Lezione 18 MSC
Teoria dei punti fissi

Roberto Gorrieri

Perché studiare questa teoria?

- Equivalenza di bisimulazione ~
  - Vista come massimo punto fisso di un'opportuna funzione tra relazioni
  - Algoritmo associato molto intuitivo
- Logiche con formule ricorsive (HML con ricorsione)
  - Necessaria per dare significato (semantica) alle formule definite ricorsivamente attraverso massimi o minimi punti fissi

Poset: partially ordered set

- Un poset (insieme parzialmente ordinato) è una coppia (D, $\leq$), dove D è un insieme e $\leq \subseteq$ DxD è una relazione
  - Riflessiva: $d \leq d \quad \forall\, d \in D$
  - Antisimmetrica: $d \leq e \wedge e \leq d \Rightarrow d = e \quad \forall\, d, e \in D$
  - Transitiva: $d \leq e \wedge e \leq f \Rightarrow d \leq f \quad \forall\, d, e, f \in D$
- Il poset (D, $\leq$) è totalmente ordinato se

$$d \leq e \vee e \leq d \qquad \forall\, d, e \in D$$

Esempi di posets

- $(N, \leq)$: l'insieme dei naturali con l'usuale ordinamento tra numeri (totalmente ordinato)
- $(A^*, \leq)$: l'insieme di tutte le parole su alfabeto A con prefix ordering: $s \leq t$ sse $\exists\, u \in A^*.\ su = t$
- $(F, \leq)$: insieme delle funzioni $f : S \rightarrow D$, dove $(D, \leq')$ è un poset, con $f \leq g$ sse $f(s) \leq' g(s)\ \forall s \in S$
- $(2^S, \subseteq)$: l'insieme delle parti di S con $\subseteq$ l'usuale operatore di contenuto o uguale tra insiemi

Estremo superiore (sup) o inferiore (inf)

- Estremo superiore = minimo maggiorante = least upper bound = sup
- Estremo inferiore = massimo minorante = greatest lower bound = inf
- Sia (D, ≤) un poset e sia X un sottoinsieme di D:
  - d $\in$ D è un maggiorante (minorante) per X sse $x \leq d$ ($d \leq x$) $\forall x \in X$
  - d è sup (inf) per X -- e lo indichiamo con $\cup X$ ($\cap X$) -- sse:
    - d è maggiorante (minorante) per X, e
    - $d \leq d'$ ($d' \leq d$) $\forall d' \in D$ che è maggiorante (minorante) per X

Esempi

- Per $(N, \leq)$, tutti i sottoinsiemi finiti X di N hanno sup (elemento massimo di X); nessun sottoinsieme infinito ha sup; tutti i sottoinsiemi X di N hanno inf (elemento minimo di X)
- Per $(2^S, \subseteq)$, ovvero l'insieme delle parti di S, una collezione X di sottoinsiemi di S ha l'unione di tutti i sottoinsiemi $\cup X$ come sup e l'intersezione di tutti i sottoinsiemi $\cap X$ come inf.
- Esercizio: dato $(D, \leq)$ e un suo sottoinsieme X, il sup $\cup X$ e l'inf $\cap X$ di X sono unici, se esistono.
- Osservazione: se il sup (inf) d di X appartiene a X, allora d è massimo (minimo) di X.

Reticolo e reticolo completo

- Un poset $(D, \leq)$ è un reticolo sse $\forall d, e \in D$ esistono in D sia il sup $\cup\{d,e\}$ che l'inf $\cap\{d,e\}$.
- Un poset $(D, \leq)$ è un reticolo completo sse il sup $\cup X$ e l'inf $\cap X$ esistono per ogni X sottoinsieme di D.
- Osservazione 1: un reticolo completo ha elemento minimo $\perp$ (bottom) ottenuto come $\cap D$ (massimo minorante di D), ed un elemento massimo T (top) ottenuto come $\cup D$ (minimo maggiorante di D).
- Osservazione 2:
  - $\cup\varnothing = \perp$ (minimo tra i maggioranti dell'insieme vuoto, ovvero minimo di D)
  - $\cap\varnothing = T$ (massimo tra i minoranti dell'insieme vuoto, ovvero massimo di D)

Esempi

- $(N, \leq)$ è un reticolo ma non è completo perché non ha sup per i suoi sottoinsiemi infiniti
- $(N \cup \{\infty\}, \leq')$ dove $n \leq' m$ vale true se $m = \infty$, altrimenti vale come $n \leq m$ (se n e m in N), è un reticolo completo
- $(2^S, \subseteq)$ è un reticolo completo
- Esercizio: $(N, \leq'')$ dove $n \leq'' m$ se n è un divisore di m, è un reticolo? È un reticolo completo?

Funzioni monotone e punti fissi

- Dato un poset $(D, \leq)$, una funzione $f: D \rightarrow D$ è monotona sse $d \leq d' \Rightarrow f(d) \leq f(d')$ $\forall d, d' \in D$
- Un elemento d è detto punto fisso sse $d = f(d)$
- Un elemento d è detto post-punto fisso (pre-punto fisso) sse $d \leq f(d)$ $(f(d) \leq d)$
- Esempio: $f: 2^N \rightarrow 2^N$ $f(X) = X \cup \{1,2\}$, f è monotona e tutti gli infiniti punti fissi sono della forma $\{Y \mid \{1,2\} \subseteq Y\}$, con $\{1,2\}$ come minimo punto fisso e N come massimo punto fisso.
- Esercizio: $g(X) = \{1,2,3\}$ se $X = \{2\}$, $g(X) = X \cup \{1,2\}$ se $X \neq \{2\}$ è monotona?

Teorema del punto fisso (Knaster 1928-Tarski 1955)

Teorema: Sia $(D, \leq)$ un reticolo completo e sia $f: D \to D$ monotona. Allora f ha un massimo punto fisso Zmax e un minimo punto fisso Zmin definiti come

$Zmax = \bigcup\{x \text{ in } D \mid x \leq f(x)\}$ (sup dei post-punti fissi)

$Zmin = \bigcap\{x \text{ in } D \mid f(x) \leq x\}$ (inf dei pre-punti fissi)

Dimostrazione: Dimostriamo che

(1) Zmax è un punto fisso: $Zmax = f(Zmax)$, e

(2) Zmax è il massimo punto fisso, ovvero se $f(d) = d$, allora $d \leq Zmax$

Sia $A = \{x \text{ in } D \mid x \leq f(x)\}$ l'insieme dei post-punti fissi, con $Zmax = \bigcup A$.

(1) Per antisimmetria, basta provare

(a) $Zmax \leq f(Zmax)$ e

(b) $f(Zmax) \leq Zmax$

(a) Per def, sappiamo che $Zmax = \bigcup A$.

Allora $\forall x \in A$, vale $x \leq Zmax$. Dato che f è monotona, $x \leq Zmax$ implica $f(x) \leq f(Zmax)$.

Quindi $\forall x \in A \;\; x \leq f(x) \leq f(Zmax)$, ovvero $f(Zmax)$ è un maggiorante per A. Per def, Zmax è il minimo maggiorante di A, e quindi

$$Zmax \leq f(Zmax)$$

(b) Per monotonia di f e quanto detto sopra, abbiamo $f(Zmax) \leq f(f(Zmax))$, ovvero $f(Zmax)$ è un post-punto fisso e quindi sta in A. Poiché Zmax è un maggiorante di A, deve essere

$$f(Zmax) \leq Zmax$$

Rimane da dimostare (2), ovvero che Zmax è il massimo punto fisso.

Sia d un qualunque punto fisso, $d = f(d)$. Allora vale anche $d \leq f(d)$, ovvero d in A, e perciò

$$d \leq \bigcup A = Zmax.$$

Esercizio: completa la dimostrazione per Zmin, ovvero dimostra che:

(3) $Zmin = f(Zmin)$, dimostrando

(c) $f(Zmin) \leq Zmin$, e

(d) $Zmin \leq f(Zmin)$,

(4) $Zmin \leq d$ per ogni d tale che $d = f(d)$

Esempio

- $(2^S, \subseteq)$ $f: 2^S \rightarrow 2^S$ monotona

  $Zmax = \cup\{X \text{ in } 2^S \mid X \subseteq f(X)\}$

  $Zmin = \cap\{X \text{ in } 2^S \mid f(X) \subseteq X\}$

Se prendiamo $S = N$ e $f(X) = X \cup \{1,2\}$, allora

$Zmax = \cup\{X \subseteq N \mid X \subseteq X\cup\{1,2\}\} = N$

$Zmin = \cap\{X \subseteq N \mid X\cup\{1,2\} \subseteq X\} = \{1,2\}$

Potenza di una funzione

- Sia f: D → D una funzione su un insieme D. Per ogni n in N, definiamo $f^n(d)$ per ogni d in D come segue:

  $f^0(d) = d$ (cioè f^0 è l'identità)

  $f^{n+1}(d) = f(f^n(d))$

Come calcolare i punti fissi?

Teorema: Sia (D, $\leq$) un reticolo completo finito e sia $f: D \rightarrow D$ una funzione monotona. Allora il minimo punto fisso

(1) Zmin = $f^m(\perp)$ per qualche m in N, mentre il massimo punto fisso

(2) Zmax = $f^M(T)$ per qualche M in N.

Dimostrazione di (1): dato che f è monotona e $\perp$ è il minimo, abbiamo che:

$\perp \leq f(\perp) \leq f^2(\perp) \leq \ldots \leq f^i(\perp) \leq \ldots$

Dato che D è finito, la catena deve essere costante da un certo punto in poi, cioè $\exists$ m. $\forall$ k $\geq$ m $f^k(\perp) = f^m(\perp)$. In particolare, $f(f^m(\perp)) = f^{m+1}(\perp) = f^m(\perp)$, cioè $f^m(\perp)$ è un punto fisso.

Per dimostrare che $f^m(\perp)$ è il minimo tra i punti fissi, sia d un punto fisso, $d = f(d)$. Vale che

$\perp \leq d$ e per monotonia $f(\perp) \leq f(d) = d$ ed in generale $f^k(\perp) \leq f^k(d) = d$ per ogni k in N, in particolare $f^m(\perp) \leq d$.

Dimostrazione di (2): Dato che f è monotona e T è il massimo, abbiamo che

$T \geq f(T) \geq f^2(T) \geq \ldots \geq f^i(T) \geq ..$

Dato che D è finito, $\exists$ M. $\forall$ $k \geq M$ si ha $f^k(T) = f^M(T)$. In particolare $f(f^M(T)) = f^{M+1}(T) = f^M(T)$,

cioè $f^M(T)$ è un punto fisso. È il massimo perché per ogni altro punto fisso d vale che

$d \leq T$ e per montonia $d = f^k(d) \leq f^k(T)$ per ogni k; in particolare $d \leq f^M(T)$.

Esempio

- g: $2^{\{0,1,2\}} \rightarrow 2^{\{0,1,2\}}$ $g(X) = (X \cap \{1\}) \cup \{2\}$
- g è monotona (facile esercizio)
- $2^{\{0,1,2\}}$ è un reticolo completo finito
- Allora posso calcolare il minimo e il massimo punto fisso:
- $g(\varnothing) = \{2\}$ $g^2(\varnothing) = g(\{2\}) = \{2\}$ $Zmin = \{2\}$
- $g(\{0,1,2\}) = \{1,2\}$ $g^2(\{0,1,2\}) = g(\{1,2\}) = \{1,2\}$ $Zmax = \{1,2\}$

Esempio: Convergenza vs Divergenza

- Dato un lts TS = (Q, A, →), uno stato q è convergente se può raggiungere uno stato di deadlock (esiste una computazione che va in deadlock), mentre è divergente se può eseguire una computazione infinita.
- N.B: uno stato q deve essere "convergente o divergente", ma può anche essere sia convergente che divergente.

Convergenza come minimo punto fisso

- 2^Q è un reticolo completo finito se Q è finito
- C: $2^Q \rightarrow 2^Q$ definita sotto è monotona

$C(X) = \{q \mid \exists q'. q \xrightarrow{\mu} q', q' \in X\} \cup \{q \mid q \text{ è deadlock}\}$

$C^1(\varnothing) = \{q \mid q \text{ è deadlock}\}$, ovvero stati che con al più zero transizioni raggiungono un deadlock

$C^2(\varnothing) = C(\{q \mid q \text{ è deadlock}\})$ = stati che possono fare una transizione e poi andare in deadlock o che sono già in deadlock, ovvero stati che eseguendo al più una transizione possono andare in deadlock

$C^k(\varnothing)$ = stati che eseguendo al più k-1 transizioni possono andare in deadlock

Divergenza come massimo punto fisso

- 2^Q è un reticolo completo finito se Q è finito
- D: $2^Q \rightarrow 2^Q$ definita sotto è monotona

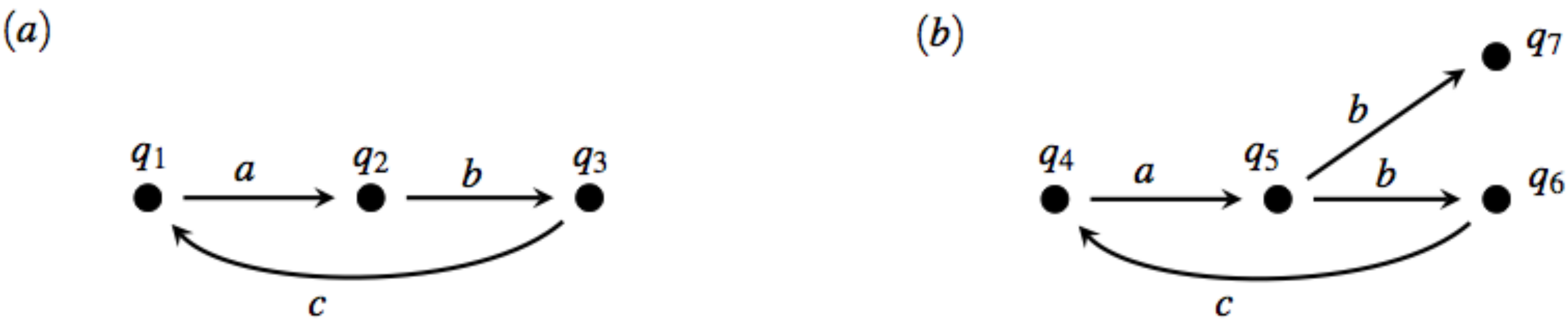
$D(X) = \{q \mid \exists q'.q \xrightarrow{\mu} q', q' \in X\}$

$D^1(Q) = \{q \mid \exists q'.q \xrightarrow{\mu} q', q' \in Q\}$, ovvero stati che possono fare almeno una transizione

$D^2(Q)$ = stati che possono fare una transizione ed arrivare su $D^1(Q)$, ovvero stati che possono fare almeno 2 transizioni

$D^k(Q)$ = stati che possono fare almeno k transizioni

In pratica ...



$C^1(\varnothing) = \{q7\}$ $C^2(\varnothing) = \{q7,q5\}$ $C^3(\varnothing) = \{q7,q5,q4\}$

$C^4(\varnothing) = \{q7,q5,q4,q6\} = C^5(\varnothing)$

$D^1(Q) = Q \setminus \{q7\} = \{q1,q2,q3,q4,q5,q6\}$

$D^2(Q) = Q \setminus \{q7\}$

Esercizio

- Uno stato è sempre convergente se tutte le sue computazioni terminano. Caratterizza l'insieme degli stati sempre convergenti come minimo punto fisso di una funzione SC. È l'insieme Zmin di SC il complemento dell'insieme Zmax di D (divergenti)?
- Uno stato è sempre divergente se tutte le sue computazioni non raggiungono mai un deadlock. Caratterizza l'insieme degli stati sempre divergenti come massimo punto fisso di una funzione SD. È l'insieme Zmax di SD il complemento dell'insieme Zmin di C (convergenti)?

Complemento di un max/min punto fisso

Suppose $f : 2^S \rightarrow 2^S$ is monotonic.

$$Z_{max} = \cup\{X \subseteq S \mid X \subseteq f(X)\}$$

What is the complement of Z_{max}, i.e. $\overline{Z_{max}} = S - Z_{max}$?

$\overline{Z_{max}} = \overline{\cup\{X \mid X \subseteq f(X)\}} = \cap\{\overline{X} \mid X \subseteq f(X)\} = \cap\{Y \mid \overline{Y} \subseteq f(\overline{Y})\} = \cap\{Y \mid \overline{f(\overline{Y})} \subseteq Y\} = \cap\{Y \mid f_d(Y) \subseteq Y\}$

where $f_d(Y) = \overline{f(\overline{Y})}$ (f_d is the dual function to f)
We note that f_d is monotonic
$X \subseteq Y \Rightarrow \overline{Y} \subseteq \overline{X} \Rightarrow f(\overline{Y}) \subseteq f(\overline{X}) \Rightarrow \overline{f(\overline{X})} \subseteq \overline{f(\overline{Y})} \Rightarrow f_d(X) \subseteq f_d(Y))$
and thus

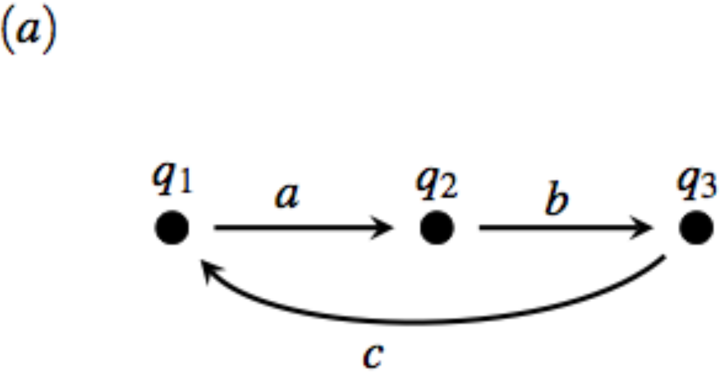
Observation

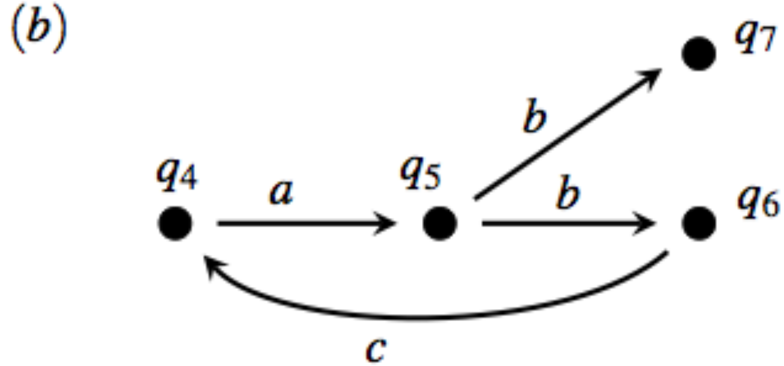
The complement of the greatest fixed point of f is the least fixed point of the dual function f_d.

Esempio

- $D(X) = \{q \mid \exists q'. q \xrightarrow{\mu} q', q' \in X\}$
- Cos'è la funzione duale 'D('X) ? – uso il pre-apice come complemento
- $'D(X) = \{q \mid \text{non } \exists q'. q \xrightarrow{\mu} q', q' \in X\} =$
  $\{q \mid \forall q'. q \xrightarrow{\mu} q', q' \notin X\}$
- $'D('X) = \{q \mid \forall q'. q \xrightarrow{\mu} q', q' \in X\} = SC(X)$

Quindi $'Zmax(D) = Zmin(SC)$ e, simmetricamente, $'Zmin(SC) = Zmax(D)$.





$D^1(Q) = Q \setminus \{q7\} = \{q1,q2,q3,q4,q5,q6\}$

$D^2(Q) = Q \setminus \{q7\}$

$SC^1(\varnothing) = \{q7\} = SC^2(\varnothing)$

$C^1(\varnothing) = \{q7\}$ $C^2(\varnothing) = \{q7,q5\}$ $C^3(\varnothing) = \{q7,q5,q4\}$

$C^4(\varnothing) = \{q7,q5,q4,q6\} = C^5(\varnothing)$

$SD^1(Q) = \{q1,q2,q3,q4,q5,q6\}$

$SD^2(Q) = \{q1,q2,q3,q4,q6\}$

$SD^3(Q) = \{q1,q2,q3,q6\}$

$SD^4(Q) = \{q1,q2,q3\} = SD^5(Q)$

Esercizio

- $C(X) = \{q \mid \exists q'. q \xrightarrow{\mu} q', q' \in X\} \cup \{q \mid q$ è deadlock$\}$
- Com'è fatta la funzione duale $'C('X)$?

Soluzione:

- $'C('X) = \{q \mid \text{non } \exists q'. q \xrightarrow{\mu} q', q' \in {}'X\} \cap \{q \mid q$ non è deadlock$\}$ =

  $\{q \mid \exists q'. q \xrightarrow{\mu} q'$ and $\forall q'. q \xrightarrow{\mu} q', q' \in X\}$ = $SD(X)$