Lezione 20 18/12/2023

Esercizio

Esercizio che non esce in esame ma può essere chiesto all'orale

Tradurre in LTL i seguenti enunciati

"Chi ruba, presto o tardi finirà in galera"

"Per superare l'esame, è necessario avere studiato"

"Se la cabina è in movimento verso l'alto, si trova all'altezza del secondo piano, ed è stato premuto il pulsante interno di richiesta del quinto piano, la cabina non cambierà direzione fino a quando avrà raggiunto il quinto piano"

Strategia: individuare le proposizioni atomiche; analizzare la struttura della frase, eventualmente riformulandola

Dobbiamo individuare nella frase gli elementi che possono corrispondere a proposizioni atomiche.

Tenendo conto che una proposizione atomica non è scomponibile dal punto di vista logico, e deve esprimere una caratteristica del sistema tale da poter stabilire in un dato stato del sistema se è vera o falsa immediatamente, cioè senza considerare altro.

Partiamo dalla prima frase. Un verbo esprime un'azione che molto spesso descrive un passaggio di stato. A noi invece interessano proposizioni atomiche che descrivano proprietà di uno stato. Ripensiamo alla frase facendo riferimento alle caratteristiche degli stati. Se rubo, passo da uno stato dove non ho rubato niente ad uno dove sono autore del furto. (per comodità parlo in prima persona, ma intendo un soggetto generico). Questa può essere una prima proposizione atomica.
Un'altra è "sono in galera".

In questo tipo di esercizio ci possono essere diverse formule che esprimono correttamente il contenuto della frase.

"Chi ruba, presto o tardi finirà in galera"

Proposizioni atomiche: hr = "ho rubato"; c = "sono in carcere"

$$G\,(hr \longrightarrow XF\,c)$$

Questa è una “legge universale” quindi mettiamo G davanti perché una cosa che vale sempre.

La formula dice che è sempre vero che se ho compiuto un furto, nel futuro sarò in galera. è stato aggiunto l’operatore X per evitare che la soluzione sia un sistema dove contemporaneamente rubo e sono in galera. Così sto dicendo che se rubo qualcosa, a partire dal prossimo stato del sistema, prima o poi (F) sarò in galera.

“Solo chi ruba finirà in galera”

$$\neg c \, W \, hr$$

Consideriamo questa variante. Qui abbiamo usato un until debole, la formula dice che non vado in galera fino a quando non rubo. Qui si potrebbe usare anche l’implicazione.

“Chi ruba finirà in carcere, ma solo dopo avere parlato con un avvocato”

pa = “ho parlato con un avvocato”

$$G\,(hr \longrightarrow (XF\,c \wedge (\neg c \,U\, pa)))$$

Un’altra variante. Una possibile soluzione è quella che aggiunge la proposizione atomica del parlare con un avvocato, questa soluzione dice che è sempre vero che se ho rubato, allora prima o poi finirò in carcere e contemporaneamente …

Negli stati in cui non ho rubato niente la formula è già vera quindi è a posto.

“Se la cabina è in movimento verso l’alto, si trova all’altezza del secondo piano, ed è stato premuto il pulsante interno di richiesta del quinto piano, allora la cabina non cambierà direzione fino a quando avrà raggiunto il quinto piano”

Proposizioni atomiche: su=“cabina sta salendo”, p_i=“cabina all’altezza del piano i, r_i=“pulsante interno del piano i è stato premuto”

$$G\,((su \wedge p_2 \wedge r_5) \longrightarrow (su \,U\, p_5))$$

è sempre vero che se “cabina in salita” “secondo piano” “richiesta del quinto piano” allora dall’istante in cui valgono queste condizioni, la cabina deve continuare a salire fino a quando si arriva al quinto piano.

Limiti espressivi di LTL

La logica temporale lineare non riesce ad esprimere proprietà che dipendono dall’esistenza di un particolare cammino con date caratteristiche.

LTL non è in grado di esprimere proprietà del tipo

esiste un cammino in cui α

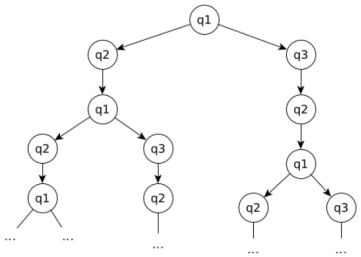
Esempi:

"è sempre possibile ritornare allo stato iniziale",
"se il processo P chiede la risorsa, è possibile raggiungere uno stato di *deadlock*"

"è possibile" senza chiedere che si debba per forza tornare non è descrivibile.

Nell'analisi e progettazione di sistemi reattivi questo può essere importante, quindi la soluzione consiste nel definire un nuovo linguaggio logico.

Alberi di computazione



Computazione: cammino nell'albero a partire dalla radice

Qui stiamo rappresentando sistemi tramite stati globali.

L'idea è che abbiamo un sistema di transizioni, fissiamo uno stato iniziale q1 e costruiamo questo albero induttivamente:

- Osserviamo quali sono le transizioni immediate da questo stato, in questo esempio a partire da q1 abbiamo due transizione, una verso q2 e una verso q3.

Proseguo ricorsivamente, da q2 vedo che posso solo tornare a q1 ma al posto di tornare indietro come in un sistema di transizioni vado avanti.

Computation Tree Logic – sintassi

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

Definiamo FBF_{CTL}

per ogni $p \in AP$, $p \in FBF_{CTL}$

Per ogni $\alpha, \beta \in FBF_{CTL}$

1. $\neg\alpha$, $\alpha \vee \beta \in FBF_{CTL}$
2. $AX\,\alpha, EX\,\alpha \in FBF_{CTL}$
3. $AF\,\alpha, EF\,\alpha \in FBF_{CTL}$
4. $AG\,\alpha, EG\,\alpha \in FBF_{CTL}$
5. $A(\alpha\,U\,\beta) \in FBF_{CTL}, E(\alpha\,U\,\beta) \in FBF_{CTL}$

Definiamo ricorsivamente le formule ben formate di CTL.

Ogni formula atomica è accettabile, possiamo combinarle con connettivi logici.

Vogliamo che questa sia comunque una logica temporale, quindi abbiamo gli stessi .. temporali della LTL ma vogliamo anche poter distinguere tra proprietà che sono vere per tutti i

cammini e proprietà che dipendono dall'esistenza di un cammino.

"A" quantificatore universale (letto: per ogni cammino) "E" quantificatore esistenziale (letto: esiste un cammino)

$AX\alpha$ "per ogni cammino, nel prossimo stato vale α". (come LTL)

$EX\alpha$ "esiste un cammino dove nel prossimo stato vale α".

Nel caso di LTL per la semantica abbiamo specificato quando un singolo cammino specifica una formula (per questo è chiamata logica lineare, si possono considerare cammini lineari indipendenti tra di loro). In CTL invece la validità di una formula nel cammino dipende dalla struttura dell'albero di computazione, cioè non solo dagli stati nel cammino ma anche da quelli delle altre diramazioni che avrei potuto seguire.

EFalpha significa "esiste un cammino a partire dallo stato corrente in cui prima o poi vale alpha".

A e E sono quantificatori sui cammini:

A: per ogni cammino

E: esiste un cammino tale che

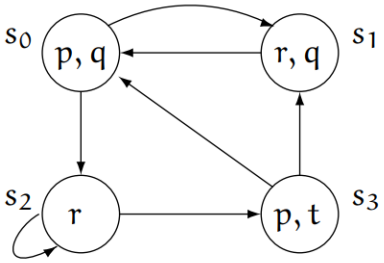
"Dopo l'accensione della spia, sarà sempre possibile riportare il sistema allo stato iniziale"

s: la spia è accesa
init: il sistema si trova nello stato iniziale

$$\mathrm{AG}\,(s \longrightarrow \mathrm{AX}\,\mathrm{EF}\,\mathrm{init})$$

"per ogni cammino è sempre vero che se la spia è accesa, dallo stato successivo esiste un cammino in cui prima o poi torno allo stato iniziale".

Esercizio



Abbiamo un modello con 4 stati (s0-s3) e 4 proposizioni atomiche (s,p,r,q). Non è specificato uno stato iniziale, l'esercizio chiede di determinare la validità delle formule in tutti gli stati del modello.

(a) $AF\,q$

(a) (formula sia LTL (scritta senza A, il quantificatore universale è implicito) che CTL). La formula dice che per ogni cammino, prima o poi q diventerà vera. Qui compare q, potremmo iniziare a trovare gli stati dove vale q (s0, s1). Negli stati dove vale q, vale anche Fq (prima o poi q). Quindi possiamo già concludere che in s0 e s1 la formula è vera. Vediamo gli altri due stati. In s3 posso andare in s0 o s1, in entrambi i cammini si arriva ad uno stato dove vale q. Nello stato s2 invece non vale, perché c'è un cammino massimale che rimane per sempre in s2, e qui q non diventa mai vera.

(b) $AG\,(EF\,(p \vee q)), \quad GF\,(p \vee q)$

La prima è una formula CTL, la seconda è LTL e non può essere scritta come CTL perché anche se mettiamo in testa il quantificatore universale, rimane il fatto che la F non ha associato un quantificatore.

Partiamo dalla seconda come LTL "per ogni cammino è sempre vero che p o q". Devo dimostrare che F non solo è valida nello stato iniziale, ma rimane valida in ogni stato del cammino, perché c'è la G davanti. In s0 non è vera perché posso andare in s2 e rimanere bloccato nel cammino massimale. Quindi anche se all'inizio p o q è vera, dopo diventa falsa.
In s1 come prima posso raggiungere s2 quindi è falsa. Analogamente in s3. A maggior ragione anche s2 falsa.

Consideriamo la formula CTL, abbiamo anche i quantificatori sui cammini. In s2 posso raggiungere s3 dove è vera p o q. Quindi è vero che c'è un cammino che parte da s2 e rimane in s2 dove non vale p o q, ma vedo che a partire da ogni stato ESISTE un cammino dove prima o poi vale p o q. Quindi la formula è vera in tutti gli stati.

(c) $EX\,(EX\,r), \quad XX\,r$

XXr (LTL) dice che tra due istanti varrà r. Da s0 c'è il cammino che va in s2 e poi va in s3, dove la proprietà

non vale. Da s1 tra due istanti mi trovo in s1 o in s2. In entrambi i casi vale r quindi la formula è verificata.

Consideriamo la variante CTL con i quantificatori esistenziali. Qui basta l'esistenza, esiste un cammino che parte da s0 che tra 2 passaggi si trova in uno stato dove vale r? si, posso andare in s2 e poi rimango in s2.

(d) $AG(AF\,q)$

Consideriamola nella forma CTL, dice che per ogni cammino è sempre vero che per ogni cammino prima o poi vale q. Possiamo leggerla come "q è inevitabile". Questa non vale in s2 perché il cammino che rimane sempre in s2 non valida q. Se all'interno ci fosse l'esiste questa formula sarebbe validata in s2.

Equivalenza tra formule

$$\alpha \equiv \beta \quad \text{se e solo se } \forall \pi : (\pi \models \alpha \longleftrightarrow \pi \models \beta)$$

diciamo che alpha e beta sono equivalenti se per ogni cammino (e in qualunque modello) alpha è vera nel cammino sse beta è vera in quel cammino. Questa è una relazione molto forte, dice che alpha e beta esprimono la stessa proprietà.

Dal punto di vista sintattico LTL e CTL sono diverse, ma a noi non interessa la differenza nella forma, potrebbe darsi che per ogni formula LTL ce ne sia una equivalente CTL e vice versa.

Confronto tra LTL e CTL

Molte proprietà interessanti si possono esprimere sia in LTL sia in CTL

Invarianti

$AG\,\neg p$ $\quad$ $G\,\neg p$

Reattività

$AG(p \longrightarrow AF\,q)$ $\quad$ $G(p \longrightarrow F\,q)$

In entrambe le logiche possiamo definire un'invariante, la differenza tra le due formule è formale dato che in LTL il quantificatore universale è implicito.

In LTL possiamo scrivere la reattività come "è sempre vero che se è vero p (servizio) allora prima o poi sarà vera q (reazione)". Possiamo scrivere la formula equivalente in CTL applicando

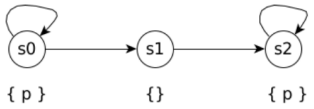
quantificatori universali agli operatori temporali della formula.

AG EF p (*reset property*): "da ogni stato raggiungibile in ogni cammino è sempre possibile raggiungere uno stato nel quale vale p"

In CTL posso scrivere una formula come questa, che non è esprimibile in LTL.

FG p: "in ogni cammino, prima o poi si raggiungerà uno stato a partire dal quale p rimane sempre vera"

Questa proprietà non si può esprimere in CTL



sintatticamente questa è una formula LTL che non possiamo leggere come CTL, perché anche aggiungendo l'operatore universale all'inizio, l'operatore G rimarrebbe senza quantificatore.

In questo sistema di transizioni p è vera in s0 e s2. In s1 p non vale. Valutiamo la formula FGp, supponiamo che s0 sia lo stato iniziale. Abbiamo 2 cammini massimali: quello che rimane sempre in s0, e quello che fa un po' di cicli su s0 (da 0 in su, numero finito) e poi va in s1 e poi infinitamente in s2.
In entrambi i cammini massimali la formula è vera.

Proviamo a vedere se si può esprimere la stessa proprietà in CTL.

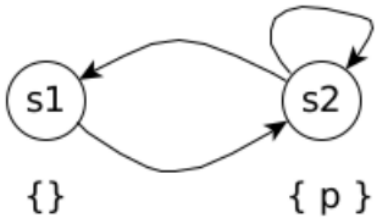
$$M, s_0 \models \mathrm{FG}\, p \quad M, s_0 \not\models \mathrm{AF\,AG}\, p$$

Proviamo ad aggiungere quantificatori universali. Vediamo se per ogni cammino prima o poi raggiungiamo uno stato a partire dal quale per ogni cammino è sempre vera p. Nel cammino che rimane sempre in s0 non è vero che ogni cammino da lì vale p, perché potrei decidere di spostarmi a s1 e lì per un istante non vale più p.
Perché la formula vuole che dopo quel "prima o poi" per ogni cammino vale sempre p. Quindi questa formula non è equivalente all'altra LTL.

$M, s_0 \models AF\,EG\,p$!

Consideriamo il secondo quantificatore esistenziale. Per ogni cammino prima o poi raggiungo uno stato a partire del quale è possibile che valga Gp. Questa formula è verificata in s0.

Questo non vuol dire che le formule siano per forza equivalenti, dice solo che sono equivalenti in questo sistema di transizioni.



Consideriamo questo secondo modello

La prima formula è verificata in s1 perché per ogni cammino, prima o poi raggiungo lo stato (s2) a partire dal quale p è sempre vera.

$M, s1 \models AF\,EG\,p$ $M, s1 \not\models FG\,p$

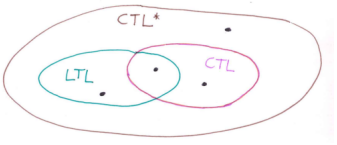
La seconda invece non è verificata in s1 perché non è vero che per ogni cammino prima o poi raggiungo uno stato dove è vera Gp.

Rispetto a questo modello le due formule non sono equivalenti, e quindi non sono equivalenti in generale.

CTL e LTL non sono fra di loro confrontabili, una non è più espressiva dell'altra. In CTL posso esprimere proprietà con l'esistenza di un cammino, ma in LTL ne ho altre che non posso esprimere in CTL.

La logica CTL* estende sia LTL sia CTL, mantenendo i due quantificatori sui cammini, ma eliminando il vincolo di CTL

$AFG\,p \vee AF\,EG\,q$ $EFG\,q$



In CTL* posso esprimere tutto quello che posso esprimere in CTL, LTL e qualcosa in più (come quest'ultima formula).

Più una logica è espressiva, più sono costosi gli algoritmi che validano le formule. Per questo siamo partiti da LTL e CTL.