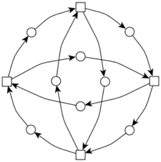
UNIVERSITÀ DEGLI STUDI DI MILANO–BICOCCA

CORSO DI LAUREA MAGISTRALE IN INFORMATICA

MODELLI DELLA CONCORRENZA

LOGICHE TEMPORALI E MODEL-CHECKING



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 $y \leq x$; $\quad x < y$ significa $(x \leq y \wedge x \neq y)$; $y > x \ldots$

Insiemi parzialmente ordinati

(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

Insiemi parzialmente ordinati

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

Insiemi parzialmente ordinati

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 $B_* \neq \emptyset$

Insiemi parzialmente ordinati

$x \in B$ 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

Insiemi parzialmente ordinati

$x \in B$ 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 $y = x$

Insiemi parzialmente ordinati

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

Insiemi parzialmente ordinati

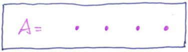
Esempi:

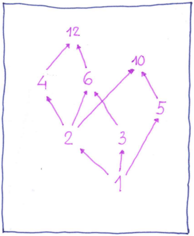
$(2^A, \subseteq)$ dove A è un insieme qualsiasi

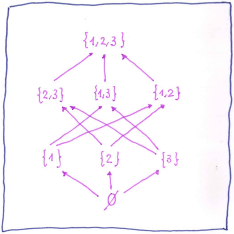
$(\mathbb{N}^+, |)$ dove $|$ indica la relazione *divide* (ad es. $3 \mid 27$, $5 \not| \, 27$)

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

Insiemi parzialmente ordinati







Reticoli

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

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 $B \subseteq L$

Funzioni e punti fissi

Consideriamo funzioni $f : X \to X$

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

(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: $\mathbb{R}$

Insiemi parzialmente ordinati e funzioni monotòne

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

Una funzione $f : A \to B$ si dice monotòna se, per ogni $x, y \in A$, vale $x \leq y \longrightarrow f(x) \leq f(y)$

Funzioni monotòne e punti fissi

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

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

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

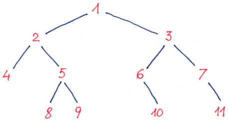
Funzioni monotòne e punti fissi

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

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

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

Funzioni monotòne e punti fissi



$A = \{1, \dots, 11\}$

$(\mathbb{P}(A), \subseteq)$

$f : \mathbb{P}(A) \to \mathbb{P}(A)$

$f(S) = S \cup \{ x \in A \mid x \text{ è figlio di un } y \in S \}$

$f(\{2,6\}) = \{2, 6, 4, 5, 10\}$ $\qquad f(\{2,6\}) \neq \{2,6\}$

$f(\{2,6,4,5,10\}) = \{2,6,4,5,10,8,9\} = M$

$f(M) = M \qquad f(\emptyset) = S$

Teorema di Knaster-Tarski

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

Caso particolare: $L = 2^A$, per un insieme A

Teorema di Knaster-Tarski – dimostrazione

Dimostriamo il teorema nel caso particolare,

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

Teorema di Knaster-Tarski – dimostrazione

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

Gli elementi di Z saranno chiamati punti pre-fissi

Teorema di Knaster-Tarski – dimostrazione

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

Gli elementi di Z saranno chiamati punti pre-fissi

L'insieme Z non può essere vuoto. Perché?

Teorema di Knaster-Tarski – dimostrazione

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

Gli elementi di Z saranno chiamati punti pre-fissi

Osservazione: se f ha dei punti fissi, Z li contiene tutti

Teorema di Knaster-Tarski – dimostrazione

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

Gli elementi di Z saranno chiamati punti pre-fissi

Poniamo $\boxed{m = \bigcap Z}$

Teorema di Knaster-Tarski dimostrazione

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

Gli elementi di Z saranno chiamati punti pre-fissi

Poniamo $m = \bigcap Z$

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

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

Teorema di Knaster-Tarski dimostrazione

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

Gli elementi di Z saranno chiamati punti pre-fissi

Poniamo $m = \bigcap Z$

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

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

Teorema di Knaster-Tarski – dimostrazione

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

Teorema di Knaster-Tarski – dimostrazione

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

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

Teorema di Knaster-Tarski – dimostrazione

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

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

quindi $\boxed{m \in Z}$

Teorema di Knaster-Tarski – dimostrazione

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

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

quindi $\boxed{m \in Z}$

Osservazione: $m = \min Z$

Teorema di Knaster-Tarski – dimostrazione

$$f(\mathfrak{m}) \subseteq \mathfrak{m}$$

Teorema di Knaster-Tarski – dimostrazione

$$f(\mathfrak{m}) \subseteq \mathfrak{m}$$

f è monotòna, quindi

$$f(f(\mathfrak{m})) \subseteq f(\mathfrak{m})$$

Teorema di Knaster-Tarski – dimostrazione

$$f(m) \subseteq m$$

f è monotòna, quindi

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

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

Teorema di Kleene

Sia $f : 2^A \to 2^A$ monotòna

La funzione f si dice continua se

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

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

Teorema di Kleene

Sia $f : 2^A \to 2^A$ monotòna

La funzione f si dice continua se

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

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

$$\boxed{f(\bigcup X_i) = \bigcup f(X_i)}$$

Teorema di Kleene

Se f è continua, allora

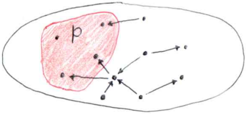
(1) il minimo punto fisso di f si può ottenere calcolando

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

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

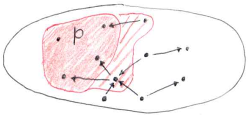
$$f(A), \quad f(f(A)), \quad f(f(f(A))), \quad \cdots$$

Teoremi di punto fisso e logiche temporali



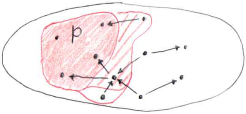
Fp

Teoremi di punto fisso e logiche temporali



Fp

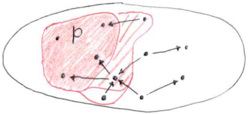
Teoremi di punto fisso e logiche temporali



$F\,p$

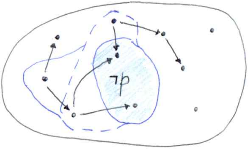
min punto fisso

Teoremi di punto fisso e logiche temporali



Fp

min punto fisso



Gp

max punto fisso

Un algoritmo per CTL

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

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

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

Un algoritmo per CTL

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

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

Un algoritmo per CTL

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

Consideriamo la formula $\alpha \equiv \mathsf{EG}\,\beta$

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

Algoritmi per LTL

Automi finiti che riconoscono parole infinite su un alfabeto finito Σ (a. di Büchi)

$$\mathcal{B} = (Q, q_0, \delta, F)$$

- Q: insieme finito di stati (*locations*)
- $q_0 \in Q$: stato iniziale
- $\delta \subseteq Q \times \Sigma \times Q$: relazione di transizione
- $F \subseteq Q$: insieme degli stati accettanti

Una parola infinita $w = a_0 a_1 \cdots$ è accettata da $\mathcal{B}$ se la sequenza corrispondente di stati $q_0 q_1 \cdots$ passa infinite volte per almeno uno stato in F

Algoritmi per LTL

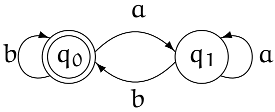
Automi finiti che riconoscono parole infinite su un alfabeto finito Σ (a. di Büchi)

$$\mathcal{B} = (Q, q_0, \delta, F)$$

- Q: insieme finito di stati (*locations*)
- $q_0 \in Q$: stato iniziale
- $\delta \subseteq Q \times \Sigma \times Q$: relazione di transizione
- $F \subseteq Q$: insieme degli stati accettanti

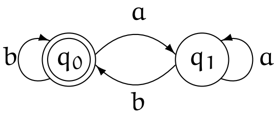
Il problema $L(\mathcal{B}) = \emptyset$? è decidibile

Algoritmi per LTL



$$
\begin{aligned}
w_1 &= \mathtt{bbbbbbbb}\cdots \\
w_2 &= \mathtt{bbaaabbbb}\cdots \\
w_3 &= \mathtt{babababab}\cdots \\
w_4 &= \mathtt{baabbbaaa}\cdots
\end{aligned}
$$

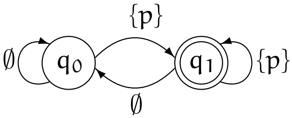
Algoritmi per LTL



$w_1 = \mathrm{bbbbbbbb}\cdots$ sì
$w_2 = \mathrm{bbaaabbbb}\cdots$ sì
$w_3 = \mathrm{babababab}\cdots$ sì
$w_4 = \mathrm{baabbbaaa}\cdots$ no

Un algoritmo per LTL

GF p



$$w_1 = \emptyset\{p\}\{p\}\emptyset\{p\}\emptyset\emptyset\cdots \qquad \text{no}$$
$$w_2 = \emptyset\{p\}\emptyset\{p\}\emptyset\{p\}\emptyset\cdots \qquad \text{sì}$$

Un algoritmo per LTL

Problema: verificare se α è vera in (M, q_0)

(1) Costruiamo l'automa $\mathcal{B}_{\neg\alpha}$

(2) Trasformiamo M in un automa etichettato da insiemi di proposizioni atomiche

(3) Calcoliamo il prodotto sincrono dei due automi $\mathcal{PS}$

(4) Se $L(\mathcal{PS}) = \emptyset$, allora $M, q_0 \models \alpha$

Il calcolo μ

Un linguaggio logico che permette di definire formule ricorsive

Il calcolo μ

Supponiamo di avere un solo operatore temporale: X. Come esprimere la proprietà $\mathrm{EF}\,\alpha$?

Il calcolo μ

Supponiamo di avere un solo operatore temporale: X. Come esprimere la proprietà $\mathsf{EF}\,\alpha$?

$$\mathsf{EF}\,\alpha \equiv \alpha \vee \mathsf{EX}\,\alpha \vee \mathsf{EXEX}\,\alpha \vee \cdots$$

Il calcolo μ

Supponiamo di avere un solo operatore temporale: X. Come esprimere la proprietà EF α?

$$\mathrm{EF}\,\alpha \equiv \alpha \vee \mathrm{EX}\,\alpha \vee \mathrm{EXEX}\,\alpha \vee \cdots$$

“Raccogliamo” EX:

$$\mathrm{EF}\,\alpha \equiv \alpha \vee \mathrm{EX}\,(\alpha \vee \mathrm{EX}\,\alpha \vee \mathrm{EXEX}\,\alpha \vee \cdots)$$

Il calcolo μ

Supponiamo di avere un solo operatore temporale: X. Come esprimere la proprietà $\mathsf{EF}\,\alpha$?

$$\mathsf{EF}\,\alpha \equiv \alpha \vee \mathsf{EX}\,\alpha \vee \mathsf{EXEX}\,\alpha \vee \cdots$$

"Raccogliamo" EX:

$$\begin{aligned}\mathsf{EF}\,\alpha &\equiv \alpha \vee \mathsf{EX}\,(\alpha \vee \mathsf{EX}\,\alpha \vee \mathsf{EXEX}\,\alpha \vee \cdots)\\ &\equiv \alpha \vee \mathsf{EX}(\mathsf{EF}\,\alpha)\end{aligned}$$

Il calcolo μ

Supponiamo di avere un solo operatore temporale: X. Come esprimere la proprietà $\mathsf{EF}\,\alpha$?

$$\mathsf{EF}\,\alpha \equiv \alpha \vee \mathsf{EX}\,\alpha \vee \mathsf{EXEX}\,\alpha \vee \cdots$$

"Raccogliamo" EX:

$$\begin{aligned} \mathsf{EF}\,\alpha &\equiv \alpha \vee \mathsf{EX}\,(\alpha \vee \mathsf{EX}\,\alpha \vee \mathsf{EXEX}\,\alpha \vee \cdots) \\ &\equiv \alpha \vee \mathsf{EX}(\mathsf{EF}\,\alpha) \end{aligned}$$

$$\mu Y.(\alpha \vee \mathsf{EX}\,Y)$$

Il calcolo μ

Supponiamo di avere un solo operatore temporale: X. Come esprimere la proprietà $AG\,\alpha$?

$$AG\,\alpha \equiv \alpha \wedge AX\,\alpha \wedge AXAX\,\alpha \wedge \cdots$$

"Raccogliamo" AX:

$$\begin{aligned} AG\,\alpha &\equiv \alpha \wedge AX\,(\alpha \wedge AX\,\alpha \wedge AXAX\,\alpha \wedge \cdots) \\ &\equiv \alpha \wedge AX(AG\,\alpha) \end{aligned}$$

$$\nu Y.(\alpha \wedge AX\,Y)$$

Il calcolo μ

$AP = \{p_1, p_2, \cdots, q, r, \cdots\}$ proposizioni atomiche

Siano α e β due formule

1. $\alpha \vee \beta$, $\neg\alpha$ sono formule
2. $EX\,\alpha$, $AX\,\alpha$ sono formule
3. $\mu Y.f(Y)$ è una formula, dove f è una formula nella quale compare Y (con restrizioni sulle negazioni)
4. $\nu Y.f(Y)$ è una formula, dove f è una formula nella quale compare Y (con restrizioni sulle negazioni)

La semantica del calcolo μ è definita su modelli di Kripke attraverso operatori di punto fisso

Il calcolo μ

$$\boxed{CTL^* \subset \mu - \text{calculus}}$$

Calcolo μ: massima potenza espressiva, alta complessità, potenziale "oscurità" delle formule

Complessità e aspetti algoritmici

M: modello di Kripke f: formula

$$\text{CTL: } O(|M| \times |f|) \qquad \text{LTL: } O(|M| \times 2^{|f|})$$

Le stime di complessità vanno interpretate *cum grano salis*

Strategie algoritmiche:

- Rappresentazioni simboliche (OBDD)
- Partial order reduction (unfolding)
- Traduzione in SAT