Logica

1.75: Dimostrazioni in Teoria Assomatica degli Insiemi

Claudio Sacerdoti Coen

<sacerdot@cs.unibo.it>

Universitá di Bologna

29/09/2020

La tecnica del maestro di sci

Dimostrazioni:

- saranno oggetto di studio in questo corso, rigorosamente regolate da un linguaggio artificiale
- le prove informali sono approssimazioni meno verbose di quelle rigorose, con dettagli mancanti, a volte errate
- per studiarle logica useremo meta-dimostrazioni informali nella meta-logica
- solamente alla fine del corso saprete come si fanno le dimostrazioni
  (logica e meta-logica possono essere identiche)
- per il momento faremo come fa il maestro di sci: fate come me!

Per ogni

$\forall$-introduzione

Per dimostrare $\forall x.P(x)$ (per ogni x vale $P(x)$):

"sia x (un insieme) fissato; ..."

(i "..." sono una prova di $P(x)$)

$\forall$-eliminazione

Da un'ipotesi o un risultato intermedio $\forall x.P(x)$ potete concludere che P valga per ciò che volete.

Implicazione

$\Rightarrow$-introduzione

Per dimostrare $P \Rightarrow Q$:

"Assumo P (H). …"

("H") è il nome dell'ipotesi;
i "…" sono una prova di Q)

$\Rightarrow$-eliminazione

Da un'ipotesi o un risultato intermedio $P \Rightarrow Q$ e da un'ipotesi o un risultato intermedio P potete concludere che Q vale.

Implicazione

$\Rightarrow$-eliminazione (variante)

Da un'ipotesi o un risultato intermedio $P \Rightarrow Q$ di nome H, se volete concludere Q, potete procedere dicendo

"per H, per dimostare Q mi posso ridurre a dimostrare P"

Abbreviazioni

Per ogni tale che

"sia x tale che $P(x)$. ..."

abbrevia

"sia x (un insieme) fissato; assumo $P(x)$; ..."

per dimostrare $\forall x.P(x) \Rightarrow Q(x)$

Abbreviazioni

Da $H_1, \dots, H_n$

"da $H_1, \dots, H_n$ ho P (H)"

dove ogni H_i ha la forma $\forall \vec{x}.Q^i_1(\vec{x}) \Rightarrow \dots \Rightarrow Q^i_{n_i}(\vec{x})$ abbrevia l'applicazione di un numero arbitrario di regole di eliminazione del per ogni e dell'implicazione applicate a partire dalle ipotesi $H_1, \dots, H_n$ e tali per cui la conclusione finale sia P. Il nome H verrà poi usato quando P è una conclusione intermedia.

Quindi

"quindi" e sinonimi sono un modo per fare riferimento all'ultima ipotesi/risultato intermedio, magari omettendone del tutto il nome nel testo.

Se e soltanto se e definizioni

Espansione di definizioni

"*P*, ovvero *Q*" usato per espandere da qualche parte in P una definizione, ottenendo la frase Q

Esempio: $A \subseteq B$ ovvero $\forall X.(X \in A \Rightarrow X \in B)$.

Coimplica-introduzione

Per dimostrare $P \iff Q$ si dimostra sia $P \Rightarrow Q$ che $Q \Rightarrow P$.

Coimplica-eliminazione

L'ipotesi $P \iff Q$ può essere usata sia come un'ipotesi $P \Rightarrow Q$, che come un'ipotesi $Q \Rightarrow P$.

Enunciati e prove

Definizioni informali

L'enunciato di un teorema è ciò che vogliamo dimostrare. Si compone di un insieme di ipotesi e di una conclusione.

Una prova (informale) è una sequenza di passi che ci convince che la conclusione "valga" quando "valgono" le ipotesi.

Convenzione

Tutte le variabili di un enunciato che non sono introdotte da un per-ogni o da un esiste si considerano introdotte da dei per-ogni all'inizio dell'enunciato (l'ordine non è rilevante).

Esempio: l'enunciato $n + m = m + n$ abbrevia $\forall n, m. n + m = m + n$.

Enunciati e prove

Assiomi

Tutti gli assiomi sono sempre utilizzabili come ipotesi in qualunque momento.

Esplicitazione della conclusione e uso di “ovvio”

Esplicitazione della conclusione

Talvolta conviene esplicitare la conclusione corrente (cosa resta da dimostrare) attraverso “dobbiamo dimostrare P”.

Ovvio

“ovvio” si usa per indicare che il lettore è in grado di ricostruire la prova per conto suo (esempio: combinando le ipotesi)

Prime dimostrazioni informali

Riflessività del $\subseteq$.

Teorema: $X \subseteq X$.
Dimostrazione: Sia X un insieme. Dobbiamo dimostrare $X \subseteq X$, ovvero $\forall Y. Y \in X \Rightarrow Y \in X$. Sia Y un insieme tale che $Y \in X$ (H). Debbo dimostrare $Y \in X$. Ovvio per l'ipotesi H.
Qed.

Anti-simmetria del $\subseteq$.

Teorema: se $X \subseteq Y$ e $Y \subseteq X$ allora $X = Y$
Dimostrazione: siano X e Y insiemi tali che $X \subseteq Y$, ovvero $\forall Z, Z \in X \Rightarrow Z \in Y$, (H_1) e $Y \subseteq X$, ovvero $\forall Z, Z \in Y \Rightarrow Z \in X$, (H_2). Dobbiamo dimostare $X = Y$. Per l'assioma di estensionalità, è sufficiente dimostrare $\forall Z, Z \in X \iff Z \in Y$. Sia Z un insieme. $Z \in X \Rightarrow Z \in Y$ vale per H_1 e $Z \in Y \Rightarrow Z \in X$ vale per H_2. Qed.

Transitività del $\subseteq$.

Teorema: se $X \subseteq Y$ e $Y \subseteq Z$ allora $X \subseteq Z$
Dimostrazione: siano X, Y e Z insiemi tali che $X \subseteq Y$, ovvero $\forall A, A \in X \Rightarrow A \in Y$ (H_1) e $Y \subseteq Z$, ovvero $\forall A, A \in Y \Rightarrow A \in Z$ (H_2). Dobbiamo dimostrare $X \subseteq Z$, ovvero $\forall B, B \in X \Rightarrow B \in Z$. Sia B un insieme t.c. $B \in X$ (H_3). Da H_3 e H_1 ho $B \in Y$. Quindi, per H_2 ho $B \in Z$. Qed.

Assurdo

assurdo-eliminazione (ex-falso quodlibet)

Se ho dimostrato l'assurdo posso concludere qualunque cosa.

Negazione

Non P è un'abbreviazione per $P \Rightarrow$ assurdo.

Pertanto per dimostrare non P si assume che P valga e si dimostra l'assurdo.

Inoltre, data un'ipotesi (o risultato intermedio) non P e un'altra ipotesi o risultato intermedio P si conclude l'assurdo.

Il vuoto è sottoinsieme di qualunque cosa.

Teorema: $\emptyset \subseteq X$.

Dimostrazione: sia X un insieme. Dobbiamo dimostrare $\emptyset \subseteq X$, ovvero $\forall Z.Z \in \emptyset \Rightarrow Z \in X$. Sia Z un insieme t.c. $Z \in \emptyset$ (H). Per l'assioma dell'insieme vuoto $Z \notin \emptyset$. Quindi per H assurdo. Quindi $Z \in X$. Qed.

L'unico sottoinsieme del vuoto è il vuoto.

Teorema: se $X \subseteq \emptyset$ allora $X = \emptyset$.
Dimostrazione: sia X un insieme tale che $X \subseteq \emptyset$, ovvero $\forall Z, Z \in X \Rightarrow Z \in \emptyset$ (H). Dobbiamo dimostrare $X = \emptyset$. Per l'assioma di estensionalità possiamo ridurci a dimostrare $\forall Z, Z \in X \iff Z \in \emptyset$. Sia Z un insieme. Che $Z \in \emptyset \Rightarrow Z \in X$ è stato provato in precedenza (prova di $\emptyset \subseteq X$ per ogni X). Inoltre $Z \in X \Rightarrow Z \in \emptyset$ vale per H. Qed.

Congiunzione

$\wedge$-introduzione

Per dimostrare $P \wedge Q$ (P e Q) si dimostrano sia P che Q.

$\wedge$-eliminazione

Un'ipotesi o un risultato intermedio $P \wedge Q$ può essere usato sia come P che come Q. In alternativa, invece di concludere o assumere $P \wedge Q$ (H), si può direttamente concludere o assumere P (H_1) e Q (H_2).

Sull'intersezione con il vuoto

Teorema: $X \cap \emptyset = \emptyset$.
Dimostrazione: sia X un insieme. Dobbiamo dimostrare $X \cap \emptyset = \emptyset$, ovvero $\forall Z.Z \in X \cap \emptyset \iff Z \in \emptyset$. Sia Z un insieme. Che $Z \in \emptyset \Rightarrow Z \in X \cap \emptyset$ lo abbiamo già dimostrato ($\emptyset \subseteq Y$ per ogni Y). Dimostriamo $Z \in X \cap \emptyset \subseteq \emptyset$. Supponiamo $Z \in X \cap \emptyset$. Quindi, per il teorema che caratterizza l'intersezione binaria, $Z \in X$ (H_1) e $Z \in \emptyset$ (H_2). Quindi $Z \in \emptyset$. Qed.

Monotonia dell'intersezione

Teorema: $X \subseteq X' \Rightarrow X \cap Y \subseteq X' \cap Y$.
Dimostrazione: siano X e X' insiemi tali che $X \subseteq X'$, ovvero $\forall Z.Z \in X \Rightarrow Z \in X'$ (H_1). Dobbiamo dimostrare $X \cap Y \subseteq X' \cap Y$, ovvero $\forall W, W \in X \cap Y \Rightarrow W \in X' \cap Y$. Sia W un insieme t.c. $W \in X \cap Y$. Per il teorema che caratterizza l'intersezione binaria, $W \in X$ (H_2) e $W \in Y$ (H_3). Dobbiamo dimostrare $W \in X' \cap Y$. Per il teorema che caratterizza l'intersezione binaria, è sufficiente dimostrare $W \in X'$ e $W \in Y$. Per H_1 e H_2 si ha $W \in X'$. Per H_3 si ha $W \in Y$. Qed.

Disgiunzione

$\vee$-introduzione

Per dimostrare $P \vee Q$ (P o Q) basta dimostrare P oppure Q dichiarandolo:
"dimostro P" oppure "dimostro Q".

$\vee$-eliminazione

Data un'ipotesi o un risultato intermedio $P \vee Q$, si può proseguire nella dimostrazione per casi, una volta assumento che P valga e una volta che Q valga:
"procedo per casi:
caso in cui valga P (H): ...
caso in cui valga Q (H): ..."

Prime dimostrazioni informali

Monotonia dell'unione

Teorema: $X \subseteq X' \Rightarrow X \cup Y \subseteq X' \cup Y$.
Dimostrazione: siano X e X' insiemi tali che $X \subseteq X'$, ovvero $\forall Z. Z \in X \Rightarrow Z \in X'$ (H_1). Dobbiamo dimostrare $X \cup Y \subseteq X' \cup Y$, ovvero $\forall W, W \in X \cup Y \Rightarrow W \in X' \cup Y$. Sia W un insieme t.c. $W \in X \cup Y$. Per l'assioma di unione binaria, $W \in X$ o $W \in Y$. Procedo per casi.

- Caso $W \in X$ (H_2): dobbiamo dimostrare $W \in X' \cup Y$. Per l'assioma di intersezione binaria, è sufficiente dimostrare $W \in X'$ o $W \in Y$. Dimostro $W \in X'$. Per H_1 e H_2 si ha $W \in X'$.
- Caso $W \in Y$ (H_2): dobbiamo dimostrare $W \in X' \cup Y$. Per l'assioma di intersezione binaria, è sufficiente dimostrare $W \in X'$ o $W \in Y$. Dimostro $W \in Y$. Ovvio per H_2.

Qed.

Prime dimostrazioni informali

Risultati intermedi

Potete anche utilizzare una regola di introduzione per dimostrare un nuovo risultato intermedio, diverso dalla conclusione corrente, a cui date un nome per utilizzarlo in seguito, a patto che abbiate già a disposizione le premesse della regola.

Esempio: se avete a dispozione A (H_1) e B (H_2), potete dire "per H_1 e H_2 si ha $A \wedge B$ (H_3)" oppure "per H_1 si ha $A \vee C$ (H_3)"

Esempio

Teorema: $X \in Y \Rightarrow X \in Y \cup Z$.
Dimostrazione: siano X, Y e Z insiemi t.c. $X \in Y$ (H). Da H ho $X \in Y \vee X \in Z$. Quindi, per l'assioma dell'unione binaria, si ha $X \in Y \cup Z$. Qed.

Esiste

$\exists$-introduzione

Per dimostrare $\exists x.P(x)$ (esiste un x per cui vale $P(x)$):

"scelgo E e dimostro $P(E)$; ..."

(i "..." sono una prova di $P(E)$)

E può essere un'espressione qualsiasi (es. $B \cap C$).

$\exists$-eliminazione

Da un'ipotesi o un risultato intermedio $\exists x.P(x)$ potete procedere nella prova dicendo
"sia x t.c. $P(x)$ (H)"

x deve essere una variabile non in uso in nessuna ipotesi o nella conclusione

Prime dimostrazioni informali

Esempio

Teorema: $X \in \bigcup F \Rightarrow \exists U.(U \in F \wedge U \neq \emptyset)$.
Dimostrazione: siano X e F insiemi t.c. $X \in \bigcup F$. Quindi, per il teorema che caratterizza l'intersezione, $\exists Y.(Y \in F \wedge X \in Y)$. Sia Y t.c. $Y \in F$ (H_1) e $X \in Y$ (H_2). Debbo dimostrare $\exists U.(U \in F \wedge U \neq \emptyset)$. Scelgo Y e dimostro $Y \in F \wedge Y \neq \emptyset$.

- $Y \in F$ vale per H_1.
- Debbo dimostrare $Y \neq \emptyset$. Suppongo $Y = \emptyset$ (K). Dobbiamo dimostrare l'assurdo. Per l'assioma di estensionalità, K e H_2, $X \in \emptyset$. Quindi, per l'assioma dell'insieme vuoto, ho un assurdo.

Qed.