

L'uso della logica modale per fornire una semantica classica alla logica intuizionista

Gabriele Vanoni

Politecnico di Milano

15 Dicembre 2016

Sommario

- 1 La logica intuizionista
- 2 La traduzione di Gödel-McKinsey-Tarski

La logica intuizionista

Le motivazioni

Dalla seconda metà dell'800 le **dimostrazioni** hanno perso in generale contenuto **computazionale**.

Le dimostrazioni spesso non sono **costruttive**, provano l'esistenza di un oggetto ma non danno un **algoritmo** per costruirlo.

Brouwer capisce che questa mancanza è data dalla legge del **terzo escluso**:

$$\vdash p \vee \neg p$$

Esempio

Non possiamo asserire che $\forall n. f(n) = 0 \vee \exists n. f(n) \neq 0$.

La corrispondenza di Curry-Howard-Lambek (cenni)

- La logica intuizionista diventa fondamentale nel secondo dopoguerra nella teoria dei **linguaggi di programmazione**.
- Infatti viene stabilita una **corrispondenza sintattica** tra le dimostrazioni in **deduzione naturale** e i programmi del **lambda-calcolo tipato semplice**.
- La corrispondenza tra prove e programmi segna la nascita della moderna **teoria dei tipi** (Martin-Lof, Coquand), dei **linguaggi funzionali** (Lisp, Haskell) e dei **proof-assistant** (Coq, HOL).
- La corrispondenza viene poi estesa alla **teoria delle categorie** e in particolare alle Categorie Cartesiane Chiuse (CCC) aventi come oggetti i tipi (formule) e come morfismi i termini (dimostrazioni).

L'interpretazione BHK

- Una dimostrazione di $A \wedge B$ è data presentando una dimostrazione di A e una dimostrazione di B .
- Una dimostrazione di $A \vee B$ è data presentando una dimostrazione di A o una dimostrazione di B .
- Una dimostrazione di $A \rightarrow B$ è una costruzione che permette di trasformare qualsiasi dimostrazione di A in una dimostrazione di B .
- L'assurdo \perp non ha dimostrazione.
- Una dimostrazione di $\neg A$ è una costruzione che trasforma ogni ipotetica dimostrazione di A in una dimostrazione di \perp (ovvero una dimostrazione di $A \rightarrow \perp$).

Ovviamente queste regole non forniscono una semantica formale, lasciando generici i concetti di dimostrazione e costruzione.

Un calcolo alla Hilbert per **Int**

Heyting e Kolmogorov proposero per **Int** un calcolo alla Hilbert con i seguenti schemi di assiomi:

- ① $P \rightarrow (Q \rightarrow P)$
- ② $(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$
- ③ $P \wedge Q \rightarrow P$
- ④ $P \wedge Q \rightarrow Q$
- ⑤ $P \rightarrow (Q \rightarrow P \wedge Q)$
- ⑥ $P \rightarrow P \vee Q$
- ⑦ $Q \rightarrow P \vee Q$
- ⑧ $(P \rightarrow R) \rightarrow ((Q \rightarrow R) \rightarrow (P \vee Q \rightarrow R))$
- ⑨ $\perp \rightarrow P$

e la regola di inferenza Modus Ponens.

La logica **Int** risulta quindi essere un sottoinsieme proprio della logica **L**, avendo questa come unico assioma in più il **principio del terzo escluso** $P \vee (P \rightarrow \perp)$.

La semantica di Kripke per Int

- Dobbiamo immaginare che se una proposizione p non è vera in un istante x , non è detto che non lo diverrà in un futuro y . La conoscenza evolve cioè da uno stato all'altro. Tuttavia ciò che è vero ovviamente nel futuro rimane vero.
- Possiamo quindi formalizzare il ragionamento costruendo un **frame** di Kripke $\mathfrak{F} = \langle \mathfrak{W}, \mathfrak{R} \rangle$ con \mathfrak{W} insieme non vuoto dei mondi e $\mathfrak{R} \subseteq \mathfrak{W} \times \mathfrak{W}$ relazione di accessibilità fra i mondi, su cui verranno costruiti i relativi **modelli** $\mathfrak{M} = \langle \mathfrak{F}, \mathfrak{V} \rangle$ assegnando una funzione di valutazione $\mathfrak{V} : \text{Var}\mathcal{L} \rightarrow \mathcal{P}(\mathfrak{W})$.
- Per dare il significato ad R di “tempo”, richiediamo che \mathfrak{R} sia un ordine parziale, ovvero sia **transitiva**, **riflessiva** e **antisimmetrica**.
- Richiediamo inoltre che la funzione di valutazione \mathfrak{V} garantisca che la verità venga mantenuta nel tempo, ovvero che se $x \in \mathfrak{V}(p)$ e $x\mathfrak{R}y$ allora $y \in \mathfrak{V}(p)$ per ogni $p \in \text{Var}\mathcal{L}$.

La semantica di Kripke per **Int** (continua)

La valutazione delle formule su un mondo x di un modello $\mathfrak{M} = \langle \mathfrak{F}, \mathfrak{V} \rangle$ costruito su un frame $\mathfrak{F} = \langle \mathfrak{W}, \mathfrak{R} \rangle$ procede dunque per induzione sulla costruzione della formula:

- $(\mathfrak{M}, x) \models p$ sse $x \in \mathfrak{V}(p)$
- $(\mathfrak{M}, x) \models P \wedge Q$ sse $(\mathfrak{M}, x) \models P$ e $(\mathfrak{M}, x) \models Q$
- $(\mathfrak{M}, x) \models P \vee Q$ sse $(\mathfrak{M}, x) \models P$ o $(\mathfrak{M}, x) \models Q$
- $(\mathfrak{M}, x) \models P \rightarrow Q$ sse per ogni y tale che $x\mathfrak{R}y$ se $(\mathfrak{M}, y) \models P$ allora $(\mathfrak{M}, y) \models Q$
- $(\mathfrak{M}, x) \not\models \perp$

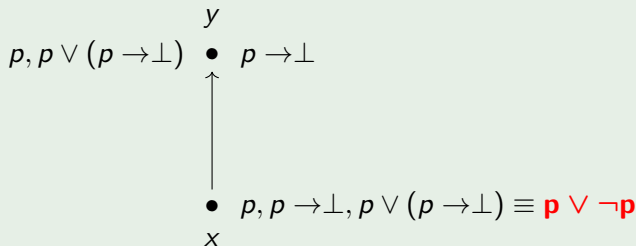
segue quindi che $(\mathfrak{M}, x) \models \neg P$ sse per ogni y tale che $x\mathfrak{R}y$ $(\mathfrak{M}, y) \not\models P$.

Si verifica facilmente per induzione sulla complessità della formula che con questa costruzione se P è vera in x e $x\mathfrak{R}y$ allora P è vera anche in y .

Esempio: il principio del terzo escluso

Esempio

Ci basta trovare un modello in cui $p \vee \neg p \equiv p \vee (p \rightarrow \perp)$ non sia valida. Consideriamo un frame con soli due mondi x e y , $\mathfrak{R} = \{(x, x), (x, y), (y, y)\}$, un'unica lettera proposizionale p e $\mathfrak{V}(p) = \{y\}$. Rappresentiamo a sinistra del mondo ciò che è vero mentre a destra ciò che non lo è (non è detto che sia falso!).



La traduzione di Gödel-McKinsey-Tarski

L'idea

- Abbiamo fornito una semantica formale ad **Int** utilizzando un frame di Kripke con particolari proprietà, che intuitivamente rispecchiano il possibile aumento di **conoscenza** nel tempo.
- Vorremmo ora formalizzare l'**interpretazione BHK** che faceva invece riferimento alla **dimostrabilità**.
- L'idea è quella di utilizzare l'operatore modale \Box con il significato di "è dimostrabile".
- Capiamo che per assegnare la corretta semantica all'operator box, necessitiamo di una teoria più forte di **K**, in particolare avremo bisogno che la dimostrabilità di A implichi A e che la dimostrabilità di A implichi la dimostrabilità della sua dimostrabilità, ovvero devono valere gli **assiomi**:
 - **T**: $\Box A \rightarrow A$
 - **4**: $\Box A \rightarrow \Box \Box A$
- Faremo vedere dunque una traduzione di **Int** in **S4**, ovvero la logica determinata dai frame **riflessivi** e **transitivi**.

Una nota sul concetto di dimostrabilità

La **semantica** che diamo all'operatore \Box è quella di “**dimostrabilità**” in un senso **informale**, non in un particolare sistema formale **S** come potrebbe essere **PA**. Infatti avremmo che in **S**:

$$\Box(0 \neq 0) \rightarrow 0 \neq 0 \text{ (assioma } \mathbf{T} \text{ e sostituzione)}$$

da cui deriviamo

$$\neg \Box(0 \neq 0) \text{ (essendo il conseguente falso),}$$

che asserisce la **coerenza** di **S**, andando contro il **secondo teorema di incompletezza**.

Per considerare la dimostrabilità in un sistema formale dobbiamo considerare non **S4**, ma la logica **GL** in cui l'operatore \Box ha le stesse proprietà del predicato “è dimostrabile in **S**” definito nella dimostrazione dei **teoremi di incompletezza**.

La traduzione

Diamo quindi una traduzione $T: For\mathcal{L} \rightarrow For\mathcal{ML}$ ottenuta dall'interpretazione BHK sostituendo alla parola “dimostrazione” o “costruzione” l'operatore \Box .

Traduzione GMT

- $T(p) = \Box p$
- $T(P \wedge Q) = T(P) \wedge T(Q)$
- $T(P \vee Q) = T(P) \vee T(Q)$
- $T(P \rightarrow Q) = \Box(T(P) \rightarrow T(Q))$
- $T(\perp) = \Box \perp$

Ciò che vogliamo dimostrare è che per ogni formula $P \in For\mathcal{L}$:

$$P \in \mathbf{Int} \text{ se e solo se } T(P) \in \mathbf{S4}.$$

Lemma preliminare

Abbiamo bisogno di alcune definizioni e lemmi preliminari.

Lemma

Sia \mathfrak{M} un modello costruito su un frame $\mathfrak{F} = \langle \mathfrak{W}, \mathfrak{R} \rangle$ transitivo. Allora per ogni mondo x in \mathfrak{W} se $(\mathfrak{M}, x) \models \Box P$ allora per ogni y tale che $x\mathfrak{R}y$ $(\mathfrak{M}, y) \models \Box P$.

Dimostrazione.

Supponiamo per assurdo che in un mondo y tale che $x\mathfrak{R}y$ $(\mathfrak{M}, y) \not\models \Box P$. Allora dovrebbe esistere un mondo z tale che $y\mathfrak{R}z$ in cui $(\mathfrak{M}, z) \not\models P$. Per la transitività di \mathfrak{R} $x\mathfrak{R}z$ e dunque contraddiremmo l'ipotesi. □

Frame skeleton

Definizione

Il frame quoziente di un frame transitivo $\mathfrak{F} = \langle \mathfrak{W}, \mathfrak{R} \rangle$ rispetto alla relazione di cluster \approx , cioè $\langle \mathfrak{W}/\approx, \mathfrak{R}/\approx \rangle$ essendo:

- \mathfrak{W}/\approx l'insieme delle classi di equivalenza di \mathfrak{W} rispetto a \approx
- $C(x)\mathfrak{R}/\approx C(y)$ se e solo se $x\mathfrak{R}y$

è chiamato frame skeleton di \mathfrak{F} e indicato con $\rho\mathfrak{F} = \langle \rho\mathfrak{W}, \rho\mathfrak{R} \rangle$.

Risulta evidente che un frame skeleton è **antisimmetrico**, **transitivo** e mantiene l'eventuale **riflessività** di \mathfrak{R} .

Costruzione del modello skeleton

Torniamo alla logica **S4**. Consideriamo un suo modello

$\mathfrak{M} = \langle \mathfrak{F}, \mathfrak{V} \rangle$. Sappiamo che è costruito su un frame

$\mathfrak{F} = \langle \mathfrak{W}, \mathfrak{R} \rangle$ transitivo e riflessivo (preordinato).

Costruiamo il frame skeleton $\rho\mathfrak{F}$ (che è parzialmente ordinato, essendo transitivo, riflessivo e antisimmetrico) e assegniamogli la valutazione $\rho\mathfrak{V}$ così definita:

$$\rho\mathfrak{V}(p) = \{C(x) : (\mathfrak{M}, x) \models \Box p\}.$$

Osserviamo che per il lemma precedente la valutazione è trasparente rispetto alla scelta del mondo all'interno del cluster e che inoltre rispetta la proprietà per cui se $C(x) \in \rho\mathfrak{V}(p)$ e $C(x)\mathfrak{R}/\approx C(y)$ allora $C(y) \in \rho\mathfrak{V}(p)$ per ogni $p \in \text{Var}\mathcal{L}$.

Chiamiamo skeleton di \mathfrak{M} il modello $\rho\mathfrak{M} = \langle \rho\mathfrak{F}, \rho\mathfrak{V} \rangle$. $\rho\mathfrak{M}$ è un modello intuizionista.

Modello modale e lemma skeleton

Osserviamo che dato un modello intuizionista $\mathfrak{N} = \langle \rho\mathfrak{F}, \mathfrak{U} \rangle$ costruito come skeleton di un frame modale \mathfrak{F} possiamo costruire un modello modale \mathfrak{M} considerando la valutazione

$$\mathfrak{V}(p) = \{x : (\rho\mathfrak{N}, C(x)) \models p\}.$$

In particolare avremo $\rho\mathfrak{M}$ isomorfo a \mathfrak{N} . Inoltre se ogni cluster di \mathfrak{F} è singolo abbiamo che \mathfrak{F} è isomorfo a $\rho\mathfrak{F}$ e \mathfrak{M} è isomorfo ad \mathfrak{N} .

Lemma (skeleton)

Per ogni modello \mathfrak{M} modale costruito su un frame preordinato, per ogni mondo x di \mathfrak{M} e per ogni formula $P \in \text{For}\mathcal{L}$
 $(\rho\mathfrak{M}, C(x)) \models P$ se e solo se $(\mathfrak{M}, x) \models T(P)$.

Lemma skeleton - dimostrazione

Dimostrazione.

La dimostrazione procede per induzione sulla complessità della formula.

Caso base (formula atomica): per la definizione di $\rho\mathfrak{M}$,
 $(\rho\mathfrak{M}, C(x)) \models p$ se e solo se $(\mathfrak{M}, x) \models \Box p$ e $T(p) = \Box p$.

Supponiamo allora che per una formula con n connettivi Q valga
 $(\rho\mathfrak{M}, C(x)) \models Q$ se e solo se $(\mathfrak{M}, x) \models T(Q)$.

Dimostriamo che la proprietà vale aggiungendo l' $n + 1$ esimo connettivo. Distinguiamo i seguenti casi.

Caso $P = Q \rightarrow R$: $(\rho\mathfrak{M}, C(x)) \models P$ se e solo se $(\rho\mathfrak{M}, C(y)) \models Q$ e $(\rho\mathfrak{M}, C(y)) \models R$ in un qualche $C(y)$ tale che $C(x) \mathfrak{R} / \approx C(y)$. È possibile per ipotesi di induzione se e solo se $(\mathfrak{M}, y) \models T(Q)$ e $(\mathfrak{M}, y) \models T(R)$ con $y \in C(y)$ cioè se e solo se $(\mathfrak{M}, x) \models \Box(T(Q) \rightarrow T(R))$ cioè $(\mathfrak{M}, x) \models T(P)$.

Gli altri casi con \wedge e \vee si provano allo stesso modo. □

T è una traduzione di **Int** in **S4**

Corollario

Per ogni frame F quasi ordinato e ogni $P \in \text{For}\mathcal{L}$
 $\rho\mathfrak{F} \models P$ se e solo se $\mathfrak{F} \models T(P)$.

Teorema

$P \in \mathbf{Int}$ se e solo se $T(P) \in \mathbf{S4}$.

Dimostrazione.

(\implies) Supponiamo che $T(P) \notin \mathbf{S4}$. Allora esiste un frame \mathfrak{F} transitivo e riflessivo per cui $\mathfrak{F} \not\models T(P)$. Per il corollario sopra allora $\rho\mathfrak{F} \not\models P$. Dunque $P \notin \mathbf{Int}$.

(\impliedby) Supponiamo che $P \notin \mathbf{Int}$. Allora esiste un frame intuizionista \mathfrak{F} per cui $\mathfrak{F} \not\models P$. Possiamo allora considerare \mathfrak{F} come un frame modale isomorfo al suo skeleton, per cui per il corollario sopra $\mathfrak{F} \not\models T(P)$ e quindi $T(P) \notin \mathbf{S4}$. □

Riferimenti bibliografici



Alexander Chagrov and Michael Zakharyashev.

Modal Logic.

Clarendon Press, 1997.



Gabriele Lolli.

Logica Intuizionista.

Note del corso di filosofia della matematica, 2013.



Giovanni Sambin.

Molteplicità delle logiche e necessità delle traduzioni. Logica intuizionistica e logica classica a confronto.

Note.



Thierry Coquand.

Constructive Logic.

Note della MAP Summer School, Trieste, August 2008.