Logica per l'informatica
Lista teoremi e assiomi

Andrea Malvezzi

10 ottobre 2024

Contents

1 Assiomi **3**
1.1 Assioma di estensionalità 3
1.1.1 Esempio 3
1.1.2 Nota Bene 3
1.2 Assioma di separazione o di comprensione 4
1.2.1 Esempio 4
1.3 Assioma dell'insieme vuoto 4
1.3.1 Esempio 4
1.4 Assioma dell'unione 5
1.4.1 Esempio 5
1.5 Assioma del singoletto 5
1.6 Assioma dell'infinito 6
1.7 Assioma dell'insieme potenza 6
1.8 Assioma di regolarità o di fondazione 6

2 Teoremi **6**

3 Definizioni **6**
3.1 Definizione di numeri naturali 6
3.1.1 Esempio 7

Introduzione

A seguire una lista di tutti i teoremi e di tutti gli assiomi utili alle dimostrazioni di laboratorio, con casi di utilizzo e spiegazioni approfondite.

1 Assiomi

1.1 Assioma di estensionalità

Due insiemi sono uguali quando contengono gli stessi elementi:

$$X, Y.(X = Y \Leftrightarrow \forall Z.(Z \in X \Leftrightarrow Z \in Y)) \tag{ax. 1}$$

Questo teorema si utilizza quando occorre indagare sull'uguaglianza tra due insiemi: potrei usarlo sia per mostrare che due insiemi siano uguali, oppure per mostrare che NON lo siano.

1.1.1 Esempio

$$A = \{1, 2\}$$
$$B = \{1\}$$

$A = B$? 1 è presente in entrambi gli insiemi, ma 2 solamente in A.

1.1.2 Nota Bene

Essendo questo un assioma "a due direzioni" (un insieme è uguale a un altro se hanno gli stessi elementi E VICEVERSA) in Lean si potrebbe realizzare DUE assiomi (uno per verso, evitando il sse), per semplificarne l'utilizzo:

axiom ax_extensionality1: $\forall A, B.(\forall Z, Z \in A \Leftrightarrow B) \Rightarrow A = B$
axiom ax_extensionality2: $\forall A, B, A = B \Rightarrow (\forall Z, Z \in A \Leftrightarrow B)$

1.2 Assioma di separazione o di comprensione

Questo assioma permette, partendo da un insieme A, di formare un sottoinsieme B in modo tale che quest'ultimo soddisfi una certa proprietà $P(X)$.

$$A, \exists B, x.(x \in B \Leftrightarrow x \in A \wedge P(x)) \tag{ax. 2}$$

B equivale al sottoinsieme che vogliamo creare, quindi possiamo scriverlo come:

$$B = \{x \in A : P(x)\} \tag{1}$$

Stiamo quindi dicendo che avendo un insieme A, esiste un insieme B che contiene elementi di A tali per cui valga la proprietà specificata come $P(x)$.

1.2.1 Esempio

Avendo un insieme A contenente alcuni numeri naturali, voglio creare un insieme B contenente solamente i numeri pari di A. Quindi:

$$A = \{1, 2, 3, 4, 5, 6, 7\}$$
$$P(x) = \text{"x è pari."}$$
$$B = \{x \in A : P(x)\}, \text{ quindi:}$$
$$B = \{2, 4, 6\}$$

1.3 Assioma dell'insieme vuoto

Avendo un insieme X vuoto, allora non ci sono elementi contenuti al suo interno:

$$\exists X, Z.(Z \notin X) \tag{ax. 3}$$

Questo assioma risulta utile nelle dimostrazioni per assurdo.

1.3.1 Esempio

L'insieme vuoto comprende se stesso?

$$\emptyset \in \emptyset?$$
$$\text{applichiamo l'assioma del vuoto: } \exists X, \forall z.(z \notin X)$$
$$\text{sapendo che l'insieme vuoto è per definizione: } \forall z.(z \notin \emptyset)$$
$$\text{abbiamo, sostituendo alla z l'insieme vuoto: } \forall \emptyset.(\emptyset \notin \emptyset)$$

Abbiamo quindi dimostrato che l'insieme vuoto non contiene sé stesso.

1.4 Assioma dell'unione

Consideriamo un insieme F come una scatola contenente n insiemi che vogliamo unire tra loro.
Allora esiste un insieme detto **insieme unione** X contenente tutti gli elementi dei sottinsiemi di F.
Quindi definendo $X = \cup F$, i membri di $\cup F$ saranno tutti i membri dei membri di F.
Si usa quando si vuole effettuare un'unione tra n insiemi e la sua proposizione è la seguente:

$$\forall F, \exists X, \forall Z.(Z \in X \Leftrightarrow \exists Y, (Y \in F \wedge Z \in Y)) \qquad \text{(ax. 4)}$$

1.4.1 Esempio

Avendo un insieme A contenente 3 sottoinsiemi che si vogliono unire tra loro, allora:

$$A = \{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$$
$$X = \cup A = \{z : \exists Y \in A : z \in Y\}$$
$$\text{quindi: } X = \{1, 2, 3, 4, 5, 6\}$$

1.5 Assioma del singoletto

Avendo un insieme X, esiste un insieme Y indicato come $\{X\}$ per cui un elemento Z appartiene ad Y se e solo se Z è X:

$$X, Z.(Z \in \{X\} \Leftrightarrow Z = X) \qquad \text{(ax. 5)}$$

Questo assioma risulta molto utile quando si vuole formare un insieme contenente solamente un elemento, detto **singoletto**.
Si usa inoltre per comporre insiemi più complessi (ma pur sempre finiti), combinando tra loro diversi singoletti.
Ad esempio, per formare la coppia (a, b) si potrebbero prima creare $\{a\}$ e $\{b\}$, e poi unirli tramite l'assioma dell'unione (ax. 4).

1.6 Assioma dell'infinito

Esiste un insieme che contiene ALMENO tutti gli encoding dei numeri meta-naturali. Questo insieme potrebbe quindi contenere anche più elementi di quelli che stiamo cercando.

$$\exists Y.(\emptyset \in Y \land \forall N.(N \in Y \Rightarrow N \cup \{N\} \in Y)) \qquad \text{(ax. 6)}$$

Il fatto che tale insieme possa contenere anche più elementi di quelli che stiamo cercando è dovuto alla presenza di una implicazione logica invece che di una COimplicazione.
L'insieme risultante si potrà poi filtrare mediante Assioma di separazione (ax. 2) per ridursi gradualmente sempre di più al sottoinsieme dei numeri naturali.

1.7 Assioma dell'insieme potenza

Questo assioma risulta particolarmente utile quando si considerano insiemi infiniti.
Afferma che preso un insieme di partenza, allora esiste un altro insieme, detto **insieme potenza**, contenente tutti i suoi sottoinsiemi:

$$A, \exists Y, z.(z \in Y \Leftrightarrow z \subseteq X) \qquad \text{(ax. 7)}$$

Y si può rappresentare come $P(x)$ o come 2^x ed è detto **insieme potenza** o **insieme delle parti**.

1.8 Assioma di regolarità o di fondazione

2 Teoremi

3 Definizioni

3.1 Definizione di numeri naturali

Per ogni meta-numero naturale n occorre definire un insieme [[n]] da identificare con tale numero n. Uno dei tanti modi per definire tali numeri, garantendo allo stesso tempo che questi siano distinti (e molte altre cose)è la seguente:

$$[[0]] := \emptyset$$
$$[[n+1]] := [[n]] \cup \{[[n]]\}$$

Dove $[[n]]$ indica la codifica del meta-numero naturale n, ottenuta unendo l'insieme corrispondente ad $n-1$ a sé stesso.

3.1.1 Esempio

$$[[0]] = \emptyset$$
$$[[1]] = \{\emptyset\}$$
$$[[2]] = \{\emptyset, \{\emptyset\}\}$$
$$[[3]] = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$

Dove l'insieme corrispondente a $n = 0$ si ottiene unendo l'insieme vuoto a sé stesso.