Lezione 21 21/12/2023

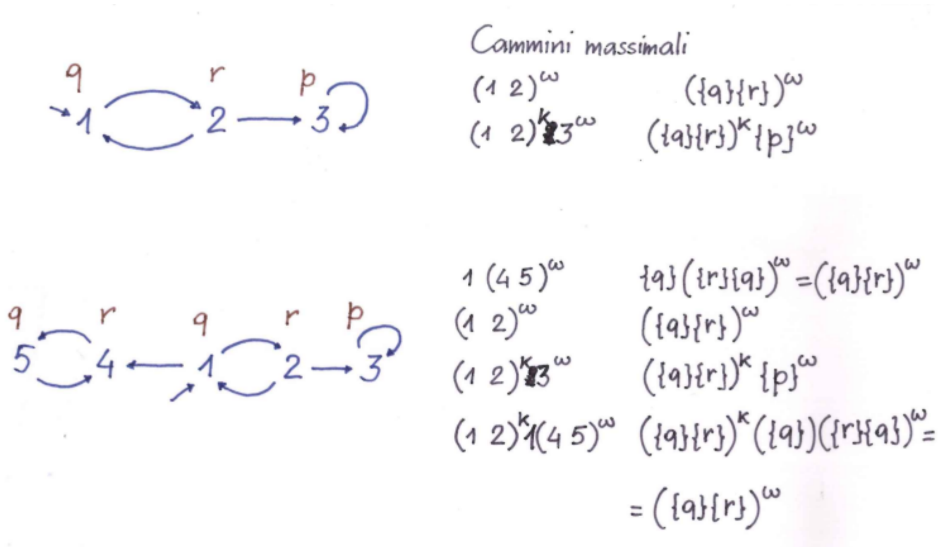
Equivalenza dei modelli rispetto a una logica

Due modelli di Kripke, M_1 e M_2, con stati iniziali q_0 e s_0 si dicono equivalenti rispetto a una logica L se, per ogni formula $\alpha \in FBF_L$

$$M_1, q_0 \models \alpha \iff M_2, s_0 \models \alpha$$

Se per ogni formula alpha, alpha è vera nello stato iniziale sse è vera nell’altro modello nello stato iniziale.

Esempio



Per dimostrare che sono equivalenti, per ciascuno dei due modelli scriviamo queste espressioni di modo da specificare tutti i cammini massimali. Nel primo caso i cammini massimali che partono dallo stato uno sono: quello che rimane a ciclo tra 1 e 2, e quello che fa un numero finito di cicli e poi rimane all’infinito su 3. Facciamo la stessa cosa per il secondo.

Prendiamo le espressioni dei cammini massimali e trasformarle sostituendo ad ogni stato l’insieme delle proposizione atomiche che sono vere in quello stato.

Insiemi parzialmente ordinati

Relazione d'ordine parziale su A: $\leq \quad \subseteq \quad A \times A$

(1) riflessiva: $x \leq x$ per ogni x in A

(2) antisimmetrica: $(x \leq y \wedge y \leq x) \longrightarrow x = y$, per ogni x e y in A

(3) transitiva: $(x \leq y \wedge y \leq z) \longrightarrow x \leq z$, per ogni x, y e z in A

Notazione:
$x \geq y$ significa $y \leq x$; $x < y$ significa $(x \leq y \wedge x \neq y)$;
$y > x \ldots$

(1) Qual è la più piccola relazione d'ordine parziale su A?

(2) Raffinamento di una relazione d'ordine parziale

(3) Relazione d'ordine totale

(4) Linearizzazione di un ordine parziale

Una linearizzazione è un raffinamento dell'ordine parziale, che è a sua volta un ordine totale.

Sia $(A, \leq)$ un insieme parzialmente ordinato, e $B \subseteq A$

$x \in A$ è un maggiorante di B se $y \leq x$ per ogni y in B

$x \in A$ è un minorante di B se $x \leq y$ per ogni y in B

Indichiamo con B^* l'insieme dei maggioranti di B

Indichiamo con B_* l'insieme dei minoranti di B

B si dice limitato superiormente se $B^* \neq \emptyset$

B si dice limitato inferiormente se $B_* \neq \emptyset$

$x \in B$ è il minimo di B se $x \leq y$ per ogni y in B

$x \in B$ è il massimo di B se $y \leq x$ per ogni y in B

$x \in B$ è minimale in B se $y \leq x$ implica $y = x$

$x \in B$ è massimale in B se $x \leq y$ implica $y = x$

più debole di minimo/massimo (se non c'è nessun elemento più piccolo/grande di x). Minimo è un elemento più piccolo di tutti gli altri, minimale è un elemento che non ha elementi più piccoli. Quindi in un insieme c'è al massimo un minimo, ma tanti minimali.

Se x è il minimo di B^*, diciamo che x è l'estremo superiore (join) di B, e scriviamo $x = \sup B$, o anche $x = \bigvee B$

Se x è il massimo di B_*, diciamo che x è l'estremo inferiore (meet) di B, e scriviamo $x = \inf B$ o anche $x = \bigwedge B$

In particolare, se $B = \{x, y\}$, scriveremo $x \vee y$ per indicare $\bigvee B$, se esiste, e $x \wedge y$ per $\bigwedge B$, se esiste

Esempio

$(2^A, \subseteq)$ dove A è un insieme qualsiasi

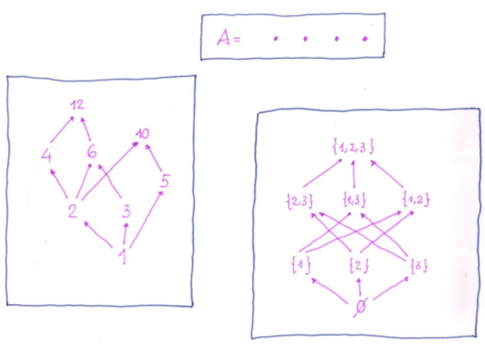
Verifichiamo se è una relazione d'ordine parziale. Vediamo che è riflessiva, antisimmetrica e transitiva quindi è giusto.
Ha un minimo? si, l'insieme vuoto.
Ha un massimo? si, A.
Estremo superiore (minimo dei maggioranti) è l'unione, l'estremo inferiore è l'intersezione.

$(\mathbb{N}^+, |)$ dove $|$ indica la relazione *divide* (ad es. $3 \mid 27$, $5 \nmid 27$)

è riflessiva (un numero divide se stesso), è antisimmetrica, è transitiva.

$$([\mathrm{FBF}_{\mathrm{LP}}]_{\equiv}, \longrightarrow)$$

Formule ben formate della logica proposizionale, due formule sono equivalenti se una implica l'altra. è riflessiva (ogni formula implica se stessa), è antisimmetrica e transitiva.



3 insiemi parzialmente ordinati.

Il primo è quello dove ci sono 4 punti senza collegamenti, è una particolare relazione di ordine parziale.

Nel secondo la relazione parziale è "divide"

Reticoli

Un reticolo è un insieme parzialmente ordinato $(L, \leq)$, tale che, per ogni $x, y \in L$, esistono $x \vee y$ e $x \wedge y$

Un reticolo si dice completo se $\bigvee B$ e $\bigwedge B$ esistono per ogni $B \subseteq L$

Un reticolo ha la proprietà che esiste il join e il meet tra due qualsiasi elementi (estremo superiore e inferiore).

Si dice completo se join e meet esistono per ogni sottoinsieme.

Se L è finito allora è anche completo. Se L è infinito potrebbe non essere completo.

Funzioni e punti fissi

Consideriamo funzioni $f : X \to X$

Un elemento $x \in X$ è un punto fisso di f se $f(x) = x$

(1) $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ Insieme dei punti fissi: $\{0, 1\}$

(2) $g : \mathbb{R}^+ \to \mathbb{R}$, $g(x) = \log(x)$ Insieme dei punti fissi: $\emptyset$

(3) $h : \mathbb{R} \to \mathbb{R}$, $h(x) = x$ Insieme dei punti fissi: $\mathbb{R}$

Insieme parzialmente ordinati e funzioni monotone

Siano $(A, \leq)$ e $(B, \leq)$ due insiemi parzialmente ordinati

Una funzione $f : A \to B$ si dice monotòna se, per ogni coppia di elementi $x, y \in A$, vale

$$x \leq y \Longrightarrow f(x) \leq f(y)$$

Funzioni monotone e punti fissi

Se $(A, \leq)$ è un insieme parzialmente ordinato, e $f : A \rightarrow A$ è una funzione monotòna, possiamo chiederci se esistano un minimo e un massimo punto fisso

Consideriamo $(2^{\mathbb{N}}, \subseteq)$ e $S \subseteq \mathbb{N}$

(1) $f(S) = S \cup \{2, 7\}$

f(S) produce l'unione tra S e questo particolare insieme. Ci chiediamo se la funzione è monotona, si. Ha punti fissi? Si, tutti gli insiemi che contengono {2,7}.

Consideriamo $A = 2^{\mathbb{N}}$ e $S \subseteq \mathbb{N}$

(2) $f(S) = S \cap \{2, 7, 8, 12, 21\}$

L'insieme vuoto è un punto fisso, gli altri punti fissi sono tutti i sottoinsiemi dell'insieme {2, 7, 8, 12, 21} quindi il più grande punto fisso è proprio quell'insieme.

(manca un altro esempio, slide "funzioni monotone e punti fissi" scritta a mano con un albero, A= {1, .., 11}

Teorema di Knaster-Tarski

è l'unico teorema per cui ci chiede di studiare la dimostrazione.

Sia $(L, \leq)$ un reticolo completo, e $f : L \rightarrow L$ sia una funzione monotòna. Allora f ha un minimo e un massimo punto fisso.

Dimostrazione

Dimostriamo il teorema nel caso particolare,

$$L = 2^A \qquad f : 2^A \longrightarrow 2^A, \text{ monotòna}$$

Dominio e codominio sono gli insiemi delle parti di A.

Costruiamo l'insieme $Z = \{T \subseteq A \mid f(T) \subseteq T\}$

Gli elementi di Z saranno chiamati punti pre-fissi

Costruiamo l'insieme Z che contiene tutti i sottoinsiemi di A per cui l'immagine di T rispetto alla funzione f è compresa in T. Questi punti si chiamano pre-fissi.

Fissato il reticolo L come insieme delle parti di A, e f che è monotona, Z non può essere vuoto. Se T è un punto fisso, allora sicuramente sta in Z. Quindi se ci sono punti fissi, sono tutti contenuti in Z.

Poniamo $m = \bigcap Z$

Formiamo l'intersezione di tutti i sottoinsiemi di A che sono nella famiglia Z.
m è un particolare sottoinsieme di A.

Per ogni S in Z, $m \subseteq S$, quindi

$$f(m) \subseteq f(S) \subseteq S$$

m è contenuto in ogni elemento S che sta in Z.

Quindi la sua immagine è contenuta in S.

Per ogni S in Z, $f(m) \subseteq S$

quindi $f(m) \subseteq \bigcap Z = m$

quindi $m \in Z$

Osservazione: $m = \min Z$

Z contiene anche m. Per come è costruito, m è anche il minimo in Z, perché è contenuto in tutti gli altri elementi.

Se riuscissimo a dimostrare che m costruito in questo modo è un punto fisso di f allora avremmo dimostrato che è il minimo punto fisso. Avremmo dimostrato il teorema.

Ora vogliamo dimostrare che m è un punto fisso di f.

$$f(m) \subseteq m$$

f è monotòna, quindi

$$f(f(m)) \subseteq f(m)$$

Allora, $f(m) \in Z$, quindi $m \subseteq f(m)$

Dato che f è monotona, deduciamo che applicando f ai due membri della disuguaglianza, la disuguaglianza è conservata.

Ricapitoliamo: abbiamo considerato un reticolo completo particolare, quello formato da tutti i sottoinsiemi di un insieme dato. abbiamo supposto di definire una funzione monotona definita sugli elementi di questo reticolo, abbiamo dimostrato che sotto queste due condizioni (reticolo completo, funzione monotona) che f ha almeno un punto fisso e almeno un minimo punto fisso. Come si fa a dimostrare che ha anche un massimo punto fisso? I reticoli hanno una simmetria dove per ogni teorema che dimostro per minimo ho anche il duale per il massimo. Potremmo dimostrarlo considerando gli elementi di Z post-fissi e invertendo intersezione con unione etc.

Bisogna fare la dimostrazione del massimo e portarla all'orale.

Dobbiamo essere capaci di ripetere la dimostrazione all'orale, portando la traccia scritta (quindi non a memoria) giustificando i passaggi.

Teorema di Kleene

Sia $f : 2^A \to 2^A$ monotòna

La funzione f si dice continua se

$$X_1 \subseteq X_2 \subseteq \cdots \subseteq X_i \subseteq \cdots$$

$$f(X_1) \subseteq f(X_2) \subseteq \cdots \subseteq f(X_i) \subseteq \cdots$$

$$f(\bigcup X_i) = \bigcup f(X_i)$$

f monotona dal reticolo a se stesso.

C'è una catena di sottoinsiemi, di inclusioni. Stessa cosa su f.

Prendiamo l'unione di tutti gli Xi che formano la catena e applichiamo f. Dall'altra parte prendiamo l'immagine di questi Xi e forniamo la loro unione. Questi due insiemi possono essere diversi, f è continua se sono uguali.

non gli interessa che memorizziamo la definizione. Ci interessa questa idea di continuità della funzione, perché se f è continua allora possiamo calcolare iterativamente il minimo del punto fisso f in questo modo:

Iniziamo ad applicare f all'insieme vuoto, se l'insieme che otteniamo è l'insieme vuoto, questo è il minimo punto fisso.
Altrimenti continuiamo ad applicare f finché non trovo un punto fisso e prima o poi troveremo il minimo punto fisso.

Se f è continua, allora

(1) il minimo punto fisso di f si può ottenere calcolando

$$f(\emptyset), \quad f(f(\emptyset)), \quad f(f(f(\emptyset))), \quad \cdots$$

(2) il massimo punto fisso di f si può ottenere calcolando

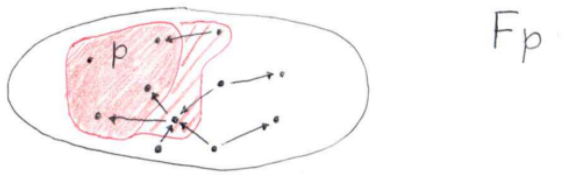
$$f(A), \quad f(f(A)), \quad f(f(f(A))), \quad \cdots$$

Esempio

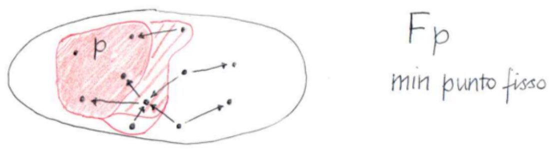
Errore nella formula: dovrebbe essere AFp (prima o poi vale p)

Isoliamo l'insieme di stati in cui vale p.

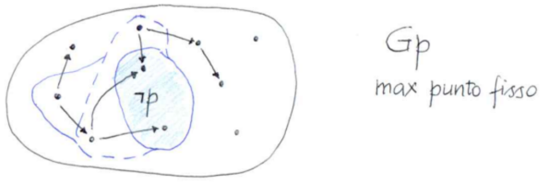
Allarghiamo questo insieme aggiungendo stati dove siamo sicuri che Fp è valida.



Possiamo aggiungere gli stati a partire dai quali in una sola transizione andiamo a finire in questo insieme.



Posso aggiungere questo stato e non gli altri perché su questo ho solo una transizione che mi porta nell'insieme, con gli altri ho alternative quindi non sono sicuro.



Qui devo ragionare al contrario, parto dagli stati dove la formula non vale e man mano mi espando. Mi fermo quando nell'iterazione non ho eliminato più niente.

Gli stati che rimangono fuori sono quelli dove vale Gp.

Un algoritmo per CTL

$$M = (Q, T, I)$$

Sia α una formula; definiamo l'estensione di α:

$$[\![\alpha]\!] = \{q \in Q \mid M, q \models \alpha\}$$

L'estensione è gli insieme di tutti gli stati in cui è valida alpha.

L'algoritmo dovrà costruire una funzione particolare per ogni formula che ci interessa.

$$M = (Q, T, I)$$

Consideriamo la formula $\alpha \equiv AF\,\beta$

A questa formula associamo una funzione $f_\alpha : 2^Q \longrightarrow 2^Q$

Per ogni $H \subseteq Q$,

$$f_\alpha(H) = [\![\beta]\!] \cup \{q \in Q \mid \forall (q, q') \in T : q' \in H\}$$

Osservazione: $f_\alpha(\emptyset) = [\![\beta]\!]$

$[\![\alpha]\!]$ è il minimo punto fisso di f_α

La formula dice: per ogni cammino prima o poi sarà vera beta.

Associamo una funzione che fa il passaggio di stati (come nell'esempio precedente)

Diciamo che falpha di H produce l'estensione di beta unito a tutti gli stati a partire dai quali sono sicuro che in un solo passaggio vado a finire in H.

Partiamo applicando f all'insieme vuoto, otteniamo questo, e continuiamo ad applicare finchè arrivo ad un insieme di stati che è il punto fisso.

$$M = (Q, T, I)$$

Consideriamo la formula $\alpha \equiv EG\,\beta$

A questa formula associamo una funzione $g_\alpha : 2^Q \longrightarrow 2^Q$

Per ogni $H \subseteq Q$,

$$g_\alpha(H) = [\![\beta]\!] \cap \{q \in Q \mid \exists (q, q') \in T : q' \in H\}$$

Osservazione: $g_\beta(Q) = [\![\beta]\!]$

$[\![\alpha]\!]$ è il massimo punto fisso di g_α

La formula dice: esiste un cammino in cui è sempre vera beta.

Dobbiamo costruire una funzione galpha (cercando il massimo punto fisso, eliminando gli stati.

La funzione g calcola l'estensione di beta (insieme di tutti gli stati in cui vale beta) e fa intersezione con gli stati dove c'è una transizione che finisce in H.

Visto che stiamo cercando il massimo punto fisso partiamo dall'insieme di tutti gli stati, eliminando gli stati dove non vale beta, e proseguiamo eliminando stati via via.

L’estensione di alpha sarà il massimo punto fisso.

Seguendo questo schema provate a scrivere la funzione associata ad AalphaUntilbeta, ragiona se devi trovare il minimo o massimo punto fisso, ricordando che until si può esprimere combinando una certa formula con l’operatore F.

In risultato di questo esercizio va portato all’orale.