Introduzione alla teoria della dimostrazione I: i calcoli di Gentzen e l'Hauptsatz[1]

Andrea Cantini

Scuola Estiva AILA 2008
Gargnano, 1-6 Settembre 2008

[1]**Disclaimer**: le note che seguono costituiscono solo un hand-out preparato ad ausilio degli studenti; non sono fatte per essere diffuse e sono da correggere in tutti sensi !!. Si tratta solo di appunti di un corso breve, L'autore sarà comunque grato per ogni segnalazione di errori, commenti critici, etc.. . . .

Indice

Sommario

Il primo capitolo contiene una introduzione ai calcoli di Gentzen (versione G3p) per il solo frammento proposizionale. Si dimostra il teorema di eliminazione delle cesure (Hauptsatz) con stima sulle lunghezza per il caso classico. Viene quindi studiato il caso della logica intuizionista e se ne descrive una variante con la proprietà di terminazione.

Nel secondo capitolo si espone l'estensione predicativa di G3p. Si prova l'Hauptsatz con alcune importanti conseguenze (in particolare il teorema d'interpolazione).

Prerequisiti: definizione di linguaggio elementare con nozioni sintattiche connesse; semantica classica e nozione di conseguenza logica. Un calcolo logico completo (con i relativi teoremi di validità e completezza).

Capitolo 1

Calcoli di Gentzen proposizionali

1.1 Un calcolo logico enunciativo delle sequenze nello stile di Gentzen

Ci accingiamo ora a sviluppare nelle sue linee fondamentali l'approccio analitico alla logica sviluppato da Gerhard Gentzen nel 1934 con il suo calcolo delle sequenze. Descriveremo una versione del calcolo, dovuta a Kleene e nota come G3, che meglio si presta alla costruzione del cosiddetto albero canonico e a possibili applicazioni allo studio della deduzione automatica.

In tale versione le entità derivate sono particolari strutture di dati, dette *sequenze*, della forma $\Gamma \Rightarrow \Delta$; ogni sequenza consta di due parti − l'antecedente Γ e il conseguente Δ − separate da $\Rightarrow$, in cui Γ, Δ sono *multinsiemi finiti*, anche vuoti, di formule nel linguaggio oggetto.

Quando una delle due parti di una sequenza è vuota, conveniamo di ometterla. Dunque anche le configurazioni formali

$$\Gamma \Rightarrow\ ; \quad \Rightarrow \Delta; \quad \Rightarrow$$

sono sequenze e come tali possibili oggetti derivabili nel calcolo. $\Rightarrow$ è detta *sequenza vuota*.

In quel che segue useremo S, possibilmente con indici, come metavariabile per sequenze.
Ricordiamo che *un multinsieme è* un insieme in cui ogni elemento possiede una molteplicità m (m intero positivo).

La molteplicità m di un elemento A di un multinsieme Γ di formule indica il *numero di occorrenze* di A in Γ. *Dunque due multinsiemi sono uguali sse hanno gli stessi elementi con le medesime molteplicità.*

Per esempio, si consideri $\{A^2, B^1, C^3\}$; esso può più perspicuamente essere rappresentato dalla collezione $\{A, A, B, C, C, C\}$; esso non differisce in quanto multinsieme da $\{C^3, B^1, A^2\}$ (dato che l'ordine non conta), ma differisce dal multinsieme $\{A^2, B, C^2\}$, che più perspicuamente è rappresentato dalla collezione $\{A, A, B, C, C\}$.

Definizione 1.1.1. G3p comprende il gruppo ID delle sequenze iniziali (assiomi) e regole per gli operatori logici. Γ, Δ, Λ (anche con indici o apici) designano multinsiemi (finiti, anche vuoti) di formule.

ID**-regola:** se p è un atomo qualsiasi,

$$\Gamma, p \Rightarrow \Delta, p;$$

$\bot/\top$**–regole:**

$$\Gamma, \bot \Rightarrow \Delta; \qquad \Gamma \Rightarrow \Delta, \top;$$

$\rightarrow$**-regole:**

$$\frac{\Gamma, A \Rightarrow B, \Delta}{\Gamma \Rightarrow A \rightarrow B, \Delta}[\Rightarrow\rightarrow]; \qquad \frac{\Gamma \Rightarrow \Delta, A \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \rightarrow B \Rightarrow \Delta}[\rightarrow\Rightarrow];$$

$\neg$**-regole:**

$$\frac{\Gamma \Rightarrow \Delta, A}{\Gamma, \neg A \Rightarrow \Delta}[\neg\Rightarrow]; \qquad \frac{\Gamma, A \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg A}[\Rightarrow\neg];$$

$\vee$**-regole:**

$$\frac{\Gamma \Rightarrow \Delta, A_1, A_2}{\Gamma \Rightarrow A_1 \vee A_2, \Delta}[\Rightarrow\vee]; \qquad \frac{\Gamma, A \Rightarrow \Delta \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \vee B \Rightarrow \Delta}[\vee\Rightarrow];$$

$\wedge$**-regole:**

$$\frac{\Gamma \Rightarrow \Delta, A \qquad \Gamma \Rightarrow \Delta, B}{\Gamma \Rightarrow \Delta, A \wedge B}[\Rightarrow\wedge]; \qquad \frac{\Gamma, A_1, A_2 \Rightarrow \Delta}{\Gamma, A_1 \wedge A_2 \Rightarrow \Delta}[\wedge\Rightarrow];$$

G3p+cut è G3p esteso con la regola Cut (cesura, in versione *context-sharing*):

$$\frac{\Gamma \Rightarrow \Delta, A \qquad A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}[\text{cut}]$$

Osservazione 1.1.2. Le regole hanno *una valenza semantica*: possono essere riguardate come regole d'uso delle costanti logiche che spiegano come introdurre una costante logica nelle premesse, risp. nelle conclusioni.

L'idea di verità sottostante è quella di costruibilità diretta mediante regole.

Dualmente, le regole possono essere considerate come *regole di refutazione*: esse rispondono cioè alla domanda: come si opera se si assume la falsità delle formule dell'antecedente e la falsità delle formule nel conseguente? La risposta è data dalle premesse delle regole di G3. In altri termini: G3 fornisce una possibile alternativa al formalismo degli alberi di Beth.

Concettualmente, *le regole di Gentzen sono naturalmente complete* nel senso che – sfruttando la simmetria sinistra/destra – abbracciano tutte le possibili situazioni argomentative che si possono presentare se si assume un approccio di tipo analitico. valida.

1.1.1 Esempi di derivazioni

Senza definire esplicitamente il concetto di derivazione, vediamone ora alcuni esempi significativi.

- *Terzo escluso*:

$$\dfrac{\dfrac{p \;\Rightarrow\; p}{\Rightarrow\; p, \neg p}\,[\Rightarrow\neg]}{\Rightarrow\; p \vee \neg p}\,[\Rightarrow\vee] \;;$$

- *Principio di non-contraddizione*:

$$\dfrac{\dfrac{\dfrac{p \;\Rightarrow\; p}{p, \neg p \Rightarrow}\,[\neg\Rightarrow]}{p \wedge \neg p \Rightarrow}\,[\wedge\Rightarrow]}{\Rightarrow\; \neg(p \wedge \neg p)}\,[\Rightarrow\neg] \;;$$

- *Consequentia mirabilis*:

$$\dfrac{\dfrac{\dfrac{p \;\Rightarrow\; p}{\Rightarrow\; p, \neg p}\,[\Rightarrow\neg] \qquad p \;\Rightarrow\; p}{\neg p \to p \Rightarrow p}\,[\to\Rightarrow]}{\Rightarrow\; (\neg p \to p) \to p}\,[\Rightarrow\to] \;;$$

- *Distributività* ("metà non-banale")

$$\dfrac{\dfrac{\dfrac{\dfrac{p\,, q \Rightarrow\; p, p \wedge r \qquad p,\, q \Rightarrow\; q, p \wedge r}{p, q \Rightarrow p \wedge q, p \wedge r} \qquad \dfrac{p,\, r \Rightarrow\; p, p \wedge q \qquad p,\, r \Rightarrow\; r, p \wedge q}{p, r \Rightarrow p \wedge q, p \wedge r}}{p, q \vee r \Rightarrow p \wedge q, p \wedge r}}{p \wedge (q \vee r) \Rightarrow p \wedge q, p \wedge r}}{p \wedge (q \vee r) \Rightarrow (p \wedge q) \vee (p \wedge r)}$$

  [Il lettore indichi le inferenze lasciate implicite.]

- *Legge di Dummett*

$$\dfrac{\dfrac{\dfrac{p\,, q \Rightarrow\; p, q}{q \Rightarrow p \to q, p}\,[\Rightarrow\to]}{\Rightarrow p \to q, q \to p}\,[\Rightarrow\to]}{\Rightarrow\; (p \to q) \vee (q \to p)}\,[\Rightarrow\vee]$$

Riflettendo sugli esempi precedenti, possiamo concludere che una derivazione $\mathcal{D}$ è un insieme di sequenze di formule, strutturato ad *albero*[1], che soddisfa le condizioni seguenti;

1. ciascuna occorrenza di una sequenza di formule in $\mathcal{D}$ individua una posizione, che viene detta *nodo*;

[1] Qui si assume come dato intuitivamente il concetto di albero, allo stesso modo in cui si accetta agli inizi dell'apprendimento della geometria elementare che il discente afferri la nozione di triangolo, cerchio. . . . In ogni caso una trattazione più astratta seguirà nella sezione **??**.

2. alcune sequenze di $\mathcal{D}$ sono *nodi terminali*, nel senso che non hanno *sopra* altre sequenze; in tal caso le sequenze sono istanze della regola ID;

3. esiste sempre in $\mathcal{D}$ una *sequenza finale* o *conclusione*, detta anche *radice*, che non ha *sotto* altre sequenze;

4. se una sequenza individua un nodo *non terminale*, allora deve essere connessa ai (al) nodi (nodo) immediatamente superiori(e) mediante una regola d'inferenza di G3p;

5. per ogni nodo terminale di $\mathcal{D}$, esiste esattamente una successione finita di nodi che lo connette alla conclusione (radice) di $\mathcal{D}$; tale cammino viene detto *ramo* (talvolta anche cammino) della derivazione $\mathcal{D}$, e ogni ramo è caratterizzato da una lunghezza, ovvero dal numero di nodi che lo costituiscono.

Le condizioni 2 e 4 corrispondono alla cosiddetta *correttezza locale* della derivazione, ovvero al fatto che una derivazione codifica un argomento deduttivo corretto, cioè generato secondo le regole d'inferenza del calcolo logico.
Se ogni ramo di una derivazione $\mathcal{D}$ ha lunghezza $\leq m$ e m è il più piccolo numero con tale proprietà, m è detta *profondità* di $\mathcal{D}$.

Esempio 1.1.3. Vediamo ora di illustrare la terminologia con qualche esempio specifico. Nella derivazione della distributività vi sono quattro nodi terminali, ovvero

- $p\,, q \Rightarrow\ p, p \wedge r$;
- $p,\ q \Rightarrow\ q, p \wedge r$;
- $p,\ r \Rightarrow\ p, p \wedge q$;
- $p,\ r \Rightarrow\ r, p \wedge q$.

Nella derivazione della *consequentia mirabilis* il nodo determinato da $\neg p \rightarrow p\ \Rightarrow\ p$ non è terminale, ma si ricava dai suoi predeccessori immediati, che sono i nodi $\Rightarrow\ p, \neg p$ e $p\ \Rightarrow\ p$ mediante l'inferenza di introduzione a sinistra dell'implicazione. Sempre nella derivazione della *consequentia mirabilis* ci sono due rami, rispettivamente:

1. $p\ \Rightarrow\ p$; $\Rightarrow\ p, \neg p$; $\neg p \rightarrow p \Rightarrow p$; $\Rightarrow (\neg p \rightarrow p) \rightarrow p$;
2. $p\ \Rightarrow\ p$; $\neg p \rightarrow p \Rightarrow p$; $\Rightarrow (\neg p \rightarrow p) \rightarrow p$.

Chiaramente i due rami hanno lunghezza rispettivamente 4 e 3.
Per esercizio si descrivano tutti i possibili rami della derivazione della distributività con le rispettive lunghezza.

Possiamo dunque sintetizzare le considerazioni precedenti nella

Definizione 1.1.4. Se S è uno dei due sistemi di regole G3p o G3p+Cut, una derivazione in S è un albero finitario localmente corretto rispetto alle regole di S.

1.1.2 Inferenze strutturali e loro ammissibilità

Accanto alle regole ufficiali del calcolo, che coinvolgono le operazioni logiche (con l'eccezione della cesura e di ID), vi sono altre inferenze che si lasciano validare dalla semantica classica.

Regole di scambio, di indebolimento e di contrazione

***Scambio*:**

$$\frac{A, B, \Gamma \Rightarrow \Delta}{B, A, \Gamma \Rightarrow \Delta}\,[C{\Rightarrow}]; \qquad \frac{\Gamma \Rightarrow \Delta, B, A}{\Gamma \Rightarrow \Delta, A, B}\,[{\Rightarrow}C];$$

***Indebolimento*:**

$$\frac{\Gamma \Rightarrow \Delta}{A, \Gamma \Rightarrow \Delta}\,[K{\Rightarrow}]; \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, A}\,[{\Rightarrow}K];$$

***Contrazione*:**

$$\frac{A, A, \Gamma \Rightarrow \Delta}{A, \Gamma \Rightarrow \Delta}\,[W{\Rightarrow}]; \qquad \frac{\Gamma \Rightarrow \Delta, A, A}{\Gamma \Rightarrow \Delta, A}\,[{\Rightarrow}W].$$

Esercizio 1.1.5. In che senso le inferenze di scambio, indebolimento e contrazione possono essere considerate semanticamente accettabili? Proporre una nozione di correttezza per le inferenze del calcolo di Gentzen (c.f.r. più avanti).

Osservazione 1.1.6. Le tre inferenze ammettono una lettura suggestiva dal punto di vista filosofico, lettura che evidenzia comunque il carattere idealizzato della logica classica. Così lo scambio ne implica il carattere atemporale (indipendenza dall'ordine delle ipotesi e delle conclusioni), mentre l'indebolimento asserisce implicitamente il carattere monotono e cumulativo dei giudizi logici: la validità di una sequenza non cambia se si aggiungono informazioni alle ipotesi o alla conclusione. La regola di contrazione esprime invece il fatto che la logica classica fa astrazione dalle risorse, ovvero da quante volte un enunciato occorre come ipotesi/come conclusione.

Osservazione 1.1.7. Il lettore probabilmente si chiederà perchè ostinarsi a lasciare fuori dal calcolo le regole strutturali. La ragione sta nel fatto che così è possibile definire un algoritmo di *proof search* che *termina sempre*.

Dal punto di vista inferenziale, è importante osservare allora che `G3p` è chiuso rispetto alle regole strutturali, in un senso forte: se si possiede una derivazione (con cesura o no) della premessa di una fra le inferenze strutturali $[C \Rightarrow]$, $[\Rightarrow C]$, $[K \Rightarrow]$,$[\Rightarrow K]$,$[W \Rightarrow]$, $[\Rightarrow W]$, è allora possibile trasformarla in una derivazione della conclusione, *senza alterarne la struttura arborea sottostante.*

Introduciamo una notazione utile a comunicare compattamente questa proprietà, ovvero l'essenza dell' ammissibilità delle regole.

Definizione 1.1.8.

1. *Complessità logica* o *rango* di una formula A. Per induzione su A, si pone:
   - $rk(A) = 0$ se A è atomica;

- $rk(\neg A) = rk(A) + 1$;
- $rk(A \circ B) = max(rk(A), rk(B)) + 1$ ($\circ$ connettivo binario).

2. *Relazione di derivabilità*:
$$\mathcal{D} \vdash_k^m \Gamma \Rightarrow \Delta$$
sse $\mathcal{D}$ è una derivazione di $\Gamma \Rightarrow \Delta$ tale che:
   - ogni ramo di $\mathcal{D}$ ha al massimo lunghezza m;
   - ogni formula che occorre come formula di cesura in $\mathcal{D}$ ha complessità logica minore di k

   $\vdash_k^m \Gamma \Rightarrow \Delta$ significa che esiste una derivazione $\mathcal{D}$ tale che $\mathcal{D} \vdash_k^m \Gamma \Rightarrow \Delta$;

3. Diciamo *ammissibile* una regola $\mathcal{R}$ con premesse $Pr_1, \ldots, Pr_k$
$$\frac{Pr_1 \ldots Pr_k}{C},$$
quando da $\vdash_k^m Pr_1, \ldots, \vdash_k^m Pr_k$ segue $\vdash_k^m C$.

Così, se $\vdash_1^3 \Gamma \Rightarrow \Delta$, la sequenza $\Gamma \Rightarrow \Delta$ è derivabile con un albero di profondità al massimo 3 e in cui la cesura si applica soltanto a formule di complessità logica minore di 1, vale a dire *formule atomiche*; se $\vdash_0^3 \Gamma \Rightarrow \Delta$, la sequenza data è comunque derivabile senza cesure e dunque in G3p.

Lemma 1.1.9. *Le regole* $[C\Rightarrow]$, $[\Rightarrow C]$, $[K\Rightarrow]$, $[\Rightarrow K]$ *sono ammissibili.*

Dimostrazione. Per l'ammissibilità di $[C\Rightarrow]$, $[\Rightarrow C]$, basta osservare che banalmente per i multinsiemi è irrilevante l'ordine.

Quanto a $[K\Rightarrow]$, $[\Rightarrow K]$, se si aggiunge ad ogni nodo di una data derivazione di $\Gamma \Rightarrow \Delta$, una nuova formula A o a destra o a sinistra, la correttezza locale è presevata (qui risulta essenziale la formulazione della regola ID). □

Lemma 1.1.10 (Eliminazione dei booleani)**.**

- $\vdash_k^m \Gamma, \top \Rightarrow \Delta$ *implica* $\vdash_k^m \Gamma \Rightarrow \Delta$*;*
- $\vdash_k^m \Gamma \Rightarrow \bot, \Delta$ *implica* $\vdash_k^m \Gamma \Rightarrow \Delta$*.*

Dimostrazione. $\top$ non è mai attiva a sinistra, così come $\bot$ non lo è mai a destra. Se si cancella ovunque $\top$ a sinistra ($\bot$ a destra) nella prova di $\vdash_k^m \Gamma, \top \Rightarrow \Delta$ ($\vdash_k^m \Gamma \Rightarrow \Delta, \bot$), si ottiene ancora una derivazione sullo stesso albero e con lo stesse cesure della medesima sequenza. □

Lemma 1.1.11. *Le regole d'inversione per le regole logiche sono ammissibili:*

1. $\vdash_k^m \Gamma, A \vee B \Rightarrow \Delta$ *implica* $\vdash_k^m \Gamma, A \Rightarrow \Delta$ *e* $\vdash_k^m \Gamma, A \Rightarrow \Delta$*;*
2. $\vdash_k^m \Gamma \Rightarrow \Delta, A \vee B$ *implica* $\vdash_k^m \Gamma \Rightarrow \Delta, A, B$*;*
3. $\vdash_k^m \Gamma, A \wedge B \Rightarrow \Delta$ *implica* $\vdash_k^m \Gamma, A, B \Rightarrow \Delta$*;*
4. $\vdash_k^m \Gamma \Rightarrow \Delta, A \wedge B$ *implica* $\vdash_k^m \Gamma \Rightarrow \Delta, A$ *e* $\vdash_k^m \Gamma \Rightarrow \Delta, B$*;*
5. $\vdash_k^m \Gamma, A \to B \Rightarrow \Delta$ *implica* $\vdash_k^m \Gamma, B \Rightarrow \Delta$ *e* $\vdash_k^m \Gamma \Rightarrow \Delta, A$*;*

6. $\vdash_k^m \Gamma \Rightarrow \Delta, A \to B$ *implica* $\vdash_k^m \Gamma, A \Rightarrow \Delta, B$;
7. $\vdash_k^m \Gamma \Rightarrow \Delta, \neg A$ *implica* $\vdash_k^m \Gamma, A \Rightarrow \Delta$;
8. $\vdash_k^m \Gamma, \neg A \Rightarrow \Delta$ *implica* $\vdash_k^m \Gamma \Rightarrow \Delta, A$
9. $\vdash_k^m \Gamma, A \leftrightarrow B \Rightarrow \Delta$ *implies* $\vdash_k^m \Gamma, A, B \Rightarrow \Delta$, $\vdash_k^m \Gamma \Rightarrow \Delta, A, B$
10. $\vdash_k^m \Gamma, \Rightarrow \Delta, A \leftrightarrow B$ *implies* $\vdash_k^m \Gamma, A \Rightarrow \Delta, B$, $\vdash_k^m B, \Gamma \Rightarrow \Delta, A$

Esercizio 1.1.12. Provare il lemma.

Lemma 1.1.13. *Le regole* [$W\Rightarrow$], [$\Rightarrow W$] *sono ammissibili.*

Dimostrazione. Si ragiona induttivamente. Se $\Gamma \Rightarrow \Delta, A, A$ è un' istanza di ID, lo è anche $\Gamma \Rightarrow \Delta, A$. Supponiamo che nell'ultima inferenza nessuna delle due occorrenze di A sia attiva. Allora, se si cancella una delle due occorrenze di A nelle premesse, la correttezza locale viene preservata e l'asserto segue per IH. Supponiamo invece che una delle due occorrenze di A sia attiva. Consideriamo solo il caso in cui A è l'implicazione $B \to C$. Dunque abbiamo:

$$\frac{B \to C, \Gamma \Rightarrow \Delta, B \qquad B \to C, \Gamma, C \Rightarrow \Delta}{B \to C, B \to C, \Gamma \Rightarrow \Delta}\,[\to\Rightarrow];$$

Dato che l'inversione dell'implicazione a sinistra è ammissibile, otteniamo per qualche $n < m$,

$$\vdash_k^n \Gamma \Rightarrow \Delta, B, B$$
$$\vdash_k^n C, C, \Gamma \Rightarrow \Delta$$

Dunque per IH:

$$\vdash_k^n \Gamma \Rightarrow \Delta, B$$
$$\vdash_k^n C, \Gamma \Rightarrow \Delta$$

da cui segue $\vdash_k^m B \to C, \Gamma \Rightarrow \Delta$. □

Concludiamo lasciando al lettore la prova del principio di identità per formule A di complessità qualsiasi:

Lemma 1.1.14 (Tautologia)**.** *Sia* $m = 2rk(A)$. *Allora:*

$$\vdash_0^m A \Rightarrow A.$$

1.2 Memo I: semantica per **G3p** e teoremi fondamentali

Definizione 1.2.1. Estendiamo ora la relazione di soddisfacibilità alle sequenze di formule dicendo che

(i) una valutazione v soddisfa la sequenza $\Gamma \Rightarrow \Delta$ sse o c'è almeno una formula $A \in \Gamma$ tale che $v(A) = 0$, oppure esiste una formula $B \in \Delta$ tale che $v(B) = 1$; scriviamo $v \models \Gamma \Rightarrow \Delta$ per designare la soddisfacibilità della sequenza rispetto alla valutazione v;

(ii) Sia Σ un insieme di formule.[2] $\Sigma \models \Gamma \Rightarrow \Delta$ sse ogni valutazione che soddisfa Σ soddisfa $\Gamma \Rightarrow \Delta$.

(iii) Se Σ è vuoto, si scrive al solito $\models \Gamma \Rightarrow \Delta$ e si dice $\Gamma \Rightarrow \Delta$ è valida.

Osservazione 1.2.2. Dalla prima clausola della definizione precedente, discende che, se $\Delta = \emptyset$, una valutazione v soddisfa $\Gamma \Rightarrow$ sse v soddisfa $\neg \bigwedge \Gamma$; dualmente, se $\Gamma = \emptyset$, v soddisfa $\Rightarrow \Delta$ iff v soddisfa $\bigvee \Delta$. Ovviamente $\Rightarrow$ non è soddisfatta da alcuna valutazione. Se sia Γ che Δ sono non vuoti, è chiaro che

$$\Sigma \models \Gamma \Rightarrow \Delta \text{ sse } \Sigma \models \bigwedge \Gamma \to \bigvee \Delta$$

Possiamo ora stabilire una importante caratteristica delle regole del calcolo delle sequenze con il seguente

Lemma 1.2.3 (Correttezza e invertibilità)**.**

(i) *In ogni regola del sistema* G3p + Cut*, se le premesse (o la premessa) sono (è) valide(a), allora anche la conclusione è valida.*

(ii) *In ogni regola di* G3p+Cut*, se la conclusione di una inferenza è valida, lo sono (lo è) anche le sue (la sua) premesse (premessa)*

I teoremi fondamentali

In primo luogo, estendiamo a insiemi qualsiasi le nozioni di contraddittorietà, consistenza e derivabilità.

Definizione 1.2.4.

1. Σ è refutabile sse esiste un suo sottinsieme finito Σ_0 tale che $\Sigma_0 \Rightarrow$ è derivabile in G3p (o equivalentemente in G3p + Cut)

2. Σ è consistente sse Σ non è refutabile;

3. $\Gamma \Rightarrow \Delta$ è derivabile da Σ, in simboli

$$\Sigma \vdash \Gamma \Rightarrow \Delta$$

   sse esiste un albero finito che ha per radice $\Gamma \Rightarrow \Delta$ ed è localmente corretto rispetto alle regole di G3p+Cut ed alla regola che permette di asserire la sequenza $\Gamma \Rightarrow A, \Delta$, per qualunque $A \in \Sigma$ (in altri termini, Σ funziona da insieme degli assiomi specifici della teoria e si può sempre iniziare un ramo di una derivazione con una sequenza di tal fatta).

Proposizione 1.2.5 (Correttezza Generale)**.** *Se* $\Sigma \vdash \Gamma \Rightarrow \Delta$*, allora*

$$\Sigma \models \Gamma \Rightarrow \Delta$$

Teorema 1.2.6 (Completezza speciale)**.** *Se* $\models \Gamma \Rightarrow \Delta$*, allora* $\Gamma \Rightarrow \Delta$ *è derivabile in* G3p*.*

Dimostrazione. Esercizio... □

[2] Si pensi a Σ come ad un insieme di assunzioni o assiomi

Corollario 1.2.7 (Eliminazione della Cesura)**.** *Se* $\Gamma \Rightarrow \Delta$ *è derivabile in* G3p+Cut*, allora* $\Gamma \Rightarrow \Delta$ *è derivabile in* G3p*, ovvero, con la notazione della definizione 1.1.8), esiste un* m *tale che*

$$\vdash_0^m \Gamma \Rightarrow \Delta$$

Dimostrazione. Per la correttezza la sequenza è valida e dunque per il teorema di completezza, è derivabile senza cesura. □

Corollario 1.2.8. A *è una tautologia sse* $\Rightarrow A$ *è derivabile in* G3p*.*

Si può allora definire facilmente un algoritmo di decisione per vedere se $\Gamma \Rightarrow \Delta$ è derivabile in G3: basta cercare una derivazione cut-free, costruendo un albero di ricerca con radice $\Gamma \Rightarrow \Delta$: dato che le regole sono invertibili e andando all'indietro si abbassa la complessità logica, ogni ramo finisce e dunque l'albero di ricerca è finito.

Osservazione 1.2.9. Applicando sempre la ricerca all'indietro del teorema di completezza, provare il teorema di esistenza della forma normale congiuntiva CNF

Teorema 1.2.10. $\Sigma \models \Gamma \Rightarrow \Delta$ *sse esiste un sottinsieme finito* Σ_0 *tale che è derivabile in* G3p *la sequenza* $\Sigma_0, \Gamma \Rightarrow \Delta$ *sse* $\Sigma \vdash \Gamma \Rightarrow \Delta$

Dimostrazione. Quanto alla prima equivalenza, si applicano nell'ordine la correttezza, il teorema di compattezza e la completezza speciale. Quanto alla seconda, basta osservare che essa, da sinistra a destra, segue applicando ripetutamente la cesura (e le regole strutturali). □

Corollario 1.2.11. $\Sigma \models A$ *sse esiste un sottinsieme finito* Σ_0 *tale che è derivabile in* G3p *la sequenza* $\Sigma_0 \Rightarrow A$ *sse* $\Sigma \vdash \Rightarrow A$

In particolare dal corollario discende che le conseguenze logiche di Σ sono tutte e sole quelle derivabili da Σ mediante G3p.

Corollario 1.2.12. Σ *è insoddisfacibile sse* Σ *è refutabile.*

Corollario 1.2.13. Σ *è soddisfacibile sse* Σ *è consistente.*

1.3 Prova costruttiva dell'Hauptsatz: il caso classico

La prova dell'Hauptsatz discende in ultima analisi dalla compattezza dello spazio di Cantor (che vale in un universo matematico solo se abitano in esso operazioni non ricorsive). Dunque la prova è non costruttiva. Vediamo ora che la proprietà semantica dell'invertibilità dà luogo a una prova interamente costruttiva (ma pur essenzialmente complessa computazionalmente).

Lemma 1.3.1. *Si può definire un'operazione* EL_0 *t. c. , se* S *è atomica e*

(i) $\mathcal{D}_0 \vdash_0^l \Gamma \Rightarrow \Delta, A$*;*

(ii) $\mathcal{D}_1 \vdash_0^0 \Gamma, A \Rightarrow \Delta$, *allora* $EL_0(\mathcal{D}_0, \mathcal{D}_1) \vdash_0^l \Gamma \Rightarrow \Delta$.

Dimostrazione. Per esercizio (applicare contrazione...) □

Lemma 1.3.2. *Si può definire un'operazione* EL_1 *t. c. , se* S *è atomica e*

(i) $\mathcal{D}_0 \vdash_0^l \Gamma \Rightarrow \Delta, A$*;*

(ii) $\mathcal{D}_1 \vdash_0^l \Gamma, A \Rightarrow \Delta$,

allora $EL_1(\mathcal{D}_0, \mathcal{D}_1) \vdash_0^{2\cdot l} \Gamma \Rightarrow \Delta$.

Dimostrazione. Idea: dato che A è atomica, A occorre a sinistra in ogni assioma di $\mathcal{D}_1$. L'operatore EL_1 sposta la cesura su A agli assiomi di $\mathcal{D}_1$ e applica EL_0. In questo modo certi rami raddoppiano... □

Definizione 1.3.3. Il concetto di *taglia* di una formula è induttivamente definito:

1. $sz(A) = 0$, se A è $\bot$ oppure $\top$;
2. $sz(A) = 1$, se A è atomica;
3. $sz(A \circ B) = sz(A) + sz(B) + 1$, dove $\circ$ è un connettivo binario;
4. $sz(\neg A) = sz(A) + 1$;

Se $\mathcal{D}$ è una derivazione e f un ramo di $\mathcal{D}$, *il numero critico del ramo* f è

$\sum\{sz(A) \mid A$ formula di cesura che occorre in una sequenza che riveste un nodo di $f\}$

Infine dicesi *numero critico di* $\mathcal{D}$ il numero

$$kr(\mathcal{D}) = \max\{kr(f) \mid f \text{ ramo di } \mathcal{D}\}$$

Si costruisce allora una operazione che abbassa il numero critico di una derivazione, raddoppiando al più la lunghezza della derivazione:

Lemma 1.3.4 (Riduzione proposizionale)**.** *Si può definire un'operazione* Red_π *tale che, se* $\mathcal{D}$ *è una derivazione di* $\Gamma \Rightarrow \Delta$ *di lunghezzza* $l > 0$*, allora* $Red_\pi\mathcal{D}$ *è ancora una derivazione di* $\Gamma \Rightarrow \Delta$ *avente lunghezza* $\leq 2 \cdot l$ *e t.c.*

$$kr(Red_\pi\mathcal{D}) < kr(\mathcal{D})$$

Dimostrazione. (Idea) Si definisce Red_π per induzione su $l > 0$. Si considera l'ultima inferenza $\mathcal{I}$. Il caso in cui $\mathcal{I}$ non è una cesura in posizione massimale si tratta applicando l'ipotesi d'induzione alla(e) sottoderivazione(i) immediata(e) e verificando che viene rispettata la condizione sul numero critico. Se invece $\mathcal{I}$ è una cesura in posizione massimale, l'operatore di riduzione viene definito applicando l'operatore d'inversione. □

Teorema 1.3.5. *Se* $\mathcal{D}_0 \vdash_k^m \Gamma \Rightarrow \Delta$*, si può costruire una derivazione* $CF(\mathcal{D})$ *t.c.*

$$CF(\mathcal{D}) \vdash_0^l \Gamma \Rightarrow \Delta,$$

dove $l \leq 2^{2^{k\cdot m}} \cdot m$

Dimostrazione. Iterando $p = kr(\mathcal{D})$-volte l'operatore di riduzione, si ottiene una derivazione cut-free di $\Gamma \Rightarrow \Delta$ di lunghezza $2^p \cdot m$. Ma con una facile induzione sulla complessità logica di A si ottiene

$$sz(A) \leq 2^{rk(A)+1} - 1.$$

Dato che $rk(A) + 1 \leq k$ per ogni formula di cesura A, vale per ogni ramo f, dato che in f ci sono meno di m formule di cesura,

$$kr(f) = \sum\{sz(A) \mid A \in f\} < 2^k \cdot m.$$

Dunque $p \leq 2^k \cdot m$ e $l \leq 2^{2^{k \cdot m}}$. □

1.4 Il caso intuizionista

Il calcolo intuizionista G3ip si ottiene considerando solo sequenze della forma $\Gamma \Rightarrow \Delta$ in cui Δ contiene al più una sola formula. A differenza del caso classico, *bisogna però modificare la regola dell'implicazione a sinistra*; altrimenti non si riesce a provare la contrazione a sinistra. Si pone allora:

$$\frac{\Gamma\,, A \to B \Rightarrow\ A \qquad \Gamma,\, B \Rightarrow\ C}{\Gamma,\ A \to B\ \Rightarrow\ C}\ [\to\Rightarrow]$$

La conseguenza è che la regola è invertibile solo parzialmente:

(*) $\vdash_k^m \Gamma, A \to B \Rightarrow \Delta$ implica $\vdash_k^m \Gamma, B \Rightarrow \Delta$;

Inoltre si omette la negazione $\neg$ definita mediante

$$\neg A := A \to \bot$$

Si può verificare che il calcolo ammette ancora eliminazione delle cesure con stima di lunghezza:

Teorema 1.4.1. *Se $\vdash_k^m \Gamma \Rightarrow A$ in G3ip allora*

$$\vdash_0^l \Gamma \Rightarrow A$$

per qualche l t.c. $l \leq 2^{2^{k \cdot m}} \cdot m$ (m lunghezza, k dipende dalla complessità delle formule di cesura).

Conseguenze

Definizione 1.4.2. Formule di Harrop è FH:

- ogni atomo è FH;
- se A e B sono FH, anche $A \wedge B$ lo è;
- se B è FH, $A \to B$ è FH.

Un utile esercizion di analisi delle prove cut-free ci fornisce una basilare proprietà della logica intuizionistica:

Teorema 1.4.3. *Se G3ip prova* $\Gamma \Rightarrow A \vee \mathcal{F}$ *e* Γ *contiene solo formule di Harrop, allora G3ip o prova* $\Gamma \Rightarrow A$ *oppure* $\Gamma \Rightarrow B$.

In particolare la logica intuizionistica è prima.

In realtà, introducendo concetti appropriati di occorrenza positiva e negativa, è possibile dimostrare un rafforzamento della proprietà della sottoformula:

Teorema 1.4.4 (Separazione, Wajsberg 1938)**.**

1. *Sia* $\mathcal{D} \vdash \Gamma \Rightarrow A$ *e sia* $\mathcal{D}$ *cut-free. Allora se* $\Delta \Rightarrow B$ *occorre in* $\mathcal{D}$*, vale che:*
   - **(i)** *le formule di* Δ *occorrono positivamente in* Γ *o negativamente in* A*;*
   - **(ii)** B *è positiva in* A *o negativa in* Γ*;*
   - **(iii)** *se* B *occorre solo positivamente (negativamente) in* $\Gamma \Rightarrow A$*, allora* B *è introdotta in* $\mathcal{D}$ *da una regola d'introduzione a destra (sinistra);*
2. *ogni sequenza derivabile in G3ip ha una derivazione che usa solo regole e assiomi per gli operatori che occorrono nella sequenza.*

1.4.1 Un calcolo con la proprietà di terminazione

In virtù dell'Hauptsatz, il problema della decisione può essere affrontato cercando sistematicamente le possibili prove cut-free. Ma G3ip non ha la proprietà della terminazione: la difficoltà è che la nuova regola per l'implicazione a sinistra non diminuisce strettamente la complessità logica, ma ripete la formula principale. Da ciò segue che qualche ramo nell'albero di ricerca può non terminare:

$$\dfrac{\dfrac{\overbrace{p \to p \Rightarrow p}^{\vdots} \qquad p \Rightarrow p}{p \to p \Rightarrow p} \qquad p \Rightarrow p}{p \to p \Rightarrow p}$$

Una soluzione è stata data in tempi relativamente recenti da Hudelmeier 1992, Dyckhoff 1992 [3]. Il punto tecnicamente rilevante consiste nel disegnare un calcolo alla Gentzen in cui le regole dell'implicazione a sinistra vengono spezzate in 4 sottocasi.

Definizione 1.4.5. G4ip si ottiene da G3ip sostituendo la regola di introduzione a sinistra per l'implicazione con le regole seguenti:

(Lat$\to$) if p is atomic,

$$\dfrac{p, B, \Gamma \Rightarrow A}{p \to B\ p, \Gamma \to A}$$

(Land$\to$)

$$\dfrac{A \to (B \to C), \Gamma \Rightarrow D}{(A \wedge B) \to C, \Gamma \to D}$$

[3] Pare che si tratti, almeno in parte, di una riscoperta di una vecchia idea di Vorob'ev, A new algorithm for derivability in the constructive propositional calculus, in: Sixteen Papers on Logic and Algebra V. A. Baranskii, I. H. Bekker, G. S. Ceitin et alii. Vorob'ev, morto nel 1995, allievo di Markov, è noto per i suoi contributi alla teoria dei giochi e autore di un classico testo sui numeri di Fibonacci.

(Lor→)

$$\frac{A \to C,\, B \to C,\, \Gamma \;\Rightarrow\; D}{(A \vee B) \to C,\, \Gamma \;\to\; D}$$

(Limp→)

$$\frac{\Gamma\,, B \to C \Rightarrow\; A \to B \qquad \Gamma,\, C \Rightarrow\; D}{\Gamma,\, (A \to B) \to C \;\Rightarrow\; D}$$

Nel nuovo sistema sono invertibili le prime tre regole dell'implicazione a sinistra), oltre a congiunzione e disgiunzione a sinistra e implicazione a destra.

Teorema 1.4.6. *Se $\mathcal{D}_0 \vdash_k^m\; \Gamma \Rightarrow A$ in G4ip, si può costruire una derivazione $J(\mathcal{D})$ di G4ip t.c.*

$$J(\mathcal{D}) \vdash_0^l\; \Gamma \Rightarrow A,$$

dove $l \leq 2^{(2^{2^{2^k}} \cdot m)} \cdot m$

Al fine di definire un algoritmo di decisione, si può associare poi alle formule una nuova misura, detta *peso*.

Definizione 1.4.7.

(1) $w(p) = w(\bot) = w(\top) = 2$;

(2) $w(A \wedge B) = w(A)(1 + w(B))$;

(3) $w(A \vee B) = w(A) + w(B) + 1$;

(4) $w(A) \cdot w(B) + 1$.

Il peso di una sequenza è definito da:

$$w(\Gamma \Rightarrow A) = \sum \{w(B) \mid B \text{ occorre in } \Gamma\}$$

NB: il peso di una formula A è connesso con la consueta complessità logica $g(A)$ dalla relazione:

$$w(A) \leq 2^{(2^{2^{g(A)}})}$$

Lemma 1.4.8. *In ogni inferenza di G4ip il peso della conclusione è maggiore del peso della(e) premessa(e).*

Si può quindi dimostrare che ogni possibile ramo di una derivazione di $\Gamma \Rightarrow A$ ha lunghezza $\leq$ del peso di $\Gamma \Rightarrow A$ e questo permette di decidere la derivabilità. Segue anzi che il problema della decisione per il caso intuizionista è in $O(n \log n)$-space.

Naturalmente vale, ma la prova non è banale, il seguente:

Lemma 1.4.9. $\Gamma \Rightarrow A$ *è derivabile in G3ip sse* $\Gamma \Rightarrow A$ *è derivabile in G4ip.*

Osservazione 1.4.10. Il calcolo G4ip è stato usato da Pitts(1992) per provare che il calcolo intuionista ammette interpolane minimale e massimale.

Problema 1. È possibile costruire una estensione di G3 che corrisponde a S4 e provare con la tecnica dell'inversione l'Hauptsatz. Rimane da vedere se esiste un calcolo alla Hudelmeier oer S4.

Capitolo 2

Calcoli di Gentzen predicativi

2.1 Un calcolo elementare alla Gentzen

Il calcolo delle sequenze G3p che abbiamo introdotto a livello proposizionale può essere agevolmente esteso al linguaggio elementare.

Adotteremo le stesse convenzioni notazionali della sezione 1.1 per quel che concerne multinsiemi, sequenze di formule, etc.

In aggiunta, *conveniamo di tenere distinte le variabili vincolate e le variabili libere* o *parametri*), continuando a usare le ultime lettere dell'alfabeto x, y, z, ... per le prime, e a, b, c, per le seconde (sappiamo che ciò non è restrittivo: perché ?).

Definizione 2.1.1. G3 comprende le regole di G3p estese al linguaggio elementare e in più le inferenze per i quantificatori:

∃-regole:

$$\frac{\Gamma,\, A[x := a] \Rightarrow \Delta}{\Gamma,\, \exists x A \Rightarrow \Delta}\,[\exists\Rightarrow]; \qquad \frac{\Gamma \Rightarrow \Delta, A[x := t], \exists x A}{\Gamma \Rightarrow \Delta, \exists x A}\,[\Rightarrow\exists];$$

Restrizione per $L\exists$: $a \notin FV(\Gamma, \Delta)$;

∀-regole:

$$\frac{\Gamma,\, A[x := t], \forall x A \Rightarrow \Delta}{\Gamma,\, \forall x A \Rightarrow \Delta}\,[\forall\Rightarrow]; \qquad \frac{\Gamma \Rightarrow \Delta, A[x := a]}{\Gamma \Rightarrow \Delta, \forall x A}\,[\Rightarrow\forall].$$

Restrizione per $R\forall$: $a \notin FV(\Gamma, \Delta)$; a è detto *parametro proprio* dell'inferenza.

G3+Cut è G3 esteso con la regola Cut (cesura, in versione *context-sharing*).

Esercizio 2.1.2. Costruire derivazioni in G3 di leggi logiche significative sui quantificatori (rapporti fra quantificatori e connettivi, leggi di Hilbert, legge dei domini costanti. . . .

2.1.1 Esempi di derivazioni

- *Universale* $\rightsquigarrow$ *Esistenziale*:

$$\dfrac{\dfrac{P(a), \forall x P(x) \Rightarrow P(a), \exists x P(x)}{P(a), \forall x P(x) \Rightarrow \exists x P(x)}\,[\Rightarrow\exists]}{\forall x P(x) \Rightarrow \exists x P(x)}\,[\forall\Rightarrow]$$

- $\exists\forall \rightsquigarrow \forall\exists$:

$$\dfrac{\dfrac{\dfrac{\dfrac{C(a,b), \forall x C(a,x) \Rightarrow C(a,b), \exists y C(y,b))}{\forall x C(a,x) \Rightarrow \exists y C(y,b), C(a,b)}\,[\forall\Rightarrow]}{\forall x C(a,x) \Rightarrow \exists y C(y,b)}\,[\Rightarrow\exists]}{\forall x C(a,x) \Rightarrow \forall x \exists y C(y,x)}\,[\Rightarrow\forall])}{\exists y \forall x C(y,x) \Rightarrow \forall x \exists y C(y,x)}\,[\exists\Rightarrow]$$

- *Principio del* τ *di Hilbert*:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(a),\ P(b) \Rightarrow P(a), \forall y P(y)}{P(b) \Rightarrow P(a), P(a) \to \forall y P(y)}\,[\Rightarrow\to]}{P(b) \Rightarrow P(a), \exists x(P(x) \to \forall y P(y))}\,[\Rightarrow\exists]}{P(b) \Rightarrow \forall x P(x), \exists x(P(x) \to \forall y P(y))}\,[\Rightarrow\forall]}{\Rightarrow P(b) \to \forall y P(y), \exists x(P(x) \to \forall y P(y))}\,[\Rightarrow\to]}{\Rightarrow \exists x(P(x) \to \forall y P(y))}\,[\Rightarrow\exists]$$

- *Terzo escluso per i quantificatori*:

$$\dfrac{\dfrac{\dfrac{\dfrac{P(a) \Rightarrow P(a), \exists y \neg P(y)}{\Rightarrow P(a), \neg P(a), \exists y \neg P(y)}\,[\Rightarrow\neg]}{\Rightarrow P(a),\ \exists y \neg P(y)}\,[\Rightarrow\exists]}{\Rightarrow \forall x P(x),\ \exists y \neg P(y)}\,[\Rightarrow\forall]}{\Rightarrow \forall x P(x) \vee \exists y \neg P(y)}\,[\Rightarrow\vee]$$

La legge dei domini costanti: sia $\forall\vee \rightsquigarrow \vee\forall$, $x \notin FV(P)$; usando le abbreviazioni

1. $\Delta_1 := \forall x(P \vee Q(x)), Q(a), Q(b)$;
2. $\Delta_2 := \forall x(P \vee Q(x)), P, Q(a)$

$$\dfrac{\dfrac{\dfrac{\forall x(P \vee Q(x)), P \Rightarrow P, Q(b) \qquad \dfrac{\dfrac{\Delta_1 \Rightarrow P, Q(b) \qquad \Delta_2 \Rightarrow P, Q(b)}{P \vee Q(b), \forall x(P \vee Q(x)),\ Q(a) \Rightarrow P, Q(b)}}{\forall x(P \vee Q(x)), Q(a) \Rightarrow P,\ Q(b)}}{\dfrac{P \vee Q(a), \forall x(P \vee Q(x)) \Rightarrow P, Q(b)}{P \vee Q(a), \forall x(P \vee Q(x)) \Rightarrow P,\ \forall x Q(x)}}}{P \vee Q(a), \forall x(P \vee Q(x)) \Rightarrow P \vee \forall x Q(x)}}{\forall x(P \vee Q(x)) \Rightarrow P \vee \forall x Q(x)}$$

2.2 Memo II: semantica predicativa e teoremi fondamentali

Si assumono come noti i fondamenti della semantica di Tarski per linguaggi elementari (strutture o realizzazioni $\mathcal{M}$ di un dato linguaggio, interpretazionσ delle variabili; nozione di valutazione $\mathcal{M}^\sigma$ di un termine e di una formula; relazione fondamentale $\mathcal{M}^\sigma \models A \ldots$).

Definizione 2.2.1. Estendiamo ora la relazione di soddisfacibilità alle sequenze di formule dicendo che

(i) una valutazione $\mathcal{M}^\sigma$ soddisfa la sequenza $\Gamma \Rightarrow \Delta$ sse o $\mathcal{M}^\sigma$ non soddisfa almeno una formula $A \in \Gamma$, oppure $\mathcal{M}^\sigma$ soddisfa almeno una formula $B \in \Delta$;

(ii) $\Sigma \models \Gamma \Rightarrow \Delta$ sse ogni valutazione $\mathcal{M}^\sigma$ che soddisfa Σ soddisfa $\Gamma \Rightarrow \Delta$.

(iii) Se Σ è vuoto, si scrive al solito $\models \Gamma \Rightarrow \Delta$ e si dice $\Gamma \Rightarrow \Delta$ è valida.

Possiamo estendere al caso elementare le nozioni di contraddittorietà, consistenza e derivabilità per insiemi qualsiasi.

Definizione 2.2.2.

1. Σ è refutabile sse esiste un suo sottinsieme finito Σ_0 tale che $\Sigma_0 \Rightarrow$ è derivabile in $\mathsf{G3}$ (o equivalentemente in $\mathsf{G3} + \mathsf{Cut}$)

2. Σ è consistente sse Σ non è refutabile;

3. $\Gamma \Rightarrow \Delta$ è derivabile da Σ, in simboli

$$\Sigma \vdash \Gamma \Rightarrow \Delta$$

   sse esiste un albero finito che ha per radice $\Gamma \Rightarrow \Delta$ ed è localmente corretto rispetto alle regole di $\mathsf{G3}+\mathsf{Cut}$ ed alla regola che permette di asserire la sequenza $\Gamma \Rightarrow A, \Delta$, per qualunque $A \in \Sigma$ (in altri termini, Σ funziona da insieme degli assiomi specifici della teoria e si può sempre iniziare un ramo di una derivazione con una sequenza di tal fatta).

Anche per $\mathsf{G3}$ si può verificare, mediante applicazione dei lemmi di coincidenza e conversione [1]:

Lemma 2.2.3 (Correttezza e invertibilità)**.**

(i) *In ogni regola del sistema $\mathsf{G3} + \mathsf{Cut}$, se le premesse (o la premessa) sono (è) valide(a), allora anche la conclusione è valida.*

(ii) *In ogni regola di $\mathsf{G3}$, se la conclusione di una inferenza è valida, lo sono (lo è) anche le sue (la sua) premesse (premessa)*

La correttezza del calcolo elementare continua a sussistere in virtù del corrispondente lemma:

[1] Accertarsi della necessità delle restrizioni su $L\forall$ $R\exists$!

Proposizione 2.2.4. *Se* Σ *è un insieme di enunciati e* $\Sigma \vdash \Gamma \Rightarrow \Delta$*, allora*

$$\Sigma \models \Gamma \Rightarrow \Delta$$

Osservazione 2.2.5.

1. L'ipotesi su Σ è necessaria (se Σ è costituito dalla formula $P(x)$, $\forall x P(x)$ è derivabile da Σ).

2. Il lemma di correttezza e invertibilità, anche se ci dice che il calcolo è in un senso preciso analitico, non deve però mascherare una differenza profonda col caso enunciativo. Il lettore avrà di certo osservato il carattere peculiare delle due inferenze d'introduzione dell'universale a sinistra e dell'esistenziale a destra: in entrambe la formula attiva dell'inferenza occorre già nella premessa e quindi procedendo all'indietro nella ricerca di una derivazione *non si diminuisce la complessità logica in gioco*. Ma ciò, come si è visto nel caso enunciativo, è essenziale per la terminazione dell'algoritmo di ricerca delle dimostrazioni. Come vedremo, la formulazione attuale delle inferenze quantificazionali è necessaria per la completezza del calcolo ed è al contempo responsabile della complessità (teorema di indecidibilità della logica elementare, Church 1936).

Osservazione 2.2.6. La semantica classica valida la cesura, ed non distingue dunque prove con cesura da quelle cut-free, per le quali, seguendo una idea di Schütte, è sufficiente utilizzare *valutazioni parziali* che possono assumere anche il valore indeterminato e seguono le tavole della *logica a tre valori forte di Kleene*. Nella semantica parziale, **non-falso** non implica **vero** e una sequenza $A \Rightarrow B$ è validata da una valutazione parziale V se da $V(A) = 1$ (A vera) segue che $V(B) \neq 0$ (A non è falsa). Dunque, se $\Rightarrow A$ e $A \Rightarrow B$ sono valide in V, si ha solo $V(A) \neq 0$ e se $V(A) = 1$, allora $V(B) \neq 0$, e non si può concludere $V(B) \neq 0$. In altri termini, la cesura non è corretta in generale rispetto alla semantica delle valutazioni parziali.

Il tema sarebbe meritevole di attenzione: è stato sviluppato nel contesto di una chiarificazione della prova della congettura di Takeuti (Hauptsatz per il calcolo di Gentzen al secondo ordine). Per ragioni di tempo e spazio si rimanda il lettore ai testi di Schütte e Girard.

Teoremi fondamentali

Definizione 2.2.7. Sia Σ un insieme *arbitrario* di formule. Allora diremo che $\Gamma \Rightarrow \Delta$ è *deducibile* da Σ - in simboli $\Sigma \Vdash \Gamma \Rightarrow \Delta$ - sse esiste un sottinsieme finito Σ_0 di Σ, tale che è derivabile in $\mathsf{G3}$ (e dunque senza cesure) la sequenza $\Sigma_0, \Gamma \Rightarrow \Delta$.

Ricordiamo senza prova il fondamentale

Teorema 2.2.8. *Un insieme di formule o è refutabile oppure è soddisfacibile in un dominio numerabile.*

Teorema 2.2.9. $\Gamma \Rightarrow \Delta$ *è deducibile senza cesure da* Σ *oppure esiste una valutazione su un dominio numerabile che soddisfa* Σ *e tutte le formule di* Γ*, ma falsifica tutte le formule di* Δ*.*

Corollario 2.2.10 (Completezza Generale)**.** *Se* $\Sigma \models \Gamma \Rightarrow \Delta$*, allora*

$$\Sigma \vdash \Gamma \Rightarrow \Delta.$$

Dunque, se Σ *contiene solo formule chiuse,*

$$\Sigma \vdash \Gamma \Rightarrow \Delta \text{ sse } \Sigma \models \Gamma \Rightarrow \Delta$$

Dimostrazione. Infatti per ipotesi deve valere, per qualche sottinsieme finito Σ_0 di Σ che

$$\Sigma_0, \Gamma \Rightarrow \Delta$$

è derivabile senza cesure in $\mathsf{G3}$. Dunque applicando un numero finito di volte la cesura con le sequenze della forma $\Gamma \Rightarrow \Delta, B$, dove $B \in \Sigma_0$, si ottiene per definizione che

$$\Sigma \vdash \Gamma \Rightarrow \Delta$$

Il viceversa segue dalla proposizione 2.2.4. □

Come già nel caso enunciativo, si ottiene anche il

Corollario 2.2.11 (Eliminazione della Cesura)**.** *Se* $\Gamma \Rightarrow \Delta$ *è derivabile in* $\mathsf{G3}$+Cut*, allora* $\Gamma \Rightarrow \Delta$ *è derivabile in* $\mathsf{G3}$*.*

La tecnica di prova consiste nel costruire in stadi un albero binario i cui nodi sono rivestiti di sequenze, in modo che, se l'albero è finito, esso è essenzialmente - a meno dell'applicazione dei lemmi di indebolimento e tautologia - una deduzione di $\Gamma \Rightarrow \Delta$ da un sottinsieme finito di Σ; altrimenti, c'è un ramo infinito dell'albero che definisce una valutazione che soddisfa i requisiti stabiliti dall'enunciato del teorema.

2.3 Inferenze ammissibili a livello elementare

Possiamo agevolmente estendere notazioni e risultati della sezione 1.1.2.

Una *derivazione* in $\mathcal{S}$ (essendo $\mathcal{S}$ $\mathsf{G3}$ oppure $\mathsf{G3}$+Cut) è un albero finitario localmente corretto rispetto alle regole di $\mathcal{S}$.

In modo analogo si definisce la *relazione di derivabilità*:

$$\mathcal{D} \vdash_k^m \Gamma \Rightarrow \Delta$$

sse $\mathcal{D}$ è una derivazione in G3 di $\Gamma \Rightarrow \Delta$ tale che:

- ogni ramo di $\mathcal{D}$ ha al massimo lunghezza m;
- ogni formula che occorre come formula di cesura in $\mathcal{D}$ ha complessità logica minore di k

$\vdash_k^m \Gamma \Rightarrow \Delta$ significa che esiste una derivazione $\mathcal{D}$ tale che $\mathcal{D} \vdash_k^m \Gamma \Rightarrow \Delta$. Il concetto di *regola ammissibile* si lascia ugualmente trasferire al caso predicativo.

Vi è tuttavia una inferenza ammissibile tipica del livello predicativo, la *sostituzione.*

Definizione 2.3.1. $\mathcal{D}[a := t]$ designa la struttura che si ottiene da $\mathcal{D}$ rimpiazzando ogni occorrenza del parametro a in $\mathcal{D}$ col termine t.

Ovviamente, $\mathcal{D}[a := t]$ non sempre è una derivazione, dato che la sostituzione può distruggere la correttezza locale delle regole $R\forall$ e $R\exists$. Ma è sempre possibile applicare gli opportuni cambi alfabetici, in modo che nessun parametro proprio della derivazione occorra nel termine t da sostituire e che $\mathcal{D}[a := t]$ sia dunque sempre una derivazione. Infatti è facile dimostrare che vale:

Lemma 2.3.2 (Cambio di parametri propri)**.** *Se $\mathcal{D} \vdash_k^m \Gamma \Rightarrow \Delta$ e b non occorre fra i parametri di $\mathcal{D}$, allora anche*

$$\mathcal{D}[a := b] \vdash_k^m \Gamma[a := b] \Rightarrow \Delta[a := b]$$

Inoltre, se $\mathcal{D} \vdash_k^m \Gamma \Rightarrow \Delta$, a occorre come parametro proprio in $\mathcal{D}$, mentre b non occorre in $\mathcal{D}$, allora esiste una derivazione $\mathcal{D}'$ in cui b occorre come pametro proprio al posto di a (e dunque a non è parametro proprio di $\mathcal{D}'$), ed inoltre

$$\mathcal{D}' \vdash_k^m \Gamma \Rightarrow \Delta$$

Dimostrazione. Per induzione su m ID, le regole proposizionali e $L\forall$, $R\exists$ sono preservate dalla sostituzione. Nel caso di $R\forall$ e $R\exists$ si applica il lemma precedente. □

Osservazione 2.3.3. *Condizione di purezza delle derivazioni*: data una derivazione, non è restrittivo supporre che i parametri propri usati nelle inferenze di introduzione dell'universale a destra e dell'esistenziale a sinistra siano tutti distinti fra di loro.

Lemma 2.3.4 (Sostituzione)**.** *Se $\vdash_k^m \Gamma \Rightarrow \Delta$, allora anche*

$$\vdash_k^m \Gamma[a := t] \Rightarrow \Delta[a := t]$$

L'idea è di rimpiazzare ovunque a con t. Ma t può contenere dei parametri che occorrono come parametri propri in una inferenza $\mathcal{D}$, per cui la sostituzione può distruggere la correttezza locale. La difficoltà si lascia evitare facendo prima una rinomina dei parametri propri della derivazione...

I lemmi di scambio, indebolimento e contrazione valgono anche per il calcolo predicativo $\mathsf{G3{+}cut}$; ma c'è bisogno di un po' di cautela per via dei quantificatori e della sostituzione. Inoltre non tutte le inferenze sono invertibili; questa è la ragione per cui la contrazione diventa ammissibile solo se la si accetta la peculiare forma delle regole $L\forall$ e $R\exists$.

Lemma 2.3.5 ($\mathsf{G3}$ e $\mathsf{G3{+}cut}$)**.** *Sono ammissibili* *(i) le regole di scambio e indebolimento;*

(ii) le regole d'inversione per le regole logiche enunciative ed inoltre, se t è un termine arbitrario:

1. $\vdash_k^m \Gamma \Rightarrow \Delta, \forall x A$ *implica* $\vdash_k^m \Gamma \Rightarrow \Delta, A[x := t]$*;*

2. $\vdash_k^m \Gamma, \exists x A \Rightarrow \Delta$ *implica* $\vdash_k^m \Gamma, A[x := t] \Rightarrow \Delta$*;*

(iii) le regole di contrazione.

Dimostrazione. La prova dell'indebolimento fa uso del cambio di parametri propri, mentre l'inversione di $R\forall$ e $L\exists$ richiede anche il lemma di sostituzione. Quanto al lemma di contrazione, consideriamo solo il caso delle inferenze su $\forall$. Supponiamo che valga

$$\vdash_k^m \Gamma \Rightarrow \Delta, \forall x A, \forall x A$$

Procedendo al solito per induzione, siamo condotti a considerare due casi. Se l'inferenza finale I non si applica a nessuna delle due occorrenze di $\forall x A$, si applica l'ipotesi d'induzione alle premesse, cancellando una occorrenza di $\forall x A$ e si esegue I. Se l'inferenza finale è una introduzione di $\forall$ che genera una occorrenza di $\forall x A$, si applica l'inversione all'altra occorrenza, ottenendo così per qualche a, che non occorre in $\Gamma, \Delta, \forall x A$ e qualche $n < m$,

$$\vdash_k^n \Gamma \Rightarrow \Delta, A[x := a], A[x := a]$$

da cui la conclusione segue cancellando prima una occorrenza di $A[x := a]$ e poi applicando $R\forall$.

Supponiamo che valga

$$\vdash_k^m \forall x A, \forall x A, \Gamma \Rightarrow \Delta$$

Come sopra, se l'ultima inferenza I non agisce sulle due occorrenze di $\forall x A$, si applica l'IH cancellando una delle due e poi si applica I. Se invece l'ultima inferenza agisce su una delle due occorrenze di $\forall x A$, si ha per qualche t e qualche $n < m$

$$\vdash_k^n \forall x A, \forall x A, A[x := t], \Gamma \Rightarrow \Delta$$

Dunque si può applicare l'ipotesi d'induzione (qui è cruciale la forma di $R\forall$!), ottenendo:

$$\vdash_k^n \forall x A, A[x := t]\,, \Gamma \Rightarrow \Delta$$

Applicando $R\forall$ segue

$$\vdash_k^m \forall x A,\ \Gamma \Rightarrow \Delta$$

□

Osservazione 2.3.6. La cesura moltiplicativa CUT_m è derivabile in G3; più precisamente:

(CUT_m) se $\vdash_k^m\ \Gamma \Rightarrow \Delta, A$ e $\vdash_k^m\ A, \Gamma' \Rightarrow \Delta'$, allora

$$\vdash^{m+1}_{\max\{k, rk(A)+1\}} \Gamma, \Gamma' \Rightarrow \Delta, \Delta'$$

Chiaramente, CUT_m crea molteplicità. Se si assume con la contrazione CUT_m si può ottenere la cesura *context-sharing*.

2.4 Prova dell'Hauptsatz e proprietà della sottoformula

Lemma 2.4.1 (Riduzione)**.** *Siano date* $\mathcal{D}_1$*,* $\mathcal{D}_2$ *tali che*

$$\begin{array}{lll} \mathcal{D}_1 & \vdash^l_k & \Gamma \Rightarrow \Delta, A \\ \mathcal{D}_2 & \vdash^m_k & A, \Gamma' \Rightarrow \Delta' \end{array}$$

dove $k = rk(A)$*. Allora si può costruire una derivazione* $\mathcal{D} = Red(\mathcal{D}_1, \mathcal{D}_2)$ *tale che*

$$\mathcal{D} \vdash^{l+m}_k \Gamma, \Gamma' \Rightarrow \Delta, \Delta'$$

Dimostrazione. Induzione su $l + m$: si suppone dunque per IH che il lemma valga già per ogni coppia di derivazioni $\mathcal{D}^*_1$, $\mathcal{D}^*_2$ tali che $rk(B) = k$, $p+q < l+m$ e

$$\mathcal{D}^*_1 \vdash^p_k \Gamma_1 \Rightarrow \Delta_1, B \quad \mathcal{D}^*_2 \vdash^q_k A, \Gamma_2 \Rightarrow \Delta_2.$$

Caso 1: A è attiva sia in $\mathcal{D}_1$ sia in $\mathcal{D}_2$ ed è atomica.

- Se $A \equiv \top$, $\top$ deve già occorrere in Δ' e $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ è già un assioma per $\top$.
- Se $A \equiv \bot$, $\bot$ deve già occorrere in Γ e $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ è già un assioma per $\bot$.
- Se A non è un booleano, A occorre sia in Γ sia in Δ' e $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ è un assiome ID.

Caso 2: A non è attiva in $\mathcal{D}_1$ oppure in $\mathcal{D}_2$. Per simmetria, consideriamo solo il secondo caso
Caso 2.1: $A, \Gamma' \Rightarrow \Delta'$ è un assioma. Dato che A non è attiva in $\mathcal{D}_2$, $\Gamma' \Rightarrow \Delta'$ è un assioma e dunque $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ è un assioma.
Caso 2.2: $A, \Gamma' \Rightarrow \Delta'$ è la conclusione di una inferenza $\mathcal{I}$ in cui A non è attiva. Dunque A occorre già nelle premesse di $\mathcal{I}$. Si applica allora ad esse e a $\mathcal{D}_1$ il lemma di riduzione per IH.

Facciamo l'esempio in cui $\mathcal{D}_2$ termina con una introduzione della $\vee$ a sinistra. Si ha dunque, per qualche $m > l, r$, essendo $\Gamma' \equiv \Gamma^*, C \vee D$:

$$\dfrac{\vdash^l \Gamma \Rightarrow \Delta, A \qquad \dfrac{\vdash^{r_0} A, C, \Gamma^* \Rightarrow \Delta' \qquad \vdash^{r_1} A, D, \Gamma^* \Rightarrow \Delta'(r_1)}{\vdash^r A, C \vee D, \Gamma^* \Rightarrow \Delta'(r)}}{\vdash^m \Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

Ma $l + r_0, l + r_1 < l + r$ e per IH:

$$\dfrac{\dfrac{\vdash^l \Gamma \Rightarrow \Delta, A \qquad \vdash^{r_0} A, C, \Gamma^* \Rightarrow \Delta'}{\vdash^{l+r_0} \Gamma, \Gamma^*, C \Rightarrow \Delta, \Delta'} \qquad \dfrac{\vdash^l \Gamma \Rightarrow \Delta, A \qquad \vdash^{r_1} A, D, \Gamma^* \Rightarrow \Delta'}{\vdash^{l+r_1} \Gamma, \Gamma^*, D \Rightarrow \Delta, \Delta'}}{\vdash^{l+r} \Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

Caso 3: A è attiva sia in $\mathcal{D}_1$ sia in $\mathcal{D}_2$ ed non è atomica. Ci limitiamo a trattare esplicitamente i casi dell'implicazione e del quantificatore universale.
Caso 3.1. Se $A := C \to D$, si ha:

$$\frac{\vdash_k^{l_0} C, \Gamma \Rightarrow \Delta, D}{\vdash_k^{l} \Gamma \Rightarrow \Delta, C \to D}$$

ed inoltre

$$\frac{\vdash_k^{r_0} \Gamma' \Rightarrow \Delta', C \qquad \vdash_k^{r_1} \Gamma', D \Rightarrow \Delta'}{\vdash_k^{r} C \to D, \Gamma' \Rightarrow \Delta'}$$

Si passa allora alla derivazione:

$$\cfrac{\cfrac{\cfrac{\vdash_k^{r_0} \Gamma' \Rightarrow \Delta', C \qquad \vdash_k^{l_0} C, \Gamma \Rightarrow \Delta, D}{\vdash^{\max(r_0,l_0)+1} \Gamma, \Gamma', C \Rightarrow \Delta, \Delta', D} \qquad \vdash_k^{r_1} \Gamma', D \Rightarrow \Delta'}{\vdash_k^{l+r} \Gamma', \Gamma', \Gamma \Rightarrow \Delta, \Delta', \Delta'}}{\vdash_k^{l+r} \Gamma', \Gamma \Rightarrow \Delta, \Delta'}$$

NB: sopra si è applicata CUT_m e la contrazione. Si osservi che

$$rk(C), rk(D) < rk(C \to D)$$

. Inoltre per ipotesi $l, r > 0$ e $\max(r_0, l_0) + 1 < l + r$ (infatti se $\max(r_0, l_0) + 1 = r_0 + 1$, $r_0 + 1 \leq r < r + l$; se invece $\max(r_0, l_0) + 1 = l_0 + 1$, $l_0 + 1 \leq l < l + r$.).
Caso 3.2. Se $A := \forall x A$, si ha, se $a \notin FV(\Gamma, \Delta,$

$$\frac{\vdash_k^{l_0} \Gamma \Rightarrow \Delta, A(a)}{\vdash_k^{l} \Gamma \Rightarrow \Delta, \forall x A}$$

e

$$\frac{\vdash_k^{r_0} A(t), \forall x A, \Gamma' \Rightarrow \Delta'}{\vdash_k^{r} \forall x A, \Gamma' \Rightarrow \Delta'}$$

Si passa allora a costruire, applicando sostituzione e contrazione, la nuova derivazione:

$$\cfrac{\cfrac{\cfrac{\vdash_k^{l} \Gamma \Rightarrow \Delta, \forall x A \qquad \vdash_k^{r_0} A(t), \forall x A, \Gamma' \Rightarrow \Delta', \Delta}{\vdash_k^{l+r_0} \Gamma, \Gamma', A(t) \Rightarrow \Delta, \Delta', D} \qquad \vdash_k^{l_0} \Gamma \Rightarrow \Delta, A(t)}{\vdash_k^{l+r} \Gamma', \Gamma, \Gamma \Rightarrow \Delta, \Delta, \Delta'}}{\vdash_k^{l+r} \Gamma', \Gamma \Rightarrow \Delta, \Delta'}$$

NB: prima di applicare la cesura moltiplicativa a $A(t)$ (che ha rango ¡k), procede a ridurre la formula principale che occorre come minore nella premessa della regola di introduzione a destra dell'universale. □

Lemma 2.4.2 (Eliminazione). *Sia* $\mathcal{D} \vdash_{k+1}^{l} \Gamma \Rightarrow \Delta$. *Allora si può costruire una derivazione* $\mathcal{D}^*$ *tale che*

$$\mathcal{D} \vdash_k^{2^l} \Gamma \Rightarrow \Delta$$

Dimostrazione. Induzione su l.
Caso 1: l'ultima inferenza non è una cesura oppure è una cesura su una formula di rango $< k$. Si applica l'IH alle premesse e si usa la monotonia di $n \mapsto 2^n$. Come esempio, si consideri il caso in cui $rk(A) < k$, $p < l$, $q < q$ e

$$\vdash_{k+1}^{p} \Gamma \Rightarrow \Delta, A, \quad \vdash_{k+1}^{q} A, \Gamma \Rightarrow \Delta.$$

Allora per IH

$$\vdash_k^{2^p} \Gamma \Rightarrow \Delta, A, \quad \vdash_k^{2^q} A, \Gamma \Rightarrow \Delta.$$

Dunque, per cesura di rango minore di k, dato che $2^p, 2^q < 2^l$, si ha

$$\vdash_k^{2^l} \Gamma \Rightarrow \Delta.$$

Caso 2: l'ultima inferenza è una cesura su A con $rk(A) = k$ e vale

$$\vdash_{k+1}^{p} \Gamma \Rightarrow \Delta, A, \quad \vdash_{k+1}^{q} A, \Gamma \Rightarrow \Delta.$$

Per IH, ancora

$$\vdash_k^{2^p} \Gamma \Rightarrow \Delta, A, \quad \vdash_k^{2^q} A, \Gamma \Rightarrow \Delta.$$

Ma sono soddisfatte le ipotesi della lemma di riduzione, applicando il quale e il lemma di contrazione si ottiene:

$$\vdash_k^{2^p+2^q} \Gamma \Rightarrow \Delta.$$

Ma

$$2^p + 2^q \leq 2^{\max(p,q)+1} \leq 2^l.$$

□

Poniamo: $2_0(l) = l$ e $2_{n+1}(l = 2^{2_n(l)}$.

Teorema 2.4.3 (Hauptsatz). *Sia $\mathcal{D} \vdash_k^l \Gamma \Rightarrow \Delta$. Allora si può costruire una derivazione $\mathcal{D}^*$ di $\Gamma \Rightarrow \Delta$, priva di cesure e di lunghezza $\lambda \leq 2_k(l)$*

Dimostrazione. Induzione su k. Se $k = 0$, non c'è nulla da provare.
Sia $k = n + 1$: applicare il lemma di eliminazione e IH. □

Corollario 2.4.4 (Teilformelsatz). *Sia $\mathcal{D}$ una derivazione di $\Gamma \Rightarrow \Delta$. Allora si può trovare una derivazione $\mathcal{D}^*$ della stessa conclusione con le seguenti proprietà:*

- *sia $\Gamma' \Rightarrow \Delta'$ una sequenza che occorre a un nodo di $\mathcal{D}^*$. Allora ogni formula che occorre in $\Gamma' \Rightarrow \Delta'$ è sottoformula di una formula che occorre in $\Gamma \Rightarrow \Delta$;*

- *$\mathcal{D}^*$ contiene solo regole logiche e/o assiomi per simboli logici che occorrono in formule della conclusione.*

Osservazione 2.4.5.

1. Dall'Hauptsatz segue la consistenza del calcolo: la sequenza vuota $\Rightarrow$ non è derivabile in G3.

2. La stima iperesponenziale è essenziale (Orevkov ha dimostrato ci sono casi in cui non si può far meglio, si veda il capitolo di Pudlak in [6]).

Osservazione 2.4.6. Le prove cut-free permettono di provare raffinamenti dell'Hauptsatz da cui segue il teorema di Herbrand. In generale, per questo tipo di applicazioni, è conveniente usare i calcoli G1, in cui si accettano esplicitamente le regole strutturali, e le regole logiche a due premesse sono moltiplicative (possono avere contesti diversi che vengono accumulati nella conclusione). Si veda 5.2 in [8] or 2.6.4 in [3]).

Teorema 2.4.7. *Sia $\mathcal{D}$ una derivazione cut-free in G1 di $\Gamma \Rightarrow \Delta$ in cui le formula di $\Gamma \Rightarrow \Delta$ sono in forma normale prenessa. Allora si può costruire una derivazione $\mathcal{D}^*$ in G1 della stessa conclusione in cui ogni inferenza sui quantificatori segue ogni inferenza sui connettivi.*

Si ha subito una versione del teorema di Herbrand:

Corollario 2.4.8. *Se $\exists\vec{x}A$ è derivabile nella logica predicativa e A è priva di quantificatori, si possono trovare (vettori di) termini $\vec{t_1}, \ldots \vec{t_p}$ tali che è una tautologia*

$$A[\vec{x} := \vec{t_1}] \vee \ldots \vee A[\vec{x} := \vec{t_p}]$$

2.5 Interpolazione

Una volta provata la completezza del calcolo $G3$ e l'eliminazione delle cesure 2.2.11, abbiamo un potente strumento metalogico per dimostrare alcuni risultati fondamentali della logica elementare. Qui ci limiteremo a provare il teorema, dimostrato da William Craig(1918-) nel 1957, che mette a fuoco un'importante proprietà della logica elementare: se si dimostra logicamente una implicazione $A \to B$, allora è possibile passare da A a B utilizzando come medio un enunciato C – detto *interpolante* – che contiene *solo i concetti comuni* – in un senso che si può precisare – ad A e B. Come vedremo, Il teorema di Craig ha un'importante applicazione alla teoria della definibilità e può essere riformulato in modo da costituire una genuina generalizzazione del teorema dell'esistenza del modello. Iniziamo con alcune definizioni e convenzioni notazionali.

Definizione 2.5.1.

- (i) Per A formula, $\Gamma \Rightarrow \Delta$ sequenza:
  - $\mathcal{L}(A)$:= l'insieme delle costanti individuali, delle costanti predicative e delle variabili che occorrono libere in A;
  - $\mathcal{L}(\Gamma) := \bigcup_{A\in\Gamma} \mathcal{L}(A)$;
  - $\mathcal{L}(\Gamma \Rightarrow \Delta) := \mathcal{L}(\Gamma) \cup \mathcal{L}(\Delta)\ \ (= \mathcal{L}(\Gamma \cup \Delta))$.

  Notare: le costanti funtoriali presenti in A non fanno parte di $\mathcal{L}(A)$.

(ii) Una *partizione* di una sequenza $S \equiv \Gamma \Rightarrow \Delta$ è una coppia ordinata

$$\mathcal{P} \equiv \langle \Gamma_1 \Rightarrow \Delta_1 \ \| \ \Gamma_2 \Rightarrow \Delta_2 \rangle$$

di sequenze, tali che $\Gamma_1 \cup \Gamma_2 = \Gamma$ e $\Delta_1 \cup \Delta_2 = \Delta$.
$\Gamma_1 \Rightarrow \Delta_1$ ($\Gamma_2 \Rightarrow \Delta_2$) è detta la parte sinistra (destra) di $\mathcal{P}$.
Notare: non si esclude il caso in cui uno di Γ_1, Γ_2 è vuoto, e/o uno di Δ_1, Δ_2 è vuoto.

(iii) Una formula C è *adatta* alla partizione $\langle \Gamma_1 \Rightarrow \Delta_1 \ \| \ \Gamma_2 \Rightarrow \Delta_2 \rangle$ sse

$$\mathcal{L}(C) \subseteq \mathcal{L}(\Gamma_1 \Rightarrow \Delta_1) \cap \mathcal{L}(\Gamma_2 \Rightarrow \Delta_2)$$

sse, a parole, le sue variabili libere e le sue costanti descrittive *che non sono funtori* (di arietà ≥ 1) occorrono sia nella sequenza $\Gamma_1 \Rightarrow \Delta_1$ sia nella sequenza $\Gamma_2 \Rightarrow \Delta_2$.

(iv) Una formula C è detta essere un'*interpolante* per la partizione $\mathcal{P} = \langle \Gamma_1 \Rightarrow \Delta_1 \parallel \Gamma_2 \Rightarrow \Delta_2 \rangle$ di $\Gamma \Rightarrow \Delta$ sse:

1. C è adatta a $\mathcal{P}$;
2. vale:

$$\mathsf{G3} \vdash \Gamma_1 \Rightarrow \Delta_1, C \qquad e \qquad \mathsf{G3} \vdash C, \Gamma_2 \Rightarrow \Delta_2 .$$

2.5.1 Il Lemma di Maehara

Salvo avviso contrario, d'ora in avanti per 'dimostrazione di $\Gamma \Rightarrow \Delta$' intendiamo: 'dimostrazione *cut-free* di $\Gamma \Rightarrow \Delta$ nel calcolo G3' (in simboli: $\mathcal{D} \vdash \Gamma \Rightarrow \Delta$). Dimostriamo il fondamentale:

Lemma 2.5.2 (Maehara 1960)**.**
Sia

$$\mathcal{D} \vdash S :\equiv \Gamma \Rightarrow \Delta.$$

Allora, per ogni partizione

$$\mathcal{P} \equiv \langle S_1 \parallel S_2 \rangle$$

della sequenza S, si dà uno dei tre casi seguenti:

(I) esiste una dimostrazione $\mathcal{D}' \vdash S_1$;

(II) esiste una dimostrazione $\mathcal{D}'' \vdash S_2$;

(III) esiste un'interpolante C *per la partizione.*

Inoltre, la dimostrazione $\mathcal{D}'$ *nel caso (I), la dimostrazione* $\mathcal{D}''$ *nel caso (II), l'interpolante* C *e le due relative dimostrazioni nel caso (III), sono* effettivamente costruibili *sulla base di* $\mathcal{D}$ *e di* $\mathcal{P}$.

Dimostrazione. Si ragiona per induzione sull'altezza della data dimostrazione cut-free $\mathcal{D}$ di S, distinguendo casi a seconda della inferenza finale R di $\mathcal{D}$.

L'interpolante viene esplicitamente costruito a partire dai dati della derivazione....

Come abbreviazione temporanea nel corso della presente dimostrazione, scriveremo $\Gamma \Rightarrow^n \Delta$ per designare la derivabilità di $\Gamma \Rightarrow \Delta$ mediante una derivazione in G3 di altezza $\leq n$.

Consideriamo esplicitamente solo il caso (complesso) del quantificatore universale

$\boxed{\text{Caso 12: } R \text{ è } [\forall\Rightarrow].}$ Allora $S \equiv \forall x A, \Gamma \Rightarrow \Delta$ e

$$\mathcal{D} \equiv \quad \dfrac{\left.\begin{matrix} \vdots \\ A[x/t], \forall x A, \Gamma \Rightarrow^{n-1} \Delta \end{matrix}\right\} \mathcal{D}_1}{\forall x A, \Gamma \Rightarrow^{n} \Delta} \ [\forall\Rightarrow]$$

per un certo termine t.

Come al solito distinguiamo:

sottocaso 12.1 $\mathcal{P} \equiv \langle \forall x A, \Gamma_1 \Rightarrow \Delta_1 \parallel \Gamma_2 \Rightarrow \Delta_2 \rangle$. Si considera allora la partizione

$$\mathcal{P}' \equiv \langle A[x/t], \forall x A, \Gamma_1 \Rightarrow \Delta_1 \parallel \Gamma_2 \Rightarrow \Delta_2 \rangle$$

della premessa, cioè della sequenza finale di $\mathcal{D}_1$. Applicando a $\mathcal{D}_1$ l'ipotesi induttiva rispetto alla partizione $\mathcal{P}'$, si ha uno di:

(I′) $\mathcal{D}' \vdash A[x/t], \forall x A, \Gamma_1 \Rightarrow \Delta_1$;

(II′) $\mathcal{D}'' \vdash \Gamma_2 \Rightarrow \Delta_2$;

(III′) esiste C adatta a $\mathcal{P}'$ tale che

$$\mathcal{D}_1' \vdash A[x/t], \forall x A, \Gamma_1 \Rightarrow \Delta_1, C \quad \text{e} \quad \mathcal{D}_1'' \vdash C, \Gamma_2 \Rightarrow \Delta_2 \,.$$

Se vale (I′), allora (prolungando $\mathcal{D}'$ con una $[\forall\Rightarrow]$) si ha che per $\mathcal{P}$ vale (I).
Se vale (II′), allora banalmente anche per $\mathcal{P}$ vale (II).
Se vale (III′), osserviamo intanto che C, pur essendo adatta a $\mathcal{P}'$, può non essere adatta a $\mathcal{P}$: infatti ci potrebbe ben essere una variabile libera o una costante individuale che occorre:

- in C,
- in $\Gamma_2 \Rightarrow \Delta_2$ e in $A[x/t]$, cosicché appartiene a

$$\mathcal{L}(A[x/t], \forall x A, \Gamma_1 \Rightarrow \Delta_1) \cap \mathcal{L}(\Gamma_2 \Rightarrow \Delta_2)\,,$$

- *ma non occorre* in $\forall x A, \Gamma_1 \Rightarrow \Delta_1$.

Siano allora:

- $c_1, \ldots, c_k$ tutte le costanti individuali che occorrono in C, in $A[x/t]$ e in $\Gamma_2 \Rightarrow \Delta_2$ ma non in $\forall x A, \Gamma_1 \Rightarrow \Delta_1$.
- $z_1, \ldots, z_m$ tutte le variabili che occorrono libere in C, in $A[x/t]$ e in $\Gamma_2 \Rightarrow \Delta_2$ ma non in $\forall x A, \Gamma_1 \Rightarrow \Delta_1$.

Prendiamo k variabili $u_1, \ldots, u_k$ nuove, e consideriamo la dimostrazione $\mathcal{D}_1^*$ che si ottiene da $\mathcal{D}_1'$ rimpiazzando ovunque, per $1 \leq i \leq k$, la costante c_i con la variabile u_i. Per le ipotesi fatte sulle costanti c_i, si ha che

$$\mathcal{D}_1^* \vdash A[x/t'], \forall x A, \Gamma_1 \Rightarrow \Delta_1, C'$$

dove

$$t' \equiv t[c_1/u_1, \ldots, c_k/u_k]$$

e

$$C' \equiv C[c_1/u_1, \ldots, c_k/u_k]\,.$$

È facile verificare che la formula

$$C^* \equiv \forall u_1 \ldots \forall u_k \forall z_1 \ldots \forall z_m\, C'$$

è adatta alla partizione $\mathcal{P}$. Quindi, grazie alle due dimostrazioni

$$\dfrac{\dfrac{\left.\begin{array}{c}\vdots\\ A[x/t'], \forall x A, \Gamma_1 \Rightarrow \Delta_1,\, C'\end{array}\right\}\mathcal{D}_1^*}{\forall x A, \Gamma_1 \Rightarrow \Delta_1,\, C'}\,[\forall\Rightarrow]}{\forall x A, \Gamma_1 \Rightarrow \Delta_1,\, C^*}\,[\Rightarrow\forall]\ m{+}k \text{ volte}$$

e

$$\dfrac{\left.\begin{array}{c}\vdots\\ C, \Gamma_2 \Rightarrow \Delta_2\end{array}\right\}\mathcal{D}_1''}{C^*, \Gamma_2 \Rightarrow \Delta_2}\,\text{Lemma di indebolimento, più } [\forall\Rightarrow]\ m{+}k \text{ volte}$$

concludiamo che per $\mathcal{P}$ si dà il caso (III) con interpolante C^*.

$\boxed{\text{sottocaso 12.2}}$ $\mathcal{P} \equiv \langle \Gamma_1 \Rightarrow \Delta_1 \ \| \ \forall x A, \Gamma_2 \Rightarrow \Delta_2 \rangle$. Si considera allora la partizione

$$\mathcal{P}' \equiv \langle \Gamma_1 \Rightarrow \Delta_1 \ \| \ A[x/t], \forall x A, \Gamma_2 \Rightarrow \Delta_2 \rangle$$

della premessa, cioè della sequenza finale di $\mathcal{D}_1$. Applicando a $\mathcal{D}_1$ l'ipotesi induttiva rispetto alla partizione $\mathcal{P}'$, si ha uno di:

(I′) $\mathcal{D}' \vdash \Gamma_1 \Rightarrow \Delta_1$;

(II′) $\mathcal{D}'' \vdash A[x/t], \forall x A, \Gamma_2 \Rightarrow \Delta_2$;

(III′) esiste C adatta a $\mathcal{P}'$ tale che

$$\mathcal{D}_1' \vdash \Gamma_1 \Rightarrow \Delta_1,\, C \quad \text{e} \quad \mathcal{D}_1'' \vdash C, A[x/t], \forall x A, \Gamma_2 \Rightarrow \Delta_2\,.$$

Se vale (I′), allora banalmente anche per $\mathcal{P}$ vale (I).
Se vale (II′), allora (prolungando $\mathcal{D}''$ con una $[\forall\Rightarrow]$) si ha che per $\mathcal{P}$ vale (II).
Se vale (III′), ragioniamo dualmente al sottocaso 12.1. Siano cioè:

- $c_1, \ldots, c_k$ tutte le costanti individuali che occorrono in C, in $A[x/t]$ e in $\Gamma_1 \Rightarrow \Delta_1$ ma non in $\forall x A, \Gamma_2 \Rightarrow \Delta_2$.
- $z_1, \ldots, z_m$ tutte le variabili che occorrono libere in C, in $A[x/t]$ e in $\Gamma_1 \Rightarrow \Delta_1$ ma non in $\forall x A, \Gamma_2 \Rightarrow \Delta_2$.

Prendiamo k variabili $u_1, \ldots, u_k$ nuove, e consideriamo la dimostrazione $\mathcal{D}_1^*$ che si ottiene da $\mathcal{D}_1''$ rimpiazzando ovunque, per $1 \leq i \leq k$, la costante c_i con la variabile u_i. Per le ipotesi fatte sulle costanti c_i, si ha che

$$\mathcal{D}_1^* \vdash C', A[x/t'], \forall x A, \Gamma_2 \Rightarrow \Delta_2$$

dove

$$t' \equiv t[c_1/u_1, \ldots, c_k/u_k]$$

e

$$C' \equiv C[c_1/u_1, \ldots, c_k/u_k]\,.$$

È facile verificare che la formula

$$C^* \equiv \exists u_1 \ldots \exists u_k \exists z_1 \ldots \exists z_m\, C'$$

è adatta alla partizione $\mathcal{P}$. Quindi, grazie alle due dimostrazioni

$$\dfrac{\left.\begin{matrix}\vdots\\ \Gamma_1 \Rightarrow \Delta_1,\, C\end{matrix}\right\}\mathcal{D}_1''}{\Gamma_1 \Rightarrow \Delta_1,\, C^*}\ \text{Lemma di indebolimento, più } [\Rightarrow\exists]\ m{+}k \text{ volte}$$

e

$$\dfrac{\dfrac{\left.\begin{matrix}\vdots\\ C, A[x/t'], \forall xA, \Gamma_2 \Rightarrow \Delta_2\end{matrix}\right\}\mathcal{D}_1^*}{C, \forall xA, \Gamma_2 \Rightarrow \Delta_2}\,[\forall\Rightarrow]}{C^*, \forall xA, \Gamma_2 \Rightarrow \Delta_2}\ [\exists\Rightarrow]\ m{+}k \text{ volte}$$

concludiamo che per $\mathcal{P}$ si dà il caso (III) con interpolante C^*. □

2.5.2 Il Teorema di Craig

Il Lemma di Maehara, *unitamente al Teorema di eliminazione delle cesure*, ci fornisce una dimostrazione *puramente sintattica* del

Teorema 2.5.3 (**di interpolazione**, Craig 1957)**.** *Se* $A \to B$ *è un* lemma logico ($\vdash A \to B$ *; equivalentemente, per il teorema di adeguatezza per la logica elementare, una* legge logica*,* $\models A \to B$) *allora vale (almeno) uno di:*

1. $\vdash \neg A$;
2. $\vdash B$;
3. *esiste una formula* C *(detta* interpolante*) tale che*

$$\mathcal{L}(C) \subseteq \mathcal{L}(A) \cap \mathcal{L}(B)\,, \quad \vdash A \to C\,, \quad \vdash C \to B\,.$$

Dimostrazione. Se $\vdash A \to B$ allora la sequenza

$$\Rightarrow A \to B$$

è dimostrabile nel calcolo delle sequenze $\mathsf{G3}$. Per il Teorema di eliminazione delle cesure e il Lemma di inversione, esiste una dimostrazione cut-free

$$\mathcal{D} \vdash A \Rightarrow B\,.$$

Applicando a $\mathcal{D}$ il Lemma di Maehara (Lemma 2.5.2) rispetto alla partizione

$$\mathcal{P} \equiv \langle A \Rightarrow \quad \| \quad \Rightarrow B\rangle$$

della sequenza finale $A \Rightarrow B$, abbiamo che si dà uno dei tre casi:

(I) $\vdash A \Rightarrow\ \ $;

(II) $\vdash\ \ \Rightarrow B$;

(III′) esiste C adatta a $\mathcal{P}$ tale che

$$\vdash A \Rightarrow C \quad \text{e} \quad \vdash C \Rightarrow B\,.$$

Nel caso (I) abbiamo, usando $[\Rightarrow\neg]$, che $\vdash\ \ \Rightarrow \neg A$, e dunque che $\neg A$ è un lemma logico.
Nel caso (II) abbiamo che B è un lemma logico.
Nel caso (III) abbiamo (per definizione di formula *adatta* a una partizione) che $\mathcal{L}(C) \subseteq \mathcal{L}(A) \cap \mathcal{L}(B)$ e che sia $A \to B$ che $C \to B$ sono lemmi logici. □

Nota Bene: Il Lemma di Maehara e il Teorema di Craig valgono anche (la dimostrazione richiede un po' di lavoro in più) quando in $\mathcal{L}(A), \mathcal{L}(\Gamma), \mathcal{L}(S)$ si fanno rientrare anche i *funtori* occorrenti in A, Γ, S.

Osservazione 2.5.4.

- Krisel 1961: non esiste una funzione ricorsiva F totale per produrre l'interpolante fra A e B che dipenda solo da A e B, ovvero tale che, se $A \to B$ è logicamente valida, $F(A, B)$ è l'interpolante fra A e B;

- Friedman-Gurevich: il teorema d'interpolazione fallisce per i modelli finiti: ci sono A e B tali che $A \to B$ è vera in ogni modello finito, ma non esiste alcun C tale che $A \to C$ e $C \to B$ sono vere in tutti i modelli finiti.

Definibilità: il metodo di Padoa-Beth In quanto segue, $\mathbf{T}$ è una arbitraria teoria il cui linguaggio $\mathcal{L}$, **privo di costanti funtoriali**, contiene la costante predicativa n-aria P e *almeno un'altra* costante predicativa.

Per Q una costante predicativa n-aria nuova (cioè che non occorre in $\mathcal{L}$), indichiamo con:

- con $\mathcal{L}^-$ il linguaggio i cui simboli descrittivi sono tutti quelli di $\mathcal{L}$, *meno* P (notare: $\mathcal{L}^-$ è un linguaggio, per l'ipotesi sopra fatta che $\mathcal{L}$ contenga altre costanti predicative oltre P);

- con $\mathcal{L}(Q)$ il linguaggio $\mathcal{L}^-$ più la costante predicativa Q;

- con $\mathbf{T}(Q)$ la teoria su $\mathcal{L}(Q)$ i cui assiomi sono ottenuti da quelli di $\mathbf{T}$ rimpiazzando ovunque P con Q.

sintattica — di *definibilità* (o non indipendenza) *del predicato* P *in* $\mathbf{T}$.

Definizione 2.5.5. P è *definibile esplicitamente* in $\mathbf{T}$ se e solo se esiste una formula A in cui P non occorre, ossia tale che $\mathcal{L}(A) \subseteq \mathcal{L}^-$, per la quale vale

$$\mathbf{T} \vdash \forall x_1 \ldots \forall x_n (P x_1, \ldots, x_n \leftrightarrow A)\,.$$

Definizione 2.5.6. P è *definibile implicitamente* in $\mathbf{T}$ se e solo se, per ogni predicato n-ario Q che non appartiene a $\mathcal{L}$, si ha che

$$\mathbf{T} + \mathbf{T}(Q) \vdash \forall x_1 \ldots \forall x_n (P x_1, \ldots, x_n \leftrightarrow Q x_1, \ldots, x_n)\,.$$

Introduciamo infine la nozione — di natura semantica — di *indipendenza di* P *in* $\mathbf{T}$.

Definizione 2.5.7. P è *indipendente* in $\mathbf{T}$ se e solo se esistono due realizzazioni $\mathcal{M}_1$ e $\mathcal{M}_2$ di $\mathcal{L}$, entrambe su uno stesso dominio M, per le quali vale:

(i) $\mathcal{M}_1$ e $\mathcal{M}_2$ sono modelli di $\mathbf{T}$;

(ii) $\mathcal{M}_1$ e $\mathcal{M}_2$ coincidono su $\mathcal{L}^-$ (ossia assegnano lo stesso significato alle costanti descrittive di $\mathcal{L}$ diverse da P);

(iii) $P^{\mathcal{M}_1} \neq P^{\mathcal{M}_2}$.

La nozione sintattica di *definibilità implicita* equivale — modulo il Teorema di adeguatezza della logica elementare — a quella semantica di *non-indipendenza*.

Fatto 2.5.8. *P è implicitamente definibile in $\mathbf{T}$ se e solo se non è indipendente in $\mathbf{T}$.*

Le due nozioni sintattiche sono equivalenti (cosicché, grazie al Fatto 2.5.8, tutte e tre le nozioni sopra introdotte risultano tra loro equivalenti).

Che la definibilità esplicita implichi la definibilità implicita è quasi ovvio:

Lemma 2.5.9. *Se P è esplicitamente definibile in $\mathbf{T}$ allora P è anche implicitamente definibile in $\mathbf{T}$.*

Il viceversa invece non è affatto ovvio, ed è un profondo risultato, che segue come *corollario del Teorema 2.5.3 di interpolazione*.

Teorema 2.5.10 (**di definibilità di Beth**; Beth 1953)**.** *Se P è implicitamente definibile in $\mathbf{T}$ allora P è anche esplicitamente definibile in $\mathbf{T}$.*

Bibliografia

[1] G. TAKEUTI, *Proof Theory*, North Holland, 1975[1], 1985[2].

[2] K. SCHÜTTE, *Proof Theory*, Berlin-Heidelberg, Springer, 1974.

[3] J. Y. GIRARD, *Proof Theory and Logical Complexity*, Bibliopolis, Napoli 1987.

[4] J. Y. GIRARD et al., *Proofs and Types*, Cambridge University Press, Cambridge 1989.

[5] W. POHLERS, *Proof Theory: an introduction*, Springer, Springer Lecture Notes in Mathematics, Heidelberg 1989.

[6] S. R. BUSS (Editor), *Handbook of Proof Theory*, North Holland, 1998.

[7] S. NEGRI AND J. VON PLATO, *Structural Proof Theory*, Cambridge University Press, Cambridge, 2001

[8] A. S. TROELSTRA AND H. SCHWICHTENBERG, *Basic Proof Theory*, Cambridge University Press, Cambridge, 1996[1], 2007[2]