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

Gabriele Vanoni

Abstract

Dopo aver brevemente presentato le motivazioni filosofiche e matematiche per cui ha senso introdurre la logica intuizionista se ne discute brevemente l'interpretazione BHK e si fornisce la semantica di Kripke. Si passa poi a presentare la traduzione di Gödel-McKinsey-Tarski che permette l'interpretazione dell'intuizionismo attraverso i connettivi modali classici, e in particolare si dimostra l'equivalenza con il sistema **S4**.

Indice

1 La logica intuizionista

Esempi introduttivi

Consideriamo questi tre **teoremi**, provenienti da aree diverse della **matematica**: **logica**, **algebra lineare** e **topologia**.

Teorema 1 (di completezza di Gödel)**.** *La logica classica predicativa è completa.*

Teorema 2 (di esistenza della base)**.** *Ogni spazio vettoriale ha una base.*

Teorema 3 (del punto fisso di Brouwer)**.** *Ogni funzione continua da un insieme convesso e compatto in sé ha almeno un punto fisso.*

L'assioma della scelta

Per dimostrare i primi due **teoremi** viene utilizzato il **lemma di Zorn**. Si può dimostrare che esso è equivalente all'**assioma della scelta AC**.

Definizione 4. Una funzione di scelta su una famiglia di insiemi x è una funzione $f : x \to \cup x$ tale che per ogni $y \in x$, $f(y) \in y$.

Assioma della scelta

Su ogni famiglia di insiemi non vuota esiste una funzione di scelta.

AC ci garantisce l'esistenza della funzione di scelta, ma nessun modo per calcolarla. Perciò quando lo utilizziamo all'interno di altre dimostrazioni queste perdono qualsiasi contenuto costruttivo, non riusciamo per esempio ad esibire dei **testimoni** (witness) nei risultati di **esistenza**.

Ancora sull'assioma della scelta

Per far capire l'utilità di **AC** Bertrand Russell scriveva:

Per scegliere un calzino da ognuna di infinite paia di calzini serve **AC**, mentre l'assioma non è necessario se si vuole scegliere una scarpa da ognuna di infinite paia di scarpe.

La quasi totalità dei matematici ritiene **AC** ovvio, ma **Gödel** e **Cohen** hanno dimostrato rispettivamente nel 1937 e nel 1963 che:

$$Con(\mathsf{ZF}) \to Con(\mathsf{ZF} + \mathsf{AC}) \text{ (\textbf{modello interno}) e}$$

$$Con(\mathsf{ZF}) \to Con(\mathsf{ZF} + \neg\mathsf{AC}) \text{ (\textbf{forcing}).}$$

AC è cioè **indipendente** (così come l'**ipotesi del continuo CH**) dagli assiomi della **teoria degli insiemi ZF**.

Banach e **Tarski** per scoraggiare l'uso di **AC** nelle dimostrazioni elaborarono un ragionamento che facendo uso di **AC** porta a duplicare il volume di una sfera con soli sezionamenti e rototraslazioni.

Le dimostrazioni per assurdo

La dimostrazione originale del teorema di Brouwer ricorre alla tecnica di **dimostrazione per assurdo**. Anche questa maniera di procedere non fornisce dimostrazioni costruttive.

In formule possiamo scrivere la "**reductio ad absurdum**" in questa maniera:

$$(\neg A \rightarrow \bot) \rightarrow A$$

o in altri termini considerando che $(P \rightarrow \bot) \longleftrightarrow \neg P$ è una tautologia:

$$\neg\neg A \rightarrow A.$$

Anche la legge della **doppia negazione** porta quindi a dimostrazioni non costruttive.

L'intuizionismo e la legge del terzo escluso

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**:

$$\vdash P \vee \neg P \equiv \neg\neg\neg P \vee P \equiv \neg\neg P \rightarrow P$$

che è equivalente alla legge della **doppia negazione** ed è implicata dall'**assioma della scelta**.

Nasce allora la **logica intuizionista**, che lo **rifiuta**.

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 della dimostrazione** e dei **linguaggi di programmazione**.
- Infatti viene stabilita una **corrispondenza sintattica** tra le dimostrazioni in **deduzione naturale intuizionista** 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, Huet), dei **linguaggi funzionali** (Haskell) e dei **proof-assistant** (Coq, HOL, Matita).
- 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

Diamo un'interpretazione delle costanti logiche intuizioniste.

- 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 $A \to B$ 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 $A \to \perp$).

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. $P \to (Q \to P)$
2. $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
3. $P \wedge Q \to P$
4. $P \wedge Q \to Q$
5. $P \to (Q \to P \wedge Q)$
6. $P \to P \vee Q$
7. $Q \to P \vee Q$
8. $(P \to R) \to ((Q \to R) \to (P \vee Q \to R))$
9. $\perp \to P$

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** $P \vee (P \to \perp)$.

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 intuizionista $\mathfrak{F} =< \mathfrak{W}, \mathfrak{R} >$ con $\mathfrak{W}$ insieme non vuoto dei **mondi** e $\mathfrak{R} \subseteq \mathfrak{W} \times \mathfrak{W}$ **relazione di accessiblità** fra i mondi, su cui verranno costruiti i relativi **modelli** $\mathfrak{M} =< \mathfrak{F}, \mathfrak{V} >$ assegnando una funzione di **valutazione** $\mathfrak{V} : Var\mathcal{L} \to \mathcal{P}(\mathfrak{W})$.
- Per dare il significato ad $\mathfrak{R}$ 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 $p \in Var\mathcal{L}$.

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

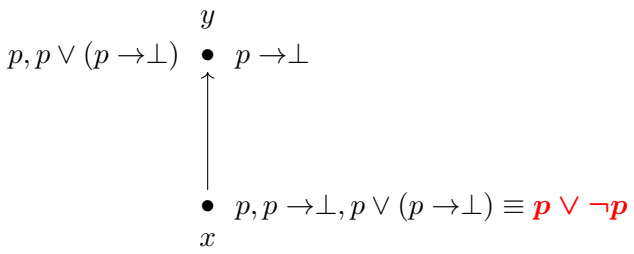
- $(\mathfrak{M}, x) \models p$ sse $x \in \mathfrak{V}(p)$
- $(\mathfrak{M}, x) \models P \wedge Q$ sse $(\mathfrak{M}, x) \models P$ e $(\mathfrak{M}, x) \models Q$
- $(\mathfrak{M}, x) \models P \vee Q$ sse $(\mathfrak{M}, x) \models P$ o $(\mathfrak{M}, x) \models Q$
- $(\mathfrak{M}, x) \models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

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

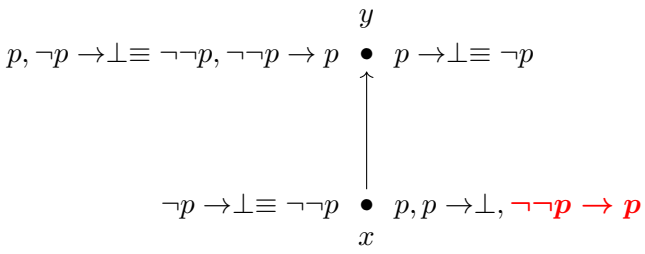
Esempio: il principio del terzo escluso

Ci basta trovare un modello in cui $p \vee \neg p \equiv p \vee (p \to \bot)$ 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!).



Esempio: la legge della doppia negazione

Possiamo utilizzare lo stesso modello dell'esempio precedente.



2 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'operatore $\Box$, necessitiamo di una teoria più forte di **K**, in particolare avremo bisogno che la dimostrabiltà di A implichi A e che la dimostrabilità di A implichi la dimostrabilità della sua dimostrabilità, ovvero devono valere gli **assiomi**:
  - **T**: $\Box A \to A$
  - **4**: $\Box A \to \Box \Box A$
- 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**:

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

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 S** dobbiamo considerare non **S4**, ma la logica **GL** in cui l'operatore $\Box$ ha le stesse proprità del predicato "è dimostrabile in **S**" definito nella dimostrazione dei **teoremi di incompletezza**.

La traduzione

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

Traduzione GMT

- $\mathsf{T}(p) = \Box p$
- $\mathsf{T}(P \wedge Q) = \mathsf{T}(P) \wedge \mathsf{T}(Q)$

- $\mathsf{T}(P \vee Q) = \mathsf{T}(P) \vee \mathsf{T}(Q)$
- $\mathsf{T}(P \to Q) = \Box(\mathsf{T}(P) \to \mathsf{T}(Q))$
- $\mathsf{T}(\bot) = \Box \bot$

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

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

Abbiamo bisogno di alcune definizioni e lemmi preliminari.

Lemma 5. *Sia $\mathfrak{M}$ un modello costruito su un frame $\mathfrak{F} =< \mathfrak{W}, \mathfrak{R} >$ 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 contraddirremmo l'ipotesi. □

Frame skeleton

Definizione 6 (relazione di cluster)**.** Dato un frame $\mathfrak{F}$ transitivo $< \mathfrak{W}, \mathfrak{R} >$ diciamo che per ogni $x, y \in \mathfrak{W}$ $x \approx y$ se e solo se o $x = y$ o $x\mathfrak{R}y$ e $y\mathfrak{R}x$.

Chiamiamo cluster un elemento di $\mathfrak{W}/\approx$ ovvero le classi di equivalenza di $\mathfrak{W}$ rispetto a $\approx$. In particolare denotiamo con $C(x)$ il cluster contenente x.

Definizione 7. Il frame quoziente di un frame transitivo $\mathfrak{F} =< \mathfrak{W}, \mathfrak{R} >$ rispetto alla relazione di cluster $\approx$, cioè $< \mathfrak{W}/\approx, \mathfrak{R}/\approx >$ 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 $\rho\mathfrak{F} =< \rho\mathfrak{W}, \rho\mathfrak{R} >$.

Il 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** $\mathfrak{M} =< \mathfrak{F}, \mathfrak{V} >$. Sappiamo che è costruito su un **frame** $\mathfrak{F} =< \mathfrak{W}, \mathfrak{R} >$ **transitivo e riflessivo** (**preordinato**).

Costruiamo il **frame skeleton** $\rho\mathfrak{F}$ (che è **parzialmente ordinato**, essendo **transitivo**, **riflessivo** e **antisimmetrico**) e assegnamogli 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 $p \in Var\mathcal{L}$.

Chiamiamo **skeleton** di $\mathfrak{M}$ il **modello** $\rho\mathfrak{M} =< \rho\mathfrak{F}, \rho\mathfrak{V} >$.

$\rho\mathfrak{M}$ è dunque un **modello intuizionista**.

Modello modale e lemma skeleton

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

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

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

Dimostrazione. La dimostrazione procede per induzione sulla complessità della formula.

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

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

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

Caso $P=Q\to R$ *(Q e R hanno al più n connettivi):* $(\rho\mathfrak{M},C(x))\not\models P$ se e solo se $(\rho\mathfrak{M},C(y))\models Q$ e $(\rho\mathfrak{M},C(y))\not\models R$ in un qualche $C(y)$ tale che $C(X)\,\mathfrak{R}/\approx C(y)$. È possibile per ipotesi di induzione se e solo se $(\mathfrak{M},y)\models\mathsf{T}(Q)$ e $(\mathfrak{M},y)\not\models\mathsf{T}(R)$ con $y\in C(y)$ cioè se e solo se $(\mathfrak{M},x)\not\models\Box(\mathsf{T}(Q)\to\mathsf{T}(R))$ cioè $(\mathfrak{M},x)\not\models\mathsf{T}(P)$.

Gli altri **casi** con $\wedge$, $\vee$ e $\bot$ si provano allo stesso modo. □

T è una traduzione di Int in S4

Corollario 9. *Per ogni frame $\mathfrak{F}$ quasi ordinato e ogni $P\in For\mathcal{L}$*
$\rho\mathfrak{F}\models P$ *se e solo se* $\mathfrak{F}\models\mathsf{T}(P)$.

Teorema 10. $P\in$ **Int** *se e solo se* $\mathsf{T}(P)\in$ **S4**.

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

($\Longleftarrow$) Supponiamo che $P\notin$ **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 $\mathfrak{F}\not\models\mathsf{T}(P)$ e quindi $\mathsf{T}(P)\notin$ **S4**. □

Alcuni riferimenti più avanzati

- Sia a **Int** sia a **S4** è associata una **semantica algebrica** con cui è possibile far vedere in un altro modo la correttezza della traduzione.
- Alle semantiche algebriche è collegata una **semantica topologica** che apre numerose vie di ricerca in diversi campi, dai **fondamenti della matematica** a quelli dei **linguaggi di programmazione**.
- Esiste una dimostrazione dell'indipendenza di **AC** e **CH** da **ZF** che fa uso di **modelli modali** di **ZF** costruiti su **frame preordinati** (logica **S4**).
- Esistono versioni **costruttive/intuizioniste** di **S4**, con relativa semantica di Kripke. Sono usate per la verifica formale di specifiche hardware.

Riferimenti bibliografici

[1] Alexander Chagrov and Michael Zakharyaschev. *Modal Logic*. Clarendon Press, 1997.

[2] Gabriele Lolli. *Logica Intuizionista*. Note del corso di filosofia della matematica, 2013.

[3] Giovanni Sambin. *Molteplicità delle logiche e necessità delle traduzioni. Logica intuizionistica e logica classica a confronto*. Note.

[4] Thierry Coquand. *Constructive Logic*. Note della MAP Summer School, Trieste, 2008.