consistente, allora la consistenza dell'aritmtica non è dimostrabile in essa stessa. Quindi il secondo teorema di completezza di Gödel, che è dimostrabile matematicamente, è addirirttura dimostrabile in PA.

Il teorema di Löb formalizzato afferma che per ogni formula S, $PA \vdash Bew(\ulcorner(Bew(\ulcorner S\urcorner) \rightarrow S)\urcorner) \rightarrow Bew(\ulcorner S\urcorner)$. Poiché $GL \vdash \Box(\Box p \rightarrow p) \rightarrow \Box p$ per il teorema di adeguatezza aritmetica $PA \vdash (\Box(\Box p \rightarrow p) \rightarrow \Box p)\sharp$, per ogni traduzione $\sharp$. Poiché ogni formula $S = \sharp(p)$ per qualche realizzazione $\sharp$, il teorema di Löb formalizzato vale in PA.

5 Il teorema del punto fisso per GL

Il teorema del punto fisso è stato dimostrato indipendentemente da G. Sambin in [11], [12] e da D. de Jongh, la dimostrazione fornita da de Jongh era di tipo semantico e così complicata che non fu mai pubblicata.

Esistono tre diverse dimostrazioni del teorema del punto fisso per il calcolo GL. Due di queste sono costruttive, forniscono cioè un algoritmo, un procedimento effettivo per poter calcolare il punto fisso H di una certa formula A modalizzata in p. La terza, invece è non costruttiva è dimostra unicamente l'esistenza del punto fisso come corollario del Lemma di unicità dei punti fissi e del teorema di definibilità di Beth per GL che può essere a sua volta ricavato dal teorema di interpolazione di Craig per GL; non viene fornito nassun metodo per il calcolo dei punti fissi. Delle due dimostrazioni costruttive, la prima è dovuta a G. Sambin e a D. de Jongh e, nella sua forma originaria fa uso prettamente di tecniche di teoria della dimostrazione. Il metodo che viene fornito per il calcolo dei punti fissi rende possibile ricavarli in modo tale che la loro struttura sia simile a quella delle formule di partenza. L'altra dimostrazione costruttiva è dovuta a Z. Gleit e W. Goldfarb e fa uso di tecniche della teoria dei modelli. L'algoritmo fornito da questa dimostrazione permette di trovare un punto fisso H di grado modale $\leqslant n$, cioè in cui vi sono formule con al massimo n modalizzatori successivi, dove n è il numero di modalizzatori presenti in A. Questa dimostrazione fornisce il migliore limite possibile al numero di modalizzatori successivi nel punto fisso H. Infine ricordiamo la dimostrazione data indipendentemente da C. Bernardi e C. Smoriński del Teorema del punto fisso per A modalizzata in p in cui non appaiono altre variabili proposizionali oltre p. Questo caso è di particolare interesse in quanto molte importanti proposizioni, come quella di Gödel, rientrano in questo caso. Le tecniche utilizzate nella dimostrazione del caso generale non possono essere considerate in nessun modo come generalizzazioni di questo caso particolare.

Come afferma Lisa Reidhaar-Olson, "The existing syntactic proofs tend to be rather complicated and magical, yet they do provide reasonable algorithms for the explicit calculation of fixed-point. [...] The previously existing semantic proofs, on the other hand, tend to displel the mystery concerning the reasons for the truth of the theorem, yet provide unreasonably cumbersome algorithms for computation. Also, the fixed-points do not tend to 'look like' the formulas from which they are derived."[6]

La dimostrazione data dalla Reidhaar-Olson ha il pregio della chiarezza dato dall'approccio semantico e fornisce un algoritmo per il calcolo di punti fissi che nella struttura sono molto simili alle formule di partenza.

Si dice che F è $k-$*decomponibile* se per qualche sequenza, possibilmente vuota $q_1, \ldots, q_k$ di variabili proposizionali distinte, per qualche proposizione $B(q_1, \ldots, q_k)$ che non contiene p ma che contiene ciascuna delle $q_1, \ldots, q_k$ e per qualche sequenza di proposizioni distinte $D_1(p), \ldots, D_k(p)$, ciascuna con-

[6]in [10], pg 37

tenente p,

$$F = B(\Box D_1(p), \ldots, \Box D_k(p))$$

Poiché A è modalizzata in p allora, per qualche k è k-decomponibile. La dimostrazione del Teorema del Punto Fisso è per induzione su k che varia sui naturali.

Per k=0 si ha che A è 0-decomponibile, cioé esiste una formula B che non contiene p e A=B. A questo punto basti notare che A non contiene p e quindi può essere presa come un punto fisso di se stessa.

Per completare l'induzione su k supponiamo che ogni formula k-decomponibile che è modalizzata in p abbia un punto fisso, assumiamo inoltre che A è $(k+1)$-decomponibile e modalizzata in p; bisogna ora dimostrare che la formula A ha un punto fisso.

Per le nostre assunzioni $A = B(\Box D_1(p), \ldots, \Box D_{k+1}(p))$ per qualche B, $q_1, \ldots, q_{k+1}$ e $D_1(p), \ldots, D_{k+1}(p)$.

Per ogni i, $1 \leqslant i \leqslant k+1$, sia A_i la formula

$$B(\Box D_1(p), \ldots, \Box D_{i-1}(p), \top, \Box D_{i+1}(p), \ldots, \Box D_{k+1}(p))$$

Ciascuna delle A_i è k-decomponibile e modalizzata in p e quindi esiste un punto fisso H_i di A_i. Consideriamo ora la formula

$$H = B(\Box D_1(H_1), \ldots, \Box D_{k+1}(H_{k+1}))$$

Dimostreremo che H è un punto fisso di A Aggiungere altrove: questa costruzione del punto fisso per A è dovuta a G. Sambin che ha fornito una dimostrazione sintattica della sua correttezza. La dimostrazione utilizzata da G. Boolos è quella che si trova nell'articolo della Reidhaar-Olson è utilizza tecniche semantiche. Nei prossimi quattro lemmi M è un modello finito, transitivo e irriflessivo, $w, x, y \in W$, e $1 \leqslant i \leqslant k+1$.

Lemma 1 *Supponiamo che* $y \models \boxdot(p \leftrightarrow A)$ *e che* $y \models \Box D_i(p)$. *Allora* $y \models D_i(p) \leftrightarrow D_i(H_i)$ *e* $y \models \Box D_i(p) \leftrightarrow \Box D_i(H_i)$

Dimostrazione

Poiché $y \models \Box D_i(p)$, per tutti gli z, yRz implica $z \models \Box D_i(p)$. Da questo si ricava che $y \models \Box D_i(p) \leftrightarrow \top$, e per tutti gli z, yRz implica $z \models \Box D_i(p) \leftrightarrow \top$. Quindi $y \models \boxdot(\Box D_i(p) \leftrightarrow \top)$. Per il Lemma 2 si ottiene che $y \models \boxdot(A \leftrightarrow A_i)$. Ancora per il Lemma 2, da $y \models \boxdot(A \leftrightarrow A_i)$ e dalla ipotesi $y \models \boxdot(p \leftrightarrow A)$, si ottiene che $y \models \boxdot(p \leftrightarrow A_i)$. Poiché H_i è un punto fisso di A_i, si ha $y \models \boxdot(p \leftrightarrow H_i)$; per il primo teorema di sostituzione $y \models D_i(p) \leftrightarrow D_i(H_i)$ e per uno dei lemmi ausiliari $y \models \Box D_i(p) \leftrightarrow \Box D_i(H_i)$.

Lemma 2 $x \models \boxdot(p \leftrightarrow A) \rightarrow \boxdot(\Box D_i(p) \rightarrow \Box D_i(H_i))$

Dimostrazione
Supponiamo che x soddisfi l'antecedente, cioè che $x \models \boxdot(p \leftrightarrow A)$, e che per ogni y, xRy o $x = y$ implica $y \models \Box D_i(p)$. Dalla prima ipotesi si ricava che $y \models \boxdot(p \leftrightarrow A)$ e per il Lemma 1 si ottiene che $y \models \Box D_i(H_i)$.

Lemma 3 $w \models \boxdot(p \leftrightarrow A) \rightarrow \boxdot(\Box D_i(H_i) \rightarrow \Box D_i(p))$

Dimostrazione
Supponiamo che x soddisfi l'antecedente, cioè che $w \models \boxdot(p \leftrightarrow A)$, e che per contrapposizione per ogni x, wRx o $w = x$ implica $x \models \neg\Box D_i(p)$. Ciò significa che esiste y di rango minimo t. c. xRy e $y \models \neg D_i(p)$; inoltre per ogni z, se yRz allora per transitività xRz e siccome $\rho(z) < \rho$ (y), $z \models D_i(p)$, per cui $y \models \Box D_i(p)$. Poiché $w \models \boxdot(p \leftrightarrow A)$ e wRy, si ottiene $y \models \boxdot(p \leftrightarrow A)$ e per il Lemma 1 si ha $y \models D_i(p) \leftrightarrow D_i(H_i)$. Quindi $y \models \neg D_i(H_i)$ e infine $x \models \neg\Box D_i(H_i)$.

Lemma 4 $w \models \boxdot(p \leftrightarrow A) \rightarrow \boxdot(\Box D_i(p) \leftrightarrow \Box D_i(H_i))$

Dimostrazione
Il lemma segue dai Lemmi 2 e 3.

Il teorema del Punto Fisso segue in modo immediato dal Lemma 4 e dal Secondo Teorema di Sostituzione:

$$\begin{array}{rcl} w \models \boxdot(p \leftrightarrow A) & \rightarrow & B(\Box D_1(p), \Box D_2(p), \ldots, \Box D_{k+1}(p)) \\ & \leftrightarrow & B(\Box D_1(H_1), \Box D_2(p), \ldots, \Box D_{k+1}(p)) \\ & \leftrightarrow & B(\Box D_1(H_1), \Box D_2(H_2), \ldots, \Box D_{k+1}(p)) \leftrightarrow \ldots \\ & \leftrightarrow & B(\Box D_1(H_1), \Box D_2(H_2), \ldots, \Box D_{k+1}(H_{k+1})) \end{array}$$

cioè $w \models \boxdot(p \leftrightarrow A) \rightarrow (A \leftrightarrow H)$. Quindi $\boxdot(p \leftrightarrow A) \rightarrow (A \leftrightarrow H)$ è una formula valida in tutti i modelli finiti, transitivi e irriflessivi; perciò per il teorema di completezza è anche un teorema di GL. Infine si ottiene il risultato desiderato applicando i teoremi di sostituzione.

5.1 Osservazioni

Il punto fisso H di A è ottenuto sostituendo le diverse occorrenze di p in A con i punti fissi H_i dei vari A_i, per $1 \leqslant i \leqslant k+1$. Quindi, adoperando questa procedura, si vede chiaramente che la struttura del punto fisso H sarà simile a quella di A. La scelta della B dalla quale si ottiene A tramite la sostituzione delle variabili proposizionali $q_1, \ldots, q_{k+1}$ con le $D_1(p), \ldots, D_{k+1}(p)$, non è determinata in modo unico. Ad esempio, se $A = \Box\Box p$ allora possiamo prendere $B(q_1) = q$ e $D_1(p) = \Box p$, oppure possiamo prendere $B(q_1) = \Box q$ e $D_1(p) = p$. Diverse analisi di A possono condurre a dei punti fissi considerevolmente diversi come complessità, ma naturalmente tutti equivalenti tra di loro in GL.

6 Le conseguenze del teorema del punto fisso

In questo paragrafo mostreremo come il teorema del punto fisso possa essere utilizzato per ricavare alcuni importanti risultati in teoria della dimostrazione.

Il teorema di Löb diventa una diretta conseguenza del teorema del punto fisso. Supponiamo che $PA \vdash Bew(\ulcorner S \urcorner) \leftrightarrow S$, stabiliamo una realizzazione $\sharp$ t. c. $\sharp(p) = S$, quindi $Bew(\ulcorner S \urcorner) \leftrightarrow S = (\Box p \leftrightarrow p)\sharp$. Per il teorema di adeguatezza algebrica del calcolo GL si ha $GL \vdash (\Box p \leftrightarrow p)\sharp$; a questo punto applichiamo il teorema del punto fisso per $A = \Box p$ e otteniamo che $GL \vdash \boxdot(p \leftrightarrow \Box p) \leftrightarrow \boxdot(p \leftrightarrow \top)$. Tramite calcolo proposizionale si ottiene ancora che $GL \vdash (p \leftrightarrow \top)$, cioè $GL \vdash p$. Un'altra applicazione del teorema di adeguatezza aritmetica di GL ci consente di concludere che $PA \vdash p\sharp$, cioè che $PA \vdash S$.

References

[1] Boolos G., *The Unprovability of Consistency: An Essay in Modal Logic*, Cambridge University Press, Cambridge, 1979.

[2] Boolos G., *The Logic of Provability*, Cambridge University Press, Cambridge, 1993.

[3] Gleit Z., *Box and Bew: Modal Logic and Provability*, Undergraduated Thesis, Philosophy and Mathematics Departments, Harvard University, 1987.

[4] Goldfarb W., Gleit Z., "Characters and fixed-points in provability logic", *Notre Dame Journal of Formal Logic*, 31, 1990, pg. 26-36.

[5] Kneale W e Kneale M., *The DEvelopment of Logic*, Oxford University Press, Oxford, 1984.

[6] Kripke S., "A completeness theorem in modal logic", *Journal of Symbolic Logic*, 24, 1959, pg. 1-14.

[7] Kripke S., "Semantical analysis of modal logic I. Normal modal propositional calculi", *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, 9, 1963, 67-96.

[8] Łukasiewicz J., *Aristotle's Syllogistic*, II ed., Oxford University Press, Oxford, 1957.

[9] Reidhaar-Olson L., "A New Proof of the Fixed-Point Theorem of Provability Logic", Master's Thesis, Mathematics Department, M.I.T., 1988.

[10] Reidhaar-Olson L., "A New Proof of the Fixed-Point Theorem of Provability Logic", *Notre Dame Journal of Formal Logic*, 31, 1990, pg. 37-43.

[11] Sambin G., "An effective fixed point theorem in intuitionistic diagonalizable algebras", *Studia Logica*, 35, 1976, pg. 345-361.

[12] Sambin G. e Valentini S., "The Modal Logic of Provability. The sequential approach", *Journal of Philosophical Logic*, 11,1982, pg. 311-342.

[13] Smoryński C., *Self-Reference and Modal Logic*, Springer-Verlag, New Tork, 1985.