Linguaggi

10: Semantica intuizionista (cenni)

Claudio Sacerdoti Coen

<sacerdot@cs.unibo.it>

Universitá di Bologna

03/12/2019

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)

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
- Il valore di verità di ogni enunciato può passare in maniera monotona dall'essere indeterminato all'avere un determinato valore che non cambia più

- 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):
   - I mondi evolvono in maniera monotona
   - Una variabile proposizionale in un mondo può valere 1 (= vero per sempre) oppure 0 (= ignota, indeterminata)
   - Una variabile A ignota in un mondo v può o meno essere definitivamente falsa (quando $v \Vdash A \Rightarrow \bot$)
   - Gli enunciati non definitivamente falsi possono evolvere in enunciati definitivamente veri (o restare ignoti)
   - $v \Vdash F \wedge G$ quando $v \Vdash F$ e $v \Vdash G$;
     $v \Vdash F \vee G$ quando $v \Vdash F$ o $v \Vdash G$;
     $v \Vdash \top$; $v \nVdash \bot$; $v \Vdash A$ sse $v(A) = 1$
   - $\neg F$ è definita come $F \Rightarrow \bot$
   - $v \Vdash F \Rightarrow G$ quando in ogni mondo $w \Vdash F$ dove w è un'evoluzione di v si ha $w \Vdash G$
     Confronto con la semantica classica: il fatto che F sia al momento ignota (non vera) non è sufficiente per concludere G

Semantica di Kripke: esempio

Consideriamo $A \wedge \neg A \Rightarrow \bot$ (principio di non contraddizione)

Sia v^0 il mondo tale che $v^0(A) = 0$ (A "falsa" o ignota) e
sia v^1 il mondo tale che $v^1(A) = 1$ (A definitivamente vera).

Il mondo v^0 ha sia v^0 che v^1 come possibili evoluzioni mentre v^1 evolve solo in v^1 (non può evolvere).

Per ogni i $v^i \Vdash A \wedge \neg A \Rightarrow \bot$ in quanto ogni possibile evoluzione di v^i non soddisfa $A \wedge \neg A$:

se $i = 0$ allora v_0 è una possibile evoluzione di $v_i = v_0$ e $v^0 \nVdash A$ e quindi anche $v^0 \nVdash A \wedge \neg A$;
inoltre in tutti i casi v_1 è una possibile evoluzione di v_i e $v^1 \nVdash \neg A = A \Rightarrow \bot$ in quanto v^1 è una possibile evoluzione di v^1 e $v^1 \Vdash A$ ma $v^1 \nVdash \bot$.

Conclusione: intuizionisticamente $\Vdash A \wedge \neg A \Rightarrow \bot$ ovvero A non può essere definitivamente vero e falso allo stesso tempo.

Semantica di Kripke: esempio

Consideriamo $A \vee \neg A$ (principio classico del terzo escluso).

Sia v il mondo tale che $v(A) = 0$ (A "falsa" o ignota).

Il mondo v ha due possibili evoluzioni: $w_1(A) = 0$, $w_2(A) = 1$.

$v \Vdash A \vee \neg A = A \vee (A \Rightarrow \bot)$ quando

$$v \Vdash A \text{ (falso) oppure } v \Vdash A \Rightarrow \bot$$

Si ha $v \Vdash A \Rightarrow \bot$ sse in ogni w_i si ha che se $w_i \Vdash A$ allora $w_i \Vdash \bot$, e $w_1 \nVdash A$ (ok) ma $w_2 \Vdash A$ e $w_2 \nVdash \bot$.

Conclusione: intuizionisticamente $\nVdash A \vee \neg A$, ovvero non tutte le A sono determinate/note.

Semantica di Kripke: esempio

Consideriamo $\neg\neg A \Rightarrow A$ (principio classico di riduzione ad assurdo).

Siano v, w_1 e w_2 come per il precedente esempio.

$v \Vdash \neg\neg A \Rightarrow A = ((A \Rightarrow \bot) \Rightarrow \bot) \Rightarrow A$ sse in ogni w_i si ha che se $w_i \Vdash (A \Rightarrow \bot) \Rightarrow \bot$ allora $w_i \Vdash A$

Ma nel mondo w_1 si ha $w_1 \nVdash A$ e $w_1 \Vdash (A \Rightarrow \bot) \Rightarrow \bot$ in quando $w_1 = v$ ha come evoluzioni w_1 e w_2 e $w_1 \nVdash \bot$ ma $w_1 \Vdash A \Rightarrow \bot$ in quando w_1 ha come evoluzioni w_1 e w_2 e $w_1 \nVdash \bot$ ma $w_1 \Vdash A$.

Conclusione: intuizionisticamente $\neg\neg A$ non è sufficiente a determinare/conoscere A.

Sul principio del terzo escluso

In generale, per un enunciato F qualunque, non si ha intuizionisticamente che $F \vee \neg F$.

Per F particolari, tuttavia, è possibile che $F \vee \neg F$ sia una tatutologia.

Esempi:

- $\not\vdash x = y \vee x \neq y$ per x, y sequenze infinite (p.e. numeri reali): nessun algoritmo può dirmi quale caso sia vero
- $\vdash P(x) \vee \neg P(x)$ dove $P(x)$ significa "x è pari": si dimostra per induzione su x dando un algoritmo che continua a dimezzare x un numero finito di volte fino a raggiungere 0 o 1

Decidibilità, indecidibilità, semi-decidibilità

Definizione: F si dice decidibile quando intuizionisticamente $\Vdash F \vee \neg F$ ovvero quando vi è un algoritmo che determina se F valga o meno.

Definizione: F si dice indecidibile quando $\nVdash F \vee \neg F$ ovvero quando vi è una dimostrazione di impossibilità di esistenza di un algoritmo che determina se F valga o meno (p.e. terminazione di programmi).

Definizione: F si dice semi-decidibile quando vi è un algoritmo che in un tempo finito ritorna 1 se F vale (tornando 0 o divergendo se F non vale).

Definizione: F si dice co-semidecidibile quando $\neg F$ è semi-decidibile.

Decidibilità, indecidibilità, semi-decidibilità

Note:

- Una F decidibile è sia semi-decibile che co-semidecidibile
- Una F è decidibile solo se è sia semi-decibile che co-semidecidibile
  Dimostrazione: lancio in parallelo i due algoritmi
- In logica classica il principio del terzo escluso vale sempre; questo spezza il legame fra decidibilità ed esistenza di algoritmi.
  In tal caso la terminologia decidibile/indecidibile/... fa riferimento solo all'esistenza di algoritmi.
- Non tutte le F sono note essere decidibili o indecidbili: posso non conoscere un algoritmo per decidere F senza avere una prova dell'impossibilità dell'esistenza di tale algoritmo

Decidibilità, indecidibilità, semi-decidibilità

Note:

- Una F decidibile è sia semi-decibile che co-semidecidibile
- Una F è decidibile solo se è sia semi-decibile che co-semidecidibile
  Dimostrazione: lancio in parallelo i due algoritmi
- In logica classica il principio del terzo escluso vale sempre; questo spezza il legame fra decidibilità ed esistenza di algoritmi.
  In tal caso la terminologia decidibile/indecidibile/... fa riferimento solo all'esistenza di algoritmi.
- Non tutte le F sono note essere decidibili o indecidbili:
  posso non conoscere un algoritmo per decidere F senza avere una prova dell'impossibilità dell'esistenza di tale algoritmo

Sulla semantica di Kripke

La semantica di Kripke ci dice cosa è possibile conoscere e cosa no (denotazioni = valori di verità)

La semantica di Kripke non ci dice in cosa consiste la conoscenza (o evidenza) per le cose conoscibili (le cui denotazioni = true).

Identificando la conoscenza con l'esistenza di un algoritmo, la semantica di Kripke non fornisce banalmente un legame fra conoscibilità e (esistenza di) algoritmi.

La sua rilevanza informatica è pertanto limitata.

Ci sono semantiche alternative le cui denotazioni sono più informative?

Semantiche intuizioniste

Diverse semantiche “equivalenti” ispirate da principi differenti:

1. Semantica alla Kripke (o dei mondi possibili)
2. Semantica di Brouwer-Heyting-Kolmogorov: informalmente

   - la denotazione di una formula è un problema da risolvere algoritmicamente
   - una formula “è vera” quando si conosce almeno un algoritmo che la risolva
   - algoritmo = evidenza
   - la denotazione di un connettivo costruisce un problema a partire da altri problemi

Brouwer-Heyting-Kolmogorov (descrizione informale)

- $[\![A]\!]^v = v(A)$ i mondi assegnano problemi alle variabili
  Es.: $v(A) =$ ordinare una lista di numeri data
- $[\![\bot]\!]^v =$ un qualunque problema noto essere indecidibile
  Es.: il problema della terminazione
- $[\![\top]\!]^v =$ un qualunque problema noto essere decidibile
  Es.: scrivere la funzione identità
- $[\![F \wedge G]\!]^v =$ il problema che consiste nel risolvere sia $[\![F]\!]^v$ che $[\![G]\!]^v$
- $[\![F \vee G]\!]^v =$ il problema che consiste nel risolvere un problema a scelta fra $[\![F]\!]^v$ e $[\![G]\!]^v$, tornando anche un booleano che dice quale si è risolto
- $[\![F \Rightarrow G]\!]^v =$ il problema che consiste nel risolvere $[\![G]\!]^v$ avendo a disposizione una soluzione per $[\![F]\!]^v$ (es.: una funzione di libreria da chiamare che risolve $[\![F]\!]^v$)

  Es.: dire se un elemento è contenuto in una struttura dati sotto l'ipotesi di saper costruire la lista di tutti gli elementi contenuti in tale struttura

Correttezza della deduzione naturale intuizionista

Tutte le regole della deduzione naturale intuizionista sono localmente corrette sia rispetto alla semantica di Kripke sia a quella informale di Brouwer-Heyting-Kolmogorov. Faccio vedere quest'ultima.

$$\frac{F_1 \quad F_2}{F_1 \wedge F_2} \qquad (\wedge_i)$$

Per risolvere algoritmicamente il problema che consiste nel risolverli entrambi esibisco algoritmicamente un programma per ognuno dei due.

$$\frac{F_1 \wedge F_2}{F_j} \qquad (\wedge_{e_j})$$

Se so risolvere algoritmicamente entrambi, posso risolverne anche solo uno dei due accoppiandolo con l'altro problema e buttando via la soluzione dell'altro.

Correttezza della deduzione naturale intuizionista

$$\frac{F_j}{F_1 \vee F_2} \quad (\vee_{i_j})$$

Per risolvere il problema che mi chiede di scegliere quale dei due risolvere, scelgo e risolvo quello.

$$\frac{F_1 \vee F_2 \qquad \begin{array}{c}[F_1]\\ \vdots \\ F_3\end{array} \qquad \begin{array}{c}[F_2]\\ \vdots \\ F_3\end{array}}{F_3} \quad (\vee_e)$$

Per risolvere algoritmicamente il problema $[\![F_3]\!]^v$ sapendo risolvere uno (ma non a mia scelta!) fra $[\![F_1]\!]^v$ e la $[\![F_2]\!]^v$ debbo saper sia risolvere $[\![F_3]\!]^v$ avendo a dispozione una soluzione algoritmica a $[\![F_1]\!]^v$ che avendo a dispozione una soluzione algoritmica a $[\![F_2]\!]^v$

Correttezza della deduzione naturale intuizionista

$$\frac{}{\top} \quad (\top_i)$$

Un problema decidibile è risolvibile algoritmicamente per definizione

$$\frac{\bot}{F} \quad (\bot_e)$$

Saper risolvere algoritmicamente un problema indecidibile è assurdo: dall'assurdo concludo qualunque cosa, compreso il saper risolvere algoritmicamente qualunque problema

Nota: la spiegazione della $\bot_e$ non è troppo convincente. Lo sarebbe se avessi dato rigorosamente la spiegazione della semantica di Brouwer-Heyting-Kolmogorov. In tal caso si capirebbe che il codice che risolve algoritmicamente il problema $[\![F]\!]^v$ non farebbe altro che invocare il codice che risolve il problema $[\![\bot]\!]^v$ e questo manderebbe in crash il programma.

Correttezza della deduzione naturale intuizionista

$$\dfrac{\begin{array}{c}[F_1]\\ \vdots \\ F_2\end{array}}{F_1 \Rightarrow F_2} \qquad (\Rightarrow_i)$$

Per risolvere algoritmicamente il problema di risolvere $[\![F_2]\!]^v$ avendo a dispozione una soluzione a $[\![F_1]\!]^v$ risolvo $[\![F_2]\!]^v$ assumendo (= prendendo in input) una soluzione algoritmica a $[\![F_1]\!]^v$

Le ipotesi di un teorema sono funzioni di libreria o funzioni prese temporaneamente in input che risolvono determinati problemi algoritmici.

Correttezza della deduzione naturale intuizionista

$$\frac{F_1 \Rightarrow F_2 \quad F_1}{F_2} \qquad (\Rightarrow e)$$

Se ho un algoritmo che mi riduce la soluzione di $[\![F_2]\!]^v$ a quella di $[\![F_1]\!]^v$ e ho un algoritmo che risolve $[\![F_1]\!]^v$, combinandoli risolvo $[\![F_2]\!]^v$.

Correttezza della deduzione naturale intuizionista

$$\dfrac{\begin{array}{c}[\neg F]\\ \vdots\\ \bot\end{array}}{F}\ (RAA)$$

La RAA non è corretta: anche sapendo ridurre un problema non decidibile al problema $[\![\neg F]\!]^v$, ovvero al problema di ridurre un problema non decidibile a $[\![F]\!]^v$, non si ottiene un algoritmo che risolva un problema $[\![F]\!]^v$ qualsiasi.

Correttezza della deduzione naturale intuizionista

$$F \vee \neg F$$

L'EM non è una tautologia: dato un generico problema $[\![F]\!]^v$, non conosco nessuna soluzione algoritmica al problema e nemmeno un modo per risolvere un problema non decidibile a partire da una soluzione algoritmica per $[\![F]\!]^v$

Completezza della deduzione naturale intuizionista

Teorema non dimostrato (completezza della deduzione naturale intuizionista): la deduzione naturale intuizionista per la logica proposizionale è completa sia rispetto alla logica intuizionista alla Kripke, sia rispetto a quella alla Brouwer-Heyting-Kolmogorov. Ovvero, per ogni Γ, F, se $\Gamma \Vdash F$ allora $\Gamma \vdash F$ dove la prova in deduzione naturale non usa RAA.

Corollario (compatibilità della logica intuizionista con quella classica): se $\Gamma \vdash F$ (o, equivalentemente, $\Gamma \Vdash F$) in logica intuizionista allora $\Gamma \vdash F$ (o, equivalentemente, $\Gamma \Vdash F$) in logica classica.