UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Metodi matematici per l'Informatica

Modulo 15 – Il sistema di Hilbert

Docente: Pietro Cenciarelli

Il sistema di Hilbert

Sistema logico assiomatico:

assiomi (proposizioni fondanti)

regole di inferenza

In un'algebra di Boole, per ogni A e B esiste un elemento $B^A = \overline{A} \vee B$ tale che $B^A \wedge A \leq B$, ovvero $(B^A \wedge A) \vee B = B$

$$[(\overline{A} \vee B) \wedge A] \vee B = [(\overline{A} \vee B) \vee B] \wedge (A \vee B)$$
$$= (\overline{A} \vee B) \wedge (A \vee B)$$
$$= (\overline{A} \wedge A) \vee B = \perp \vee B = B$$

Il sistema di Hilbert

Sistema logico assiomatico:

assiomi (proposizioni fondanti)

regole di inferenza

$$A \vee (B \vee C) = (A \vee B) \vee C$$

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$

$$A \vee \bot = A$$

...

$$\frac{A = B}{B = A} \qquad \frac{A = B \quad B = C}{A = C} \qquad \ldots$$

$$[(\overline{A} \vee B) \wedge A] \vee B = [(\overline{A} \vee B) \vee B] \wedge (A \vee B)$$

$$= (\overline{A} \vee B) \wedge (A \vee B)$$

$$= (\overline{A} \wedge A) \vee B = \bot \vee B = B$$

Il sistema di Hilbert

assiomi

David Hilbert
1862 - 1943

$A \rightarrow A$

$B \rightarrow (A \rightarrow B)$

$(A \rightarrow (B \rightarrow C)) \rightarrow (A \rightarrow B) \rightarrow (A \rightarrow C)$

$(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$

… *schemi* di assioma!

$(P \rightarrow Q) \rightarrow (P \rightarrow Q)$ *istanza* del primo schema

$(P \wedge Q) \rightarrow ((Q \rightarrow R) \rightarrow (P \wedge Q))$ *istanza* del secondo

…

Il sistema di Hilbert

regole di inferenza

David Hilbert
1862 - 1943

Modus ponens $\dfrac{A \quad A \to B}{B}$

$A \to A$

$B \to (A \to B)$

$(A \to (B \to C)) \to (A \to B) \to (A \to C)$

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

Il sistema di Hilbert

dimostrazioni (formalmente)

Una *dimostrazione* di una proposizione A è una sequenza di proposizioni, di cui A è l'ultima, ciascuna delle quali è una istanza di assioma o è ottenuta per modus ponens da due proposizioni che la precedono.

$$\dfrac{A \to (A \to A) \qquad \dfrac{A \to ((A \to A) \to A) \qquad (A \to ((A \to A) \to A)) \to (A \to (A \to A)) \to (A \to A)}{(A \to (A \to A)) \to (A \to A)}}{A \to A}$$

Il sistema di Hilbert

dimostrazioni (formalmente)

Ax1 $B \to (A \to B)$

Ax2 $(A \to (B \to C)) \to (A \to B) \to (A \to C)$

Ax3 $(\neg A \to \neg B) \to (B \to A)$

1, Ax1 $A \to ((A \to A) \to A)$

2, Ax2 $(A \to ((A \to A) \to A)) \to (A \to (A \to A)) \to (A \to A)$

3, MP 1 2 $(A \to (A \to A)) \to (A \to A)$

4, Ax1 $A \to (A \to A)$

5, MP 3 4 $A \to A$

Il sistema di Hilbert

dimostrazioni (formalmente)

Una *dimostrazione* di una proposizione A è una sequenza di proposizioni, di cui A è l'ultima, ciascuna delle quali è un'istanza di assioma o è ottenuta per modus ponens da due proposizioni che la precedono.

Una *dimostrazione* di una proposizione A da un insieme di premesse $\Gamma = \{B_1, B_2, \dots B_n\}$ è una sequenza di proposizioni, di cui A è l'ultima, ciascuna delle quali è un'istanza di assioma, o una proposizione in Γ, o è ottenuta per modus ponens da due proposizioni che la precedono.

$B_1, B_2, \dots B_n \vdash A$ *sequente*

vuol dire: *esiste una dimostrazione di* A *dalle premesse in* $B_1, B_2, \dots B_n$

($\vdash A$ se non ci sono premesse)

Deduzione

$C_1, C_2, \ldots C_n, A \vDash B$ se e solo se $C_1, C_2, \ldots C_n \vDash A \rightarrow B$

(*deduzione semantica*)

?

$C_1, C_2, \ldots C_n, A \vdash B$ se e solo se $C_1, C_2, \ldots C_n \vdash A \rightarrow B$

(…si deriverebbe immediatamente $\dfrac{A \vdash A}{\vdash A \rightarrow A}$)

Deduzione

☺

$$C_1, C_2, \ldots C_n, A \vdash B \quad \Leftarrow \quad C_1, C_2, \ldots C_n \vdash A \to B$$

1.	...		1.	...
2.	...		2.	...
⋮			⋮	
m.	...		m.	...
m+1.	$A \to B$		m+1.	$A \to B$
m+2.	A	(ipotesi)		
m+3.	B	(MP m+1, m+2)		

Deduzione

$$C_1, C_2, \ldots C_n, A \vdash B \quad \Longrightarrow \quad C_1, C_2, \ldots C_n \vdash A \rightarrow B$$

1. B.
2. …

⋮

m. …

m+1. B

per induzione su m

Se m = 0…

- $B = A$ oppure
- $B = C_i$ oppure
- B è un assioma

Deduzione

$C_1, C_2, \ldots C_n, A \vdash B \quad \Longrightarrow \quad C_1, C_2, \ldots C_n \vdash A \to B$

1. B

per induzione su m

Se m = 0…

$\vdash A \to A$ e dunque

$C_1, C_2, \ldots C_n \vdash A \to A$

✔ $B = A$ oppure

$B = C_i$ oppure

B è un assioma

Deduzione

$C_1, C_2, \ldots C_n, A \vdash B \quad \Longrightarrow \quad C_1, C_2, \ldots C_n \vdash A \rightarrow B$

1. B
2. $B \rightarrow (A \rightarrow B)$
3. $(A \rightarrow B)$

per induzione su m

Se m = 0…

✔ $B = A$ oppure

✔ $B = C_i$ oppure

B è un assioma

Deduzione

$C_1, C_2, \ldots C_n, A \vdash B \quad \Longrightarrow \quad C_1, C_2, \ldots C_n \vdash A \rightarrow B$

1. B
2. $B \rightarrow (A \rightarrow B)$
3. $(A \rightarrow B)$

per induzione su m

Se m = 0… ☺

✔ B = A oppure

✔ $B = C_i$ oppure

✔ B è un assioma

Deduzione

$C_1, C_2, \ldots C_n, A \vdash B \quad \Longrightarrow \quad C_1, C_2, \ldots C_n \vdash A \rightarrow B$

per induzione su m

Se m = 0… ☺

Altrimenti

- ✔ B = A oppure
- ✔ B = C_i oppure
- ✔ B è un assioma oppure

  B è ottenuto per MP

Deduzione

$C_1, C_2, \ldots C_n, A \vdash B \quad \Longrightarrow \quad C_1, C_2, \ldots C_n \vdash A \rightarrow B$

1. …
$\vdots$
i. C
$\vdots$
j. $C \rightarrow B$
$\vdots$
m+1. B (MP i, j) $i, j \leq m$

per induzione su m

Se m = 0… ☺

Altrimenti B è ottenuto per MP

Per ipotesi induttiva

$C_1, C_2, \ldots C_n \vdash A \rightarrow C$

$C_1, C_2, \ldots C_n \vdash A \rightarrow (C \rightarrow B)$

Deduzione

$$C_1, C_2, \dots C_n, A \vdash B \quad \Longrightarrow \quad C_1, C_2, \dots C_n \vdash A \to B$$

per induzione su m

Se m = 0… ☺

Altrimenti B è ottenuto per MP

Per ipotesi induttiva

$C_1, C_2, \dots C_n \vdash A \to C$

$C_1, C_2, \dots C_n \vdash A \to (C \to B)$

$A \to C$

$A \to (C \to B)$

$(A \to (C \to B)) \to ((A \to C) \to (A \to B))$

(assioma 2)

$(A \to C) \to (A \to B)$

$A \to B$

Deduzione

☺

$C_1, C_2, \ldots C_n, A \vdash B \quad \Longrightarrow \quad C_1, C_2, \ldots C_n \vdash A \rightarrow B$

$A \rightarrow B, B \rightarrow C, A \vdash A$	*ipotesi*
$A \rightarrow B, B \rightarrow C, A \vdash A \rightarrow B$	*ipotesi*
$A \rightarrow B, B \rightarrow C, A \vdash B$	MP
$A \rightarrow B, B \rightarrow C, A \vdash B \rightarrow C$	*ipotesi*
$A \rightarrow B, B \rightarrow C, A \vdash C$	MP
$A \rightarrow B, B \rightarrow C \vdash A \rightarrow C$	*deduzione*
$A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)$	*deduzione*
$\vdash (A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$	*deduzione*

Deduzione

$C_1, C_2, \ldots C_n, A \vdash B$ se e solo se $C_1, C_2, \ldots C_n \vdash A \rightarrow B$

A

$A \rightarrow B$

B

$B \rightarrow C$

C

$A \rightarrow C$

$(B \rightarrow C) \rightarrow (A \rightarrow C)$

$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$

non è una dimostrazione di

$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$ ...

Deduzione

$C_1, C_2, \ldots C_n, A \vdash B$ se e solo se $C_1, C_2, \ldots C_n \vdash A \rightarrow B$

$A \rightarrow B, B \rightarrow C, A \vdash A$

$A \rightarrow B, B \rightarrow C, A \vdash A \rightarrow B$

$A \rightarrow B, B \rightarrow C, A \vdash B$

$A \rightarrow B, B \rightarrow C, A \vdash B \rightarrow C$

$A \rightarrow B, B \rightarrow C, A \vdash C$

$A \rightarrow B, B \rightarrow C \vdash A \rightarrow C$

$A \rightarrow B \vdash (B \rightarrow C) \rightarrow (A \rightarrow C)$

$\vdash (A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$

è *una dimostrazione di*

$\vdash (A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$!

Un calcolo di sequenti

$C_1, C_2, \ldots C_n, A \vdash B$ se e solo se $C_1, C_2, \ldots C_n \vdash A \rightarrow B$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash A \rightarrow B}{\Gamma \vdash B}$$

$$\boxed{\begin{array}{l} \\ \\ m. \;\; A \end{array}} \qquad \Gamma \vdash A$$

$$\boxed{\begin{array}{l} \\ \\ n. \;\; A \rightarrow B \end{array}} \qquad \Gamma \vdash A \rightarrow B$$

m+n+1. B MP m, m+n

Un calcolo di sequenti

$C_1, C_2, \ldots C_n, A \vdash B$ se e solo se $C_1, C_2, \ldots C_n \vdash A \rightarrow B$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash A \rightarrow B}{\Gamma \vdash B} \qquad \frac{\Gamma \vdash \neg A \rightarrow \neg B}{\Gamma \vdash B \rightarrow A}$$

contrapposizione

$\Gamma \vdash \neg A \rightarrow \neg B$

n. $\neg A \rightarrow \neg B$

n+1. $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$ *AX3*

n+2. $B \rightarrow A$ MP n, n+1

Un calcolo di sequenti

$C_1, C_2, \ldots C_n, A \vdash B$ se e solo se $C_1, C_2, \ldots C_n \vdash A \to B$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B} \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash A \to B}{\Gamma \vdash B} \qquad \frac{\Gamma \vdash \neg A \to \neg B}{\Gamma \vdash B \to A}$$

$$\frac{\Gamma \vdash A \to B}{\Gamma, A \vdash B} \quad ☺ \qquad \frac{\dfrac{\Gamma \vdash A \to B}{\Gamma, A \vdash A \to B} \quad \Gamma, A \vdash A}{\Gamma, A \vdash B}$$

UNITELMA SAPIENZA
SAPIENZA Università di Roma
Dipartimento di Informatica

Un calcolo di sequenti

(*logica classica*)

$$
\cfrac{\cfrac{\cfrac{\cfrac{\neg\neg A \vdash \neg\neg A \qquad \neg\neg A \vdash \neg\neg A \to (\neg\neg\neg\neg A \to \neg\neg A)}{\neg\neg A \vdash \neg\neg\neg\neg A \to \neg\neg A}}{\neg\neg A \vdash \neg A \to \neg\neg\neg A}}{\neg\neg A \vdash \neg\neg A \to A} \qquad \neg\neg A \vdash \neg\neg A}{\cfrac{\neg\neg A \vdash A}{\vdash \neg\neg A \to A}}
$$

Un calcolo di sequenti

(*logica classica*)

$$
\dfrac{\dfrac{\dfrac{\dfrac{A,\ \neg A \vdash A \qquad \dfrac{\dfrac{A,\ \neg A \vdash \neg A \qquad A,\ \neg A \vdash \neg A \to (\neg B \to \neg A)}{A,\ \neg A \vdash \neg B \to \neg A} \qquad A,\ \neg A \vdash (\neg B \to \neg A) \to (A \to B)}{A,\ \neg\neg A \vdash A \to B}}{A,\ \neg A \vdash B}}{A \vdash \neg A \to B}}{\vdash A \to (\neg A \to B)}
$$

$$
\vdash {\color{red} A \to (A \vee B)}
$$

Correttezza e completezza

$\vdash A$ *se e solo se* $\models A$