DEDUZIONE E CONSEGUENZA LOGICA

Uno degli scopi principali della Logica Matematica, oltre a quello di fornire un linguaggio sufficientemente espressivo per la formalizzazione rigorosa di asserti matematici, è quello di permettere la definizione rigorosa del concetto di validità e di dimostrazione di un *teorema*.

Un teorema asserisce la verità di un asserto A (l'enunciato) rispetto ad un insieme di ipotesi $\{A_1, \ldots, A_n\}$ (gli *assiomi*) che tipicamente descrivono le proprietà e le definizioni degli oggetti matematici di riferimento.

Cosa vuol dire quindi che un teorema è valido? L'idea intuitiva è che l'enunciato A è vero assumendo che le ipotesi $\{A_1, \ldots, A_n\}$ siano vere, ovvero che la formula A è vera in tutte le interpretazioni che soddisfano tutte le formule $\{A_1, \ldots, A_n\}$. Questa idea è formalizzata dal seguente concetto di *conseguenza logica*.

1 Conseguenza Logica

Per definire formalmente il concetto di conseguenza logica diciamo che una teoria Γ (ovvero un insieme di formule) è vera in una interpretazione $\mathcal{I}$ ($\mathcal{I} \models \Gamma$) sse $\mathcal{I} \models A$ per ogni formula $A \in \Gamma$.

Definizione 1.1 (Conseguenza Logica) *Sia Γ una teoria ed A una formula. Si dice che A è* conseguenza logica *di Γ ($\Gamma \models A$) se e soltanto se $\mathcal{I} \models A$ in ogni interpretazione $\mathcal{I}$ tale che $\mathcal{I} \models \Gamma$.*

Notate che la teoria Γ può anche essere vuota. In tal caso $\emptyset \models A$ vuol dire che A è vera in ogni interpretazione. Di conseguenza $\emptyset \models A$ (indicato comunemente come $\models A$) vuol dire che A è valida.

Per esempio, abbiamo $\models A \wedge B \to A$. Inoltre abbiamo anche $A \wedge B \models A$ dato che in ogni interpretazione in cui $A \wedge B$ è vera, è vera A. Questo ovviamente non afferma la validità di A! Afferma che A è vera qualora A e B siano vere. Invece abbiamo $A \vee B \not\models A$, dato che esiste una interpretazione in cui $A \vee B$ è vera ed A è falsa (quando B è vera).

Questi esempi suggeriscono un collegamento ovvio tra conseguenza logica ed implicazione. È evidente che $\models A \wedge B \to A$ e $A \wedge B \models A$ vogliono di fatto dire la stessa cosa. Vale infatti la seguente proprietà.

Teorema 1.2 (Teorema di Conseguenza Logica) *Sia A, B formule e Γ una teoria. Abbiamo*

$$\Gamma, A \models B \Longleftrightarrow \Gamma \models A \to B.$$

Il Teorema 1.2 è basato sulle seguenti considerazioni. Dalla Def. di conseguenza logica $\Gamma, A \models B$ sse $\mathcal{I} \models B$ in ogni $\mathcal{I}$ tale che $\mathcal{I} \models \Gamma$ e $\mathcal{I} \models A$. Notiamo per ogni interpretazione $\mathcal{J}$ tale che $\mathcal{J} \models \Gamma$ abbiamo $\mathcal{J} \models A$ o $\mathcal{J} \not\models A$. Vuol dire che per ogni interpretazione $\mathcal{J}$ tale che $\mathcal{J} \models \Gamma$, o $\mathcal{J} \models A$ e $\mathcal{J} \models B$ oppure $\mathcal{J} \not\models A$. Il tutto è equivalente a dire che $\mathcal{J} \models A \rightarrow B$ per ogni interpretazione $\mathcal{J}$ tale che $\mathcal{J} \models \Gamma$.

2 Sistemi Formali di Deduzione

Ma come si fa a dimostrare la validità di un teorema, ovvero come si fa a dimostrare $\Gamma \models A$? Una dimostrazione è costituita da una serie di passaggi logici, o deduzioni, che permettono di dedurre la conclusione A a partire dall'insieme di premesse Γ. Come facciamo ad essere sicuri che la dimostrazione "A segue da Γ" sia *corretta* ovvero che $\Gamma \models A$?

Come abbiamo osservato nell'introduzione al corso l'idea fondamentale è quella di introdurre degli shemi generali di deduzione la cui validità dipende dalla sintassi delle formule piuttosto che dal loro significato. Gli insiemi di regole di deduzione di questo tipo costituiscono un *sistema di dimostrazione formale* $\mathcal{S}$. Il sistema è corretto se è consistente con il concetto semantico di conseguenza logica: ogni volta che si può dimostrare che " A segue da Γ" usando le regole di $\mathcal{S}$ allora $\Gamma \models A$.

Più in dettaglio indichiamo con $\Gamma \vdash_{\mathcal{S}} A$ il fatto che esiste una dimostrazione di A a partire dalle premesse Γ. Si dice che $\mathcal{S}$ è

corretto: Se $\Gamma \vdash_{\mathcal{S}} A$ implica $\Gamma \models A$;

completo: Se $\Gamma \models A$ implica $\Gamma \vdash_{\mathcal{S}} A$.

In letteratura si trovano vari sistemi formali di dimostrazione. In questo corso presenteremo un sistema formale di dimostrazione, le cui regole di inferenza formalizzano *schemi di ragionamento ben noti.* Presenteremo le regole di deduzione discutendone la correttezza, che deriva tipicamente da semplici proprietà semantiche. Il problema della completezza esula dagli obiettivi del corso.

2.1 Regole di Inferenza

Introduciamo un primo insieme di *regole di inferenza* che hanno la forma

$$\frac{A_1 \ldots A_n}{A}$$

Il significato di una regola di questo tipo è che A segue dalle premesse $A_1, \ldots, A_n$ (dove eventualmente $n = 0$).

Il concetto di validità delle regole di questo tipo è piuttosto semplice e corrisponde all'idea intuitiva. Una regola di inferenza di questo tipo è *valida* (corretta) sse [1] A è *conseguenza logica* di $\{A_1, \ldots, A_n\}$ ovvero

$$\{A_1, \ldots, A_n\} \models A.$$

[1] ovvero $\models (A_1 \wedge \ldots \wedge A_n) \rightarrow A$.

$$\frac{A}{A \vee B}\text{ or-intro} \qquad \frac{A \wedge B}{A}\text{ and-elim}$$

$$\frac{A, B}{A \wedge B}\text{ and-intro} \qquad \frac{A, A \to B}{B}\text{ modus ponens}$$

$$\frac{\neg B, A \to B}{\neg A}\text{ modus tollens} \qquad \frac{A \to B, B \to C}{A \to C}\text{ trans}$$

$$\frac{A \vee B, \neg A}{B}\text{ disj. syllogism} \qquad \frac{A, \neg A}{\perp}\text{ contradiction}$$

$$\frac{A \equiv B, A}{B}\text{ equivalence}$$

Table 1: Regole di Inferenza

Notate che questa nozione di validità formalizza l'idea intuitiva per cui assumendo vere le premesse allora la conclusione è vera. Le regole di inferenza del nostro sistema formale (escluse quelle per i quantificatori) sono presentate nella Tabella 1.

Vediamo alcune regole nel dettaglio, cercando di giustificare la loro validità.

1. Le regole *or-intro*, *and-intro* e *and-elim* sono ovvie. Infatti $\{A\} \models A \vee B$, $\{A \wedge B\} \models A$ e $\{A, B\} \models A \wedge B$.

2. La regola *modus ponens* formalizza l'idea che per dimostrare che la conclusione di una implicazione è vera è sufficiente provare che la premessa è vera. Il ragionamento è valido in quanto (basta guardare la tabella di verità)
$$\{A, A \to B\} \models B.$$

3. La regola *modus tollens* formalizza l'idea che se la conclusione di un implicazione è falsa allora anche la premessa deve essere falsa. La validità del ragionamento segue dalla validità di *modus ponens* per la proprietà contrappositiva.

4. La regola *disjunctive syllogism* formalizza l'idea che se ci sono due alternative e la prima (o eventualmente la seconda) non vale, allora deve valere la seconda (resp. la prima). Il ragionamento è valido in quanto (basta guardare la tabella di verità)
$$\{A \vee B, \neg A\} \models B.$$

5. La regola *equivalence* dice che le formule si possono trasformare in formule equivalenti. Questa regola è valida perchè due formule equivalenti hanno esattamente lo stesso valore di verità. Di conseguenza se A è vera è vero anche B. Notate che dire $A \equiv B$ è equivalente a dire $\models A \leftrightarrow B$.

Le regole di inferenza sono della forma

$$\frac{A_1 \ldots A_n}{A}$$

e dipendono dalla sintassi delle premesse $A_1, \ldots, A_n$. Ma come si costruisce una *dimostrazione* utilizzando le regole di inferenza?

Una dimostrazione di A a partire da un insieme di premesse Γ è una successione di passi in cui ad ogni passo si applica una regola di inferenza che consente di derivare la conclusione B a partire dall'insieme di premesse $B_1, \ldots, B_n$, che possono essere formule di Γ ma anche tutte le formule derivate nei passi di dimostrazione precedenti.

Definizione 2.1 (dimostrazioni) *Una* dimostrazione *di una formula A a partire da un insieme di premesse Γ ($\Gamma \vdash A$) è una sequenza di formule $A_1,, \ldots, A_n$ in cui:*

(1) ogni formula A_i è un elemento di Γ oppure è ottenuta applicando una regola di inferenza (della Tabella 1) alle premesse Γ_i dove $\Gamma_i \subseteq \{A_1, \ldots, A_{i-1}\}$

(2) A_n è proprio A.

La (1) mette in luce il fatto che, in una dimostrazione di $\Gamma \vdash A$, le premesse che si possono utilizzare in un passo sono non solo le premesse date Γ ma anche tutte le formule derivate nei passi di dimostrazione precedenti. La (2) mette in luce il fatto che l'ultima formula deve essere la conclusione A. Notate che al primo passo solo le premesse Γ sono utilizzabili. Inoltre notate che non tutte le premesse Γ devono necessariamente essere utilizzate nella prova.

2.1.1 Esempi

Vediamo alcuni esempi di *dimostrazioni*. Indichiamo esplicitamente quali asserti sono premesse e diamo ad ogni passaggio, ovvero applicazione di una regola di inferenza, una giustificazione, indicando la regola di inferenza e le premesse a cui è applicata.

Esempio 2.2 *Sia $\Gamma = \{A, B, (A \wedge B) \rightarrow (C \vee D), \neg D\}$. Diamo una prova $\Gamma \vdash C$.*

1. *A (Premessa)*
2. *B (Premessa)*
3. *$A \wedge B$ (*and-intro *da 1. e 2.)*
4. *$(A \wedge B) \rightarrow (C \vee D)$ (Premessa)*

5. $C \vee D$ (modus ponens *da 3. e 4.).*

6. $\neg D$ *(Premessa)*

7. C (disjunctive syllogism *da 5. e 6.)*

Esempio 2.3 *Sia* $\Gamma = \{P \to Q, \neg P \to R, R \to S\}$. *Diamo una prova di* $\Gamma \vdash \neg Q \to S$.

1. $P \to Q$ *(Premessa)*

2. $P \to Q \equiv \neg Q \to \neg P$ *(regole di equiv);*

3. $\neg Q \to \neg P$ (equivalence *da 1. e 2.)*

4. $\neg P \to R$ *(Premessa)*

5. $\neg Q \to R$ (trans *da 3. e 4.)*

6. $R \to S$ *(premessa)*

7. $\neg Q \to S$ (trans *da 5. e 6.)*

Esempio 2.4 *Sia* $\Gamma = \{P, P \to Q, P \to \neg Q\}$. *Diamo una prova di* $\Gamma \vdash A \wedge \neg A$.

1. P *(Premessa)*

2. $P \to Q$ *(Premessa)*

3. Q (modus ponens *da 1. e 2.).*

4. $P \to \neg Q$ *(Premessa)*

5. $\neg Q$ (modus ponens *da 1. e 4.).*

6. $\perp$ (contradiction *da 3. e 5.)*

7. $A \wedge \neg A \equiv \perp$ *(equivalenza)*

8. $A \wedge \neg A$ (equivalence *da 6. e 7.)*

Esempio 2.5 *Dire se la seguente è una prova corretta di* $\{A \vee B, B \to C\} \vdash C$.

1. $A \vee B$ *(Premessa)*

2. $B \to C$ *(Premessa)*

3. C (modus ponens *da 1. e 2.)*

La prova non è corretta infatti l'applicazione del modus ponens *richiede che la premessa dell'implica sia vera. Non possiamo derivare* A *da* $A \vee B$.

Esempio 2.6 *Dire se la seguente è una prova corretta di* $\{B, A \vee B, B \to C\} \vdash C$.

1. B (Premessa)

2. $B \to C$ (Premessa)

*3. C (*modus ponens *da 1. e 2.)*

La prova è corretta. Notate che la premessa $A \vee B$ non viene utilizzata. L'importante è che in una prova $\Gamma \vdash A$ tutte le premesse appartengano a Γ e non il vice-versa!!!!!!

2.1.2 Correttezza

Le dimostrazioni ottenibili con la Def. 2.1 sono corrette, nel senso che $\Gamma \vdash A$ implica $\Gamma \models A$. Cerchiamo di capire perchè. La cosa fondamentale è capire che le formule ottenute come conclusioni dei passaggi precedenti possono essere usate come premesse dei passaggi successivi.

Consideriamo per semplicità di avere una prova di $\Gamma \vdash B_2$ costituita da due passaggi dove per ogni $i \in \{1, 2\}$, Γ_i è l'insieme delle premesse usate per concludere B_i. Notiamo che Γ_i può essere un sottoinsieme di Γ oppure può contenere formule derivate in precedenza. Dato che ogni regola applicata è valida, abbiamo

$$\Gamma_1 \models B_1$$

$$\Gamma_2 \models B_2$$

Se $\Gamma_2 \subseteq \Gamma$ allora dalla correttezza dell'ultima regola di inferenza $\Gamma_2 \models B_2$, e quindi $\Gamma \models B_2$. Supponiamo invece che una delle premesse dell'ultimo passaggio sia una formula derivata in precedenza (ovvero $B_1 \not\in \Gamma$).

Abbiamo quindi $\Gamma \models B_1$ e $\Gamma, B_1 \models B_2$. Dalla Def. di conseguenza logica (vedi Def. 1.1) vuol dire che

1. B_1 è vera in tutte le interpretazioni in cui Γ è vera;

2. B_2 è vera in tutte le interpretazioni in cui Γ e B_1 sono vere.

Da 1) segue che le interpretazioni in cui Γ è vera e le interpretazioni in cui sia Γ che B_1 sono vere coincidono. Per cui da 2) segue che B_2 è vera in tutte le interpretazioni in cui Γ è vera, ovvero $\Gamma \models B_2$.

Notate che data la correttezza del sistema di prova garantisce che $\Gamma \vdash A$ implica $\Gamma \models A$. Negli esempi precedenti avremmo quindi potuto costruire facilmente le tavole di verità per dimostrare direttamente $\Gamma \models A$!

Ricordiamoci però che dimostrare la validità in Logica Predicativa non è cosi semplice (Vedi gli esercizi della Sezione **??**.)

2.2 Le alte regole di inferenza

Le regole di inferenza della Tabella 1 non sono sufficienti per dimostrare molti asserti matematici. Per avere un sistema formale più interessante è necessario introdurre delle regole di inferenza più complesse, le cui premesse possono essere delle formule o delle sottodimostrazioni. Le regole hanno la forma

$$\frac{\Psi_1, \ldots, \Psi_n, A_1, \ldots, A_k}{A}$$

dove A è la conclusione, $A_1, \ldots, A_k$ sono formule e $\Psi_1, \ldots, \Psi_n$ sono asserti del tipo $\begin{matrix}[C_i] \\ B_i\end{matrix}$.

Il significato delle premesse A_i è quello solito, il significato delle premesse $\begin{matrix}[C_i] \\ B_i\end{matrix}$ è il seguente: se c'e' una una dimostrazione che B_i segue dalla premessa C_i. Le formule C_i esprimono quindi delle *ipotesi aggiuntive* che vengono aggiunte per derivare B_i.

Il concetto di validità di queste regole spiega meglio questa idea. Una regola di inferenza di questo tipo è *corretta* sse

$$\text{Se } C_1 \models B_1, \ldots, C_n \models B_n \text{ allora } \{A_1, \ldots, A_k\} \models A.$$

Questa proprietà chiarisce meglio il significato delle premesse Ψ_i. Una regola di questo tipo: (i) serve per dimostrare A a partire dalle premesse $A_1, \ldots, A_k$; (ii) si applica alle premesse $A_1, \ldots, A_k$, $B_1, \ldots, B_n$ a patto di avere derivato le sottoprove $C_1 \vdash B_1, \ldots, C_n \vdash B_n$. Le premesse aggiuntive $C_1, \ldots, C_n$ sono utilizzate per costruire la dimostrazione ma non sono premesse necessarie alla formula A, infatti abbiamo $\{A_1, \ldots, A_k\} \models A$. Di fatto queste sottoprove sono cancellate quando deriviamo A.

La definizione di dimostrazione $\Gamma \vdash A$ (vedi Def. 2.1) si estende a queste regole in accordo all'idea che si possono utilizzare come premesse anche formule che saranno cancellate in seguito da una regola condizionale.

Definizione 2.7 (dimostrazioni) *Una* dimostrazione *di una formula A a partire da un insieme di premesse Γ ($\Gamma \vdash A$) è una sequenza di formule $A_1, , \ldots, A_n$ in cui:*

(1) ogni formula A_i è

1. *un elemento di Γ;*
2. *l'ipotesi di una regola condizionale applicata al passo j dove $j > i$;*
3. *ottenuta applicando una regola di inferenza alle premesse $\Gamma_i \subseteq \{A_1, \ldots, A_{i-1}\}$.*

(2) A_n è proprio A.

Possiamo quindi introdurre le regole in modo da chiarire questi concetti non semplici.

2.2.1 Implicazioni

Supponiamo di volere dimostrare una implicazione $A \to B$. Dal Teorema di Conseguenza Logica (vedi Teo. 1.2) sappiamo che

$$\models A \to B \;\text{ se } A \models B.$$

Questa proprietà suggerisce che per dimostrare $A \to B$ bisogna trovare una sottodimostrazione che B segue da A. Questo ragionamento è alla base della seguente regola di inferenza

$$\frac{\begin{matrix}[A] \\ B\end{matrix}}{A \to B}\ \text{imp}$$

Notate il ruolo della formula A. Si assume A per dimostrare $A \to B$, ma l'ipotesi A è una premessa aggiuntiva funzionale al fatto di derivare B. Una volta derivata $A \to B$ l'ipotesi A viene cancellata.
Vediamo degli esempi.

Esempio 2.8 *Supponiamo di volere provare che la formula $(A \land B) \to A$ è valida. Seguendo la regola (imp) dobbiamo assumere la premessa $(A \land B)$ e cercare di derivare A.*

1. $A \land B$ *(Premessa*)*
2. A (and-elim *da 1.)*
3. $(A \land B) \to A$ (imp *da 2.)*

Notate che la premessa 1. è la premessa dell'implicazione che è cancellata dal passaggio 3. (come indicato dall'asterisco). Dato che la premessa 1. è cancellata abbiamo dimostrato $\vdash (A \land B) \to A$.

Esempio 2.9 *Supponiamo di volere provare che la formula $((P \to Q) \land P) \to Q$ è valida. Assumiamo la premessa e tentiamo di derivare la conclusione.*

1. $(P \to Q) \land P$ *(Premessa*)*
2. $(P \to Q)$ (and-elim *da 1.)*
3. P (and-elim *da 1.)*
4. Q (modus ponens *da 2. e 3.)*
5. $((P \to Q) \land P) \to Q$ (imp *da 4.).*

Notate che la premessa 1. è cancellata dall'ultimo passaggio. abbiamo dimostrato $\vdash ((P \to Q) \land P) \to Q$.

2.2.2 Contrappositiva

Un altro modo per provare una implicazione $A \to B$ è quello di sfruttare la proprietà contrappositiva $A \to B \equiv \neg B \to \neg A$. Quindi abbiamo dal Teorema di Conseguenza Logica

$$\models A \to B \text{ se } \neg B \models \neg A.$$

Questo ragionamento è alla base della seguente regola di inferenza

$$\frac{\begin{matrix}[\neg B] \\ \neg A\end{matrix}}{A \to B}\ \text{cont-imp}$$

2.2.3 Per assurdo

Un metodo di prova ben noto è quello per assurdo. Supponiamo di volere provare una formula A. Notiamo che per la *contrappositiva*

$$(A \to B) \equiv (\neg B \to \neg A).$$

Inoltre $\models A$ equivale a $\models \top \to A$. Quindi per la contrappositiva $\models \neg A \to \bot$ implica $\models \top \to A$, ovvero $\models A$. Quindi abbiamo per il Teorema di Conseguenza Logica (Teo. 1.2)

$$\models A \text{ se} \neg A \models \bot.$$

Questo ragionamento è alla base della seguente regola di inferenza

$$\cfrac{\begin{matrix}[\neg A]\\ \bot\end{matrix}}{A}\ \text{assurdo}$$

Esempio 2.10 *Dimostriamo che* $\{P \to \neg Q, P \to Q\} \vdash \neg P$.

1. P *(Premessa*)*
2. $P \to \neg Q$ *(Premessa)*
3. $\neg Q$ *(*modus ponens *da 1. e 2.)*
4. $P \to Q$ *(Premessa)*
5. Q *(*modus ponens *da 4. e 1.)*
6. $\bot$ *(*contradiction *da 3. e 5.)*
7. $\neg P$ *(*assurdo *da 6.)*

Notate che l'effetto dell'ultimo passaggio è quello di cancellare la premessa aggiuntiva 1. La dimostrazione formalizza il ragionamento intuitivo: *Supponiamo che P sia vero. .....troviamo una contraddizione, allora $\neg P$ è vero.*

2.2.4 Per casi

Un altro metodo di prova ben noto è quello per casi. Supponiamo di volere derivare una formula A da una formula del tipo $B \vee C$. Se $B \vee C$ vale sappiamo che vale B o vale C ma non sappiamo quale dei due. Non è quindi sufficente mostrare solo che A segue da B o che A segue da C. Solo se A è derivabile sia da A che da B allora possiamo dire che A è conseguenza logica di $B \vee C$. Infatti vale la seguente proprietà semantica

$$B \vee C \models A \text{ se } B \models A \text{ e } C \models A.$$

Questo ragionamento è alla base della seguente regola di inferenza

$$\cfrac{\begin{matrix}[B]\\ A\end{matrix} \qquad \begin{matrix}[C]\\ A\end{matrix} \qquad B \vee C}{A}\ \text{per casi}$$

Notate che le premesse aggiuntive B e C servono per considerare separatamente le due alternative. Dopo l'applicazione della regola solo la premessa $B \vee C$ rimane.

Esempio 2.11 *Dimostriamo che* $\{P \vee Q, P \rightarrow C, Q \rightarrow C, C \rightarrow D\} \vdash D$.
Proviamo che

1. $P \rightarrow C$ *(Premessa)*
2. P *(Premessa*)*
3. C (modus ponens *da 1. e 2.)*
4. $Q \rightarrow C$ *(Premessa)*
5. Q *(Premessa*)*
6. C (modus ponens *da 4. e 5.)*
7. $P \vee Q$ *(Premessa)*
8. C (per casi *da 3. e 6. e 7.)*
9. $C \rightarrow D$ *(Premessa)*
10. D (modus ponens)

Notate che l'effetto dell'applicazione della regola per casi 8. è quello di cancellare le premesse 2. P *e 5 .* Q *che abbiamo aggiunto per dimostrare* $P \vdash C$ *e* $Q \vdash C$.

Nota 2.12 *Un caso particolare della regola per casi si presenta quando le due alternative sono* R *e* $\neg R$ *per una qualche formula* R*. In tal caso* $R \vee \neg R$ *è una formula valida, che non deve essere assunta o dimostrata. In pratica la regola di inferenza è*

$$\frac{\begin{array}{cc}[R] & [\neg R] \\ A & A\end{array}}{A} \ \textit{per casi}$$

2.2.5 Equivalenze

Per dimostrare le equivalenze, ovvero le formule del tipo $A \leftrightarrow B$ si può utilizzare la seguente proprietà

$$\models A \leftrightarrow B \text{ sse } \models A \rightarrow B \text{ e } \models B \rightarrow A.$$

Questo ragionamento è alla base della seguente regola di inferenza condizionale.

$$\frac{\begin{array}{cc}[B] & [A] \\ A & B\end{array}}{A \leftrightarrow B} \ \text{sse}$$

Ovviamente una formule del tipo $A \leftrightarrow B$ si può dimostrare anche facendo una serie di passaggi che trasformano una formula nell'altra in cui ogni passaggio preserva l'equivalenza.

Nota 2.13 (Correttezza) *Le dimostrazioni ottenibili con la Def. 2.7 sono corrette, nel senso che* $\Gamma \vdash A$ *implica* $\Gamma \models A$. *Il ragionamento è simile a quello fatto nel paragrafo 2.1.2.*

2.3 Regole di Inferenza coi quantificatori

Per completare la presentazione delle regole di inferenza vediamo le regole di inferenza per i quantificatori che completano le regole della Tabella 1. Le regole per i quantificatori sono di due tipi:

Regole di generalizzazione Sono regole di inferenza per dimostrare formule del tipo $\forall x A$ e $\exists x A$.

Regole di istanziazione Sono regole di inferenza per dedurre una conclusione da premesse della forma $\forall x A$ e $\exists x A$.

2.3.1 Regole di generalizzazione

Ci sono due regole diverse; una per il quantificatore esistenziale ed una per quello universale.

1. La regola del quantificatore esistenziale è basata sull'idea che per provare una formula del tipo $\exists x A$ bisogna trovare uno *specifico valore* di x per cui A vale. Abbiamo quindi la seguente regola dove t è un termine
$$\frac{A[t/x]}{\exists x A}\ \exists - \mathrm{G}$$
2. La regola del quantificatore universale è un po' più complicata. Infatti per provare una formula del tipo $\forall x A$ bisogna dimostrare che A vale in generale per qualsiasi valore di x. Per rappresentare ogni valore di x si utilizza una nuova variabile x_0 che sta per un elemento *generico ed arbitrario*. Abbiamo quindi la seguente regola dove x_0 è una variabile
$$\frac{A[x_0/x]}{\forall x A}\ \forall - \mathrm{G}$$
Notate che, siccome x_0 deve rappresentare un elemento generico, questa regola si può applicare se e solo se nel corso della dimostrazione non si sono fatte assunzioni su x_0 e non si sono dati valori particolari ad x_0.

2.3.2 Regole di istanziazione

Ci sono due regole diverse; una per il quantificatore esistenziale ed una per quello universale.

1. La regola per il quantificatore universale è basata sull'idea che, se vale $\forall x A$, allora vale A in cui possiamo sostituire ad x qualunque valore. Abbiamo quindi la seguente regola dove t è un termine
$$\frac{\forall x A}{A[t/x]}\ \forall - \mathrm{I}$$

2. La regola per il quantificatore esistenziale è più complicata. Infatti, se vale $\exists x A$, sappiamo che A vale per almeno un valore ma non sappiamo per quale valore. Per rappresentare questo valore indefinito di x si utilizza una nuova variabile x_0. Abbiamo quindi la seguente regola dove x_0 è una variabile
$$\frac{\exists x A}{A[x_0/x]} \exists - \mathrm{I}$$
Notate che x_0 deve rappresentare un elemento che non si conosce. Quindi nel corso della dimostrazione non si possono fare assunzioni su x_0 e non si possono assegnare valori particolari ad x_0.

2.3.3 Esempi

Esempio 2.14 *Dimostriamo che* $\{\forall x(P(x) \to Q(x)), P(a)\} \vdash Q(a)$.

1. $\forall x(P(x) \to Q(x))$ *(Premessa)*
2. $P(a) \to Q(a)$ *($\forall$-I da 1.)*
3. $P(a)$ *(Premessa)*
4. $Q(a)$ *(*modus ponens *da 2. e 3.)*

Notate che questa è la prova del famoso sillogismo

"Se Ogni uomo è mortale e Socrate è un uomo, allora Socrate è mortale"

se si assume il significato dei simboli in cui, a sta per Socrate, P per uomo e Q per mortale.

Ma visto che la dimostrazione è valida indipendentemente dal significato dei simboli è anche vero che

"Se Ogni uomo è immortale e Socrate è un uomo, allora Socrate è immortale"

assumendo per Q il significato di immortale.

Esempio 2.15 *Dimostrare che* $\{\forall x(P(x) \to Q(x)), \forall x P(x)\} \vdash \forall x Q(x)$.

1. $\forall x P(x)$ *(Premessa)*
2. $P(x)$ *($\forall$-I da 1.)*
3. $\forall x(P(x) \to Q(x))$ *(Premessa)*
4. $P(x) \to Q(x)$ *($\forall$-I da 3.)*
5. $Q(x)$ *(*modus ponens *da 2. e 4.)*
6. $\forall x Q(x)$ *($\forall$-G da 5.)*

Notate che la regola di $\forall$-G può essere utilizzata in quanto x rappresenta un termine generico su cui non si fanno assunzioni.

Esempio 2.16 *[Controesempi] Proviamo a dare invece una prova di*

$$\{\forall x(P(x) \to Q(x)), \exists x P(x)\} \vdash \forall x Q(x).$$

1. $\exists x P(x)$ *(Premessa)*
2. $P(x)$ *($\exists$-I da 1.)*
3. $\forall x(P(x) \to Q(x))$ *(Premessa)*
4. $P(x) \to Q(x)$ *($\forall$-I da 3.)*
5. $Q(x)$ *(*modus ponens *da 2. e 4.)*
6. *?*

Non possiamo utilizzare la regola di $\forall$-G per derivare $\forall x Q(x)$ in quanto x rappresenta un elemento indefinito e non un elemento generico.

Vale la pena a questo punto di discutere un aspetto importante: cosa possiamo concludere quando non riusciamo ad ottenere una prova di $\Gamma \vdash A$? È sufficiente per concludere $\Gamma \not\models A$? Cosa ci assicura che non esista un'altra prova magari ottenuta applicando le regole in un altro ordine?

In effetti il fatto di non avere trovato una prova di $\Gamma \vdash A$ non è sufficiente per concludere $\Gamma \not\models A$. Per mostrare che $\Gamma \not\models A$ è necessario trovare un controesempio, *ovvero una interpretazione $\mathcal{I}$ tale che $\mathcal{I} \models \Gamma$ e $\mathcal{I} \not\models A$.*

Per esempio mostriamo che

$$\{\forall x(P(x) \to Q(x)), \exists x P(x)\} \not\models \forall x Q(x)$$

Dobbiamo trovare una interpretazione $\mathcal{I} = (D_{\mathcal{I}}, \alpha_{\mathcal{I}})$ in cui

1. $\forall x(P(x) \to Q(x))$ *vale;*
2. $\exists x P(x)$ *vale*
3. $\forall x Q(x)$ *non vale.*

Per esempio possiamo prendere il dominio $D_{\mathcal{I}} = \{a, b\}$ e la seguente interpretazione dei simboli

$$TS_{\mathcal{I}}(P) = \{a\}$$

$$TS_{\mathcal{I}}(Q) = \{a\}$$

2.3.4 Esercizi

Esercizio 2.17 *Provare $\vdash ((P \vee Q) \wedge \neg Q) \to P$. Utilizziamo il metodo per dimostrare le implicazioni, $\vdash ((P \vee Q) \wedge \neg Q) \to P$ segue da $(P \vee Q) \wedge \neg Q \vdash P$.*

1. $(P \vee Q) \wedge \neg Q$ *(Premessa*)*
2. $P \vee Q$ *(*and-elim. *da 1.)*
3. $\neg Q$ *(*and-elim. *da 1.)*

4. P (disj. syll. *da 2. e 3.)*

5. $((P \vee Q) \wedge \neg Q) \to P$ (imp*).*

Esercizio 2.18 *Provare* $\vdash (P \wedge Q \to R) \to (P \to (Q \to R))$*. Utilizzando il metodo per dimostrare le implicazioni sappiamo che*

$$\vdash (P \wedge Q \to R) \to (P \to (Q \to R)) \textit{ segue da } (P \wedge Q \to R) \vdash (P \to (Q \to R))$$

$$(P \wedge Q \to R) \vdash (P \to (Q \to R)) \textit{ segue da } (P \wedge Q \to R), P \vdash (Q \to R)$$

$$(P \wedge Q \to R), P \vdash (Q \to R) \textit{segue da } (P \wedge Q \to R), P, Q \vdash R.$$

Quindi abbiamo

1. P *(Premessa*)*
2. Q *(Premessa*)*
3. $P \wedge Q$ (and-intro *1. e 2.)*
4. $(P \wedge Q \to R)$ *(Premessa*)*
5. R (modus ponens *da 3. e 4.)*
6. $Q \to R$ (imp*)*
7. $P \to (Q \to R)$ (imp *)*
8. $(P \wedge Q \to R) \to (P \to (Q \to R))$ (imp*).*

Esercizio 2.19 *Provare che* $\vdash ((P \to Q) \to R) \to (\neg R \to (P \to \neg Q))$.

Le prove dei teoremi matematici possono essere molto complesse e lunghe. Di conseguenza è conveniente suddividere una prova in tante sottoprove più semplici da comprendere. Gli asserti che si dimostrano separatamente si chiamano comunemente *lemmi* o *proposizioni*. I lemmi sono proprietà che possono essere utilizzate in prove successive tutte le volte che si vuole e senza ridimostrarne la validità.

Esempio 2.20 (Modularità) *Supponiamo di volere dimostrare che* $(\forall x A) \vee (\forall x B) \to \forall x(A \vee B)$ *è valida. Abbiamo già dimostrato la validità di questa formula nell'Esercizio* **??**. *Facciamolo però vedere utilizzando le regole formali.*

Facciamo vedere che

- $\forall x A \vdash \forall x(A \vee B)$
  1. $\forall x A$ *(Premessa)*
  2. A *($\forall$-I da 1.)*
  3. $A \vee B$ (or-intro *da 2.)*
  4. $\forall x(A \vee B)$ *($\forall$-G da 3.)*

- $\forall x B \vdash \forall x (A \vee B)$.

    1. $\forall x B$ *(Premessa)*
    2. B *($\forall$-I da 1.)*
    3. $A \vee B$ *(*or-intro *da 2.)*
    4. $\forall x (A \vee B)$ *($\forall$-G da 3.)*

A questo punto possiamo utilizzare le dimostrazioni precedenti (senza doverle ridimostrare) nella prova di

$$\vdash (\forall x A) \vee (\forall x B) \rightarrow \forall x (A \vee B).$$

1. $(\forall x A) \vee (\forall x B)$ *(Premessa*)*
2. $(\forall x A) \vdash \forall x (A \vee B)$ *(Prova Precedente)*
3. $(\forall x B) \vdash \forall x (A \vee B)$ *(Prova Precedente)*
4. $\forall x (A \vee B)$ *(*per casi *da 1., 2. e 3.)*
5. $(\forall x A) \vee (\forall x B) \rightarrow \forall x (A \vee B)$ *(*imp*)*

Notate che la versione informale di questa prova vista nell'Esercizio **??** non è altro che una astrazione di questa prova formale, ovvero segue lo stesso schema logico ed gli stessi passaggi deduttivi, con la differenza che alcuni passaggi sono omessi e che non tutto è completamente giustificato in modo preciso.

References

[1] Kenneth H. Rosen. *Discrete Mathematics and its Applications.* McGraw-Hill International Editions, 1999.

[2] Daniel J. Velleman *How to Prove it.* Cambridge University Press, 1998.