# Linguaggi

## 10: Semantica intuizionista (cenni)

Claudio Sacerdoti Coen

<sacerdot@cs.unibo.it>

Universitá di Bologna

18/11/2020

# Outline

# Semantica intuizionista

Wikipedia: "*Nella filosofia della matematica, l'intuizionismo è un approccio alla matematica in cui ogni oggetto matematico è considerato un prodotto dell'attività costruttiva della mente umana. Per l'intuizionismo, l'esistenza di un ente è equivalente alla possibilità della sua costruzione. Vengono quindi rifiutate le dimostrazioni che implicano esplicitamente l'utilizzo di insiemi a cardinalità infinita e l'utilizzo in questi casi dei ragionamenti basati sul principio del terzo escluso.*"

Semantica intuizionista $\approx$ semantica
- dell'evidenza (evidenza = costruzione)
- della conoscenza diretta (evidenza = conoscenza diretta)
- della calcolabilità (evidenza = programma)

# Semantica intuizionista

Confronta: matematica come

- scoperta (in logica classica)
- invenzione (in logica intuizionista)

Cibo per la mente:

- come sarà la matematica di un alieno senza parti discrete (dita, intelligenze individuali, etc.)?
- e quella di un alieno che veda in maniera discreta percependo solamente un'immagine ogni 2s?

# Evidenze indirette vs evidenze dirette

Cos'è un'evidenza indiretta?

Il poliziotto riceve la concitata chiamata del matematico: c'è un omicida nell'aula. Infatti nessuno è entrato e uscito (come si evince dalle telecamere) e nell'aula c'è un uomo con un pugnale conficcato nelle scapole e non può essersi pugnalato così da solo. Quindi non può non esserci un omicida. Il poliziotto chiede: "e chi è?" Risposta: e chi lo sa!

So che c'è $\neq$ so chi è: la prima affermazione non richiede una evidenza diretta, la seconda sì.

In logica classica: $\exists x.P(x)$ significa "so che c'è un $x$ t.c. $P(x)$".
In logica intuizionista: $\exists x.P(x)$ significa "so chi è quell'$x$ t.c. $P(x)$" (dalla prova posso ricavare un algoritmo per capire chi è)

# Evidenze indirette, prove per assurdo e logica classica

Teorema: esistono infiniti numeri primi.

Dimostrazione classica: per assurdo assumiamo che ne esista solamente un insieme finito $\{p_1, \ldots, p_n\}$ e consideriamo $q = p_1 * \ldots * p_n + 1$, che non può essere primo in quanto maggiore di ognuno dei $p_i$. Quindi, poichè $q$ non è primo, esiste almeno un $i$ e un $k$ t.c. $q = p_i * k$. Quindi $1 = q - p_1 * \ldots * p_n = p_i * k - p_1 * \ldots * p_n = p_i * (k - p_1 * \ldots * p_{i-1} * p_{i+1} * \ldots * p_n)$. Il che è assurdo poichè nessun numero primo $p_i$ divide 1. Quindi esistono infiniti numeri primi. Qed.

E quali sono questi numeri primi? Il teorema non ne fornisce nessuno!

# Prove classiche vs prove intuizioniste

Teorema: per ogni $n$, $n$ è pari o non è pari.
Dimostrazione classica: ovvio per EM. Qed.

5 è pari? la prova classica non ce lo dice

Dimostrazione intuizionista: procediamo per induzione strutturale su $n$.
Caso O: $0 = 2 * 0$ e quindi 0 è pari.
Caso $Sm$: per ipotesi induttiva $m$ è pari oppure non lo è. Procediamo per casi: se $m$ è pari allora esiste $k$ t.c. $m = 2 * k$ e $Sm = 2 * k + 1$ non è pari in quanto non divisibile per due; se $m$ non è pari allora esiste $k$ t.c. $m = 2 * k + 1$ e $Sm = 2 * k + 2 = 2 * (k + 1)$ e quindi $Sm$ è pari. Qed.

La prova contiene un algoritmo per ricorsione strutturale: 5 è dispari perchè 4 è pari perchè 3 è dispari perchè 2 è pari perchè 1 è dispari perchè 0 è pari

# Prove classiche vs prove intuizioniste

Tutte le prove intuizioniste di $\forall i.\exists o.P(i,o)$ (per ogni input esiste un output in relazione $P$ con l'input) contengono un algoritmo per calcolare $o$ a partire da $i$.

Una dimostrazione classica dello stesso enunciato può essere molto più breve perchè fa solo metà del lavoro, ci dice che $o$ esiste, ma non ci spiega come calcolarlo.

Quando non esiste nessun algoritmo in grado di determinare $o$ a partire da $i$ (la funzione da $i$ a $o$ non è calcolabile, vedi pacco di lucidi sui paradossi) allora le uniche dimostrazioni sono classiche.

# Contro il modello classico

Nella semantica classica

- Il valore di verità di ogni enunciato è sempre determinato
- Il valore di verità di ogni enunciato è immutabile

Queste ipotesi sono appropriate per la verità “platonica”, ma non per la conoscenza e per mondi non deterministici.

- Prima o poi per la strada passerà una cinquecento viola
- La posizione di una particella è esattamente $x$ e il suo momento è $w$
- I due numeri reali $x$ e $y$ sono uguali
- Dalla scheda sonora leggerò come rumore bianco il seguente pattern
- Il seguente programma $f$ diverge sull’input $z$

# Semantiche intuizioniste

Nelle semantiche intuizioniste

- Il valore di verità di ogni enunciato è determinato solo quando se ne ha una prova/evidenza DIRETTA (un ALGORITMO)
- Il valore di verità di ogni enunciato può passare in maniera monotona dall'essere indeterminato all'avere un determinato valore che non cambia più (scopro almeno un algoritmo o dimostro che non può esserci)

- Prima o poi per la strada passerà una cinquecento viola
- La posizione di una particella è esattamente $x$ e il suo momento è $w$
- I due numeri reali $x$ e $y$ sono uguali
- Dalla scheda sonora leggerò come rumore bianco il seguente pattern
- Il seguente programma $f$ diverge sull'input $z$

# Semantiche intuizioniste

Diverse semantiche “equivalenti” ispirate da principi differenti:

1. Semantica alla Kripke (o dei mondi possibili):
   - L’insieme delle denotazioni è $\{0, 1\}$ ma questa volta 1 significa VERO e 0 significa IGNOTO. Si ha che $A$ è FALSO quando $\neg A$ vale 1, non quando $A$ vale 0.
   - I mondi assegnano a ogni variabile proposizionale una denotazione $\{0, 1\}$, ma possono evolvere: se un mondo $v$ è tale che $v(A) = 0$ allora può evolvere in un mondo $v'$ uguale a $v$, tranne che per $v'(A) = 1$.
   - La funzione $[\![F]\!]^v$ è definita in maniera complessa per tenere conto del fatto che il mondo $v$ può evolvere. (OMESSA)
   - se $v(A) = 0$ allora $v \not\Vdash A \vee \neg A$
   - LE DENOTAZIONI $\{0, 1\}$ SONO LIVELLI DI CONOSCENZA, NON ALGORITMI!
2. Semantica di Brouwer-Heyting-Kolmogorov

# Semantiche intuizioniste

Diverse semantiche “equivalenti” ispirate da principi differenti:

1. Semantica alla Kripke (o dei mondi possibili)
2. Semantica di Brouwer-Heyting-Kolmogorov:
   - Formula $F$ = descrizione di un problema
     es. $\forall i.\exists o.P(i,o)$
   - Denotazione di $F$ = insieme di evidenze, ovvero insieme di algoritmi conosciuti per il problema $F$
   - Insieme vuoto = assenza di algoritmi $\approx$ falsità;
     Insieme non vuoto = almeno un algoritmo = $\approx$ verità
   - Un connettivo descrive un problema a partire da altri problemi
   - La denotazione di un connettivo è un insieme di algoritmi che risolvono il problema composto usando gli algoritmi per i problemi semplici

# Semantica di Brouwer-Heyting-Kolmogorov

Definizione: un mondo $v$ è una funzione dall'insieme $\{A, B, \ldots\}$ all'insieme di tutti gli insiemi di algoritmi.

- $[\![A]\!]^v = v(A)$
- $[\![\bot]\!]^v = \emptyset$
- $[\![\top]\!]^v = \{\star\}$ ($\top$ è un problema banale e $\star$ lo risolve)
- $[\![F \wedge G]\!]^v = [\![F]\!]^v \times [\![G]\!]^v$
  (l'$\wedge$ chiede di risolvere entrambi i problemi;
  algoritmo = coppia di un algoritmo per $F$ e uno per $G$)
- $[\![F \vee G]\!]^v = [\![F]\!]^v \oplus [\![G]\!]^v$
  (l'$\vee$ chiede di risolvere uno dei due problemi dicendo quale;
  algoritmo = coppia $\langle b, \pi \rangle$ dove
  $b = 0$ e $\pi$ è un algoritmo per $F$ oppure
  $b = 1$ e $\pi$ è un algoritmo per $G$)
- $[\![F \Rightarrow G]\!]^v = [\![G]\!]^{v[\![F]\!]^v}$
  (procedure che mappano soluzioni a $F$ in soluzioni a $G$)

# Semantica di Brouwer-Heyting-Kolmogorov

Esempio: $\Vdash A \wedge (A \Rightarrow B) \Rightarrow B$.

In ogni mondo $v$ si ha

$$[\![A \wedge (A \Rightarrow B) \Rightarrow B]\!]^v = [\![B]\!]^{v[\![A]\!]^v \times [\![A \Rightarrow B]\!]^v}$$

Sia $f(\langle a, g \rangle) = g(a)$.

Si ha $f \in [\![B]\!]^{v[\![A]\!]^v \times [\![A \Rightarrow B]\!]^v}$; infatti

- $\langle a, g \rangle \in [\![A]\!]^v \times [\![A \Rightarrow B]\!]^v$ quindi
- $a \in [\![A]\!]^v$ e $g \in [\![A \Rightarrow B]\!]^v = [\![B]\!]^{v[\![A]\!]^v}$ e quindi
- $g(a) \in [\![B]\!]^v$ come richiesto

Quindi, $f$ è un algoritmo che risolve il problema $A \wedge (A \Rightarrow B) \Rightarrow B$ in ogni mondo $v$ e quindi $A \wedge (A \Rightarrow B) \Rightarrow B$ è una tautologia.

# Logica intuizionista: risultati omessi

1. $\not\Vdash A \vee \neg A$
   per un problema $A$ ignoto non conosciamo nessun algoritmo che lo risolva e nemmeno possiamo dire che tale algoritmo non esista
2. Per $A$ particolari (es. $A = n$ è pari) si può dimostrare $A \vee \neg A$ dando un algoritmo (nell'esempio: l'algoritmo ci dice se $n$ è pari oppure no). In tal caso $A$ si dice decidibile.
3. $\not\Vdash \neg\neg A \Rightarrow A$
   il fatto che non possa non esserci un algoritmo per un problema $A$ ignoto non ci dà un algoritmo per $A$
4. Teorema: per ogni $\Gamma, F$, se $\Gamma \Vdash F$ in logica intuizionista allora $\Gamma \Vdash F$ anche in logica classica
   La logica intuizionista ci parla di conoscenza algoritmica (vero $\approx$ so qual'è la soluzione), quella classica di verità (vero $\approx$ so che c'è la soluzione)

# Logica intuizionista: risultati omessi

Teorema (correttezza): per ogni $\Gamma$ e $F$, se $\Gamma \vdash F$ senza usare la RAA allora $\Gamma \Vdash F$ in logica proposizionale intuizionista.
Dimostrazione: omessa.

Ovvero: se riesco a dimostrare $F$ a partire da $\Gamma$ allora ricavo (almeno un) algoritmo che risolva il problema $F$ usando algoritmi per i problemi in $\Gamma$ (es. una libreria di codice per $\Gamma$).

Teorema (completezza debole): per ogni insieme finito di formule $\Gamma$ e per ogni $F$, se $\Gamma \Vdash F$ in logica proposizionale intuizionista allora $\Gamma \vdash F$ senza usare la RAA.
Dimostrazione: omessa.

# Conclusioni

- La semantica intuizionista non assume determinatezza del mondo e immutabilità e ci parla di conoscenza (algoritmica) e non di semplice verità
- La deduzione naturale proposizionale SENZA usare la RAA è completa per la semantica intuizionista
- Le prove intuizioniste sono preferibili a quelle classiche ove possibile: esse contengono un algoritmo che può essere esplicitato
- Dal punto di vista della conoscenza/algoritmico la RAA è pura magia: $\Vdash A \vee \neg A$ significherebbe per ogni $A$ sapere se $A$ vale oppure no / avere un algoritmo che per ogni $A$ o risolve $A$ oppure dimostra che $A$ è insolubile

# Sulla completezza della logica proposizionale classica

Teorema di completezza (forte) per la logica proposizionale classica: per ogni $\Gamma$, $F$, se $\Gamma \Vdash F$ allora $\Gamma \vdash F$.

Teorema di completezza debole per la logica proposizionale classica: per ogni $\Gamma$, $F$ t.c. $\Gamma$ sia un insieme finito, se $\Gamma \Vdash F$ allora $\Gamma \vdash F$.

La versione debole è dimostrabile usando la meta-logica intuizionista, ovvero c'è un algoritmo che dati $\Gamma$ (finito) e $F$ permette di costruire un albero di deduzione naturale per $\Gamma \vdash F$.

La versione forte è dimostrabile solo usando la meta-logica classica, ovvero l'albero di deduzione naturale per $\Gamma \vdash F$ esiste, ma non c'è un algoritmo che permette di costruirlo.

# Sulla completezza della logica proposizionale classica

Intuizioni:

- che nel caso forte non vi sia un algoritmo è abbastanza intuitivo: l'algoritmo in un tempo finito dovrebbe saper analizzare un'infinità di ipotesi ($\Gamma$) per scegliere quali usare
- l'algoritmo per il caso debole funziona in questo modo: siano $V_1, V_2, \ldots, V_n$ le variabili che occorrono in $\Gamma$ (finito!) e $F$. L'albero inizia per casi su $V_1 \vee \neg V_1$ (per EM), in ogni ramo va per casi su $V_2 \vee \neg V_2$, etc. fino ad andare per casi su $V_n \vee \neg V_n$. A questo punto ogni ramo ci parla di un solo mondo e si può dimostrare la tesi a partire dalle ipotesi con una prova intuizionista meccanica.
- che ci sia una dimostrazione in meta-logica classica del caso forte è sorprendente! (vedi slide dopo)

# Teorema di compattezza per la logica proposizionale classica

Il teorema di completezza forte ha come corollario il sorprendente teorema di compattezza:

Teorema di compattezza: per ogni $\Gamma, F$, se $\Gamma \Vdash F$ allora esiste un $\Delta \subseteq \Gamma$, $\Delta$ finito t.c. $\Delta \Vdash F$.

Dimostrazione: siano $\Gamma, F$ t.c. $\Gamma \Vdash F$. Per il teorema di completezza forte si ha $\Gamma \vdash F$. Quindi c'è un albero di deduzione naturale, necessariamene finito, che dimostra $F$ e le cui foglie non scaricate formano un sottoinsieme finito $\Delta$ di $\Gamma$ t.c. $\Delta \vdash F$. Per il teorema di correttezza si ha $\Delta \Vdash F$. Qed.

# Teorema di compattezza per la logica proposizionale classica

Perchè il teorema di compattezza è sorprendente?

1. Esistono infiniti mondi
2. In $\Gamma \Vdash F$ le ipotesi $\Gamma$ filtrano via i mondi fino a quando quelli che restano non soddisfano tutti $F$
3. Infinite ipotesi (quando $\Gamma$ è infinito) permettono di filtrare via un'infinità di mondi in modo molto preciso
4. Il teorema di compattezza ci dice che in verità un numero finito di ipotesi contenute in $\Gamma$ sono già sufficienti a filtrare via abbastanza mondi da rendere comunque $F$ vera nei rimanenti

Ovviamente il teorema di compattezza è dimostrabile solo in una meta-logica classica (un algoritmo dovrebbe scegliere da infinite ipotesi $\Gamma$ quelle da tenere).

# Teorema di compattezza per la logica proposizionale classica

Il fallimento del teorema di compattezza quando le logiche diventano più complesse è il principale responsabile dell'impossibilità di raggiungere la completezza per tali logiche:

1. logiche più ricche a livello di connotazioni richiedono mondi più complessi, il cui insieme finisce per avere cardinalità maggiore
2. le prove rimangono sempre oggetti finiti e pertanto possono sempre usare solamente un numero finito di ipotesi
3. un numero finito di ipotesi diventa insufficiente per filtrare via dall'insieme di tutti i mondi quelli che non soddisfano la conclusione del teorema da dimostrare