Formal methods - Temporal logic

Francesco Penasa

March 13, 2020

1 LTL vs CTL

1. many CTL formulas connt be expressed in LTL
2. many LTL formulas cannot be expressed in CTL
3. some formulas can be expressed both in LTL and in CTL

LTL reason in terms of all path from the beginning (medieval metaphor). CTL reason in every single state in the path. Everything in this form $GFsomething \rightarrow something$ don't have an equivalent in CTL. LTL = techniques based with automata CTL = techniques based with symbolic M.C.

2 CTL*

Unified framework (super logic) that contain CTL and LTL.

$$M, s \models AE\psi \ iff \ M, s \models E\phi$$

With a nested path quantifier implicitly we consider only the inner one. Substantially, as CTL but X, G, F, U are not necessarily precede by A, E.

3 CTL* vs LTL & CTL)

There are formula than can't be represented neither in CTL nor in LTL but in CTL* (e.g. $E(GFp \rightarrow GFp)$)

$$LTL \ U \ CTL \in CTL*$$

4 Fairness & Fair Kripke Models

Consider a variant of the mutual exclusion in which one process can stay permanently in the critical zone

$$M \models AG(T_1 \rightarrow AFC_1), M \models AG(T_2 \rightarrow AFC_2)$$

Nope.

It is desirable that certain (typically Boolean) conditions ϕ hold infinitely often: $AGAF\phi$ ($GF\phi$ in LTL). These are called **fairness conditions**. Fairness condition:

$$\neg EFEG\neg\phi$$

(it is never reached a state from which ϕ is forever false)

Example: it is not desirable that, once a process is in the critical section, it never exists: $AGAF\neg C_1$ ($\neg EFEGC_1$)

Fair Kripke models A Fair Kripke model $M_f := (S, R, I, AP, L, F)$
F: a set of fairness conditions F = $f_1, ..., f_n$ with $f_i \in S$
E.g. 2 := GFq
Fair path π: at least one state for each f_i occurs infinitely often in π (ϕ_i holds infinitely often in $\pi : \pi \models GF\phi_i$)
Fair state: it lays on at least one fair path.
In CTL Fairness conditions **cannot** be encoded into the formula itself. In LTL Fairness conditions **can** be encoded into the formula itself GFf_i.

5 Exercises

Improved Labeled CNF-ization Consider the following Boolean formula ϕ

$$((\neg A_1 \wedge \neg A_2) \vee (A_7 \wedge A_4) \vee (\neg A_3 \wedge A_2) \vee (A_5 \wedge \neg A_4))$$

Using the *improved* CNF_{label} conversion, produce the CNF formula $CNF_{label}(\phi)$. *Substantially, we have to transform in CNF* $B_1 \rightarrow (\neg A_1 \wedge \neg A_2)$

$$(B)\wedge$$

$$(\neg B \vee B_1 \vee B_2 \vee B_3 \vee B_4)\wedge$$

$$(\neg B_1 \vee \neg A_1) \wedge (\neg B_1 \wedge \neg A_2)\wedge$$

$$...$$

$$(\neg B_4 \vee A_5) \wedge (\neg B_4 \vee \neg A_4)$$

NNF conversion NNF = negative normal form is the form in which a form is written as $\wedge$ and $\vee$ and all negations are written on the bottom at literal level. *Substantially, put all negations near to literals, and write all with OR and AND*

Consider the following boolean formula:

$$\neg(((\neg A_1 \rightarrow \neg A_2) \wedge ()$$

Compute the Negative Normal Form.

$$sdf$$

$$asd$$

we can expand the implication first OR we can remember $\neg(A \rightarrow B) = A \wedge \neg B$

$$sad$$

LTL Model Checking (path) Consider the following path π insert figure For each of the following facts, say if it is true or false in LTL.

1. $\pi, S_0 \models GFq$ TRUE
2. $\pi, S_0 \models FG(q \leftrightarrow \neg p)$ TRUE
3. $\pi, S_2 \models Gp$ FALSE
4. $\pi, S_2 \models pUq$ TRUE

LTL Model Checking Consider the following Kripke Model M insert figure For each of the following facts, say if it is true or false in LTL.

1. $M \models (pUq)$ TRUE
2. $M \models G(\neg p \rightarrow F\neg q)$ TRUE
3. $M \models Gp \rightarrow Gq$ TRUE all paths where Gp holds Gq holds.
4. $M \models FGp$ FALSE

CTL Model Checking Consider the following Kripke Model M insert figure For each of the following facts, say if it is true or false in CTL.

1. $M \models AF\neg p$ FALSE
2. $M \models EGp$ FALSE for ALL starting point EXIST one path where Gp
3. $M \models A(pUq)$ TRUE
4. $M \models E(pU\neg q)$ TRUE (in S_1 $pU\neg q$ is already verified).

CTL Model Checking Consider the following Kripke Model M insert figure For each of the following facts, say if it is true or false in CTL.

1. $M \models AF\neg q$ FALSE
2. $M \models EGq$ FALSE
3. $M \models ((AGAFp \vee AGAFq) \wedge (AGAF\neg p \vee AGAF\neg q)) \rightarrow q$ TRUE because in both initial state q is true.
4. $M \models AFEG(p \wedge q)$ FALSE

Fair CTL Model Checking Consider the following fair Kripke Model M insert figure For each of the following facts, say if it is true or false in CTL.

1. $M \models AF\neg p$ TRUE
2. $M \models A(pU\neg q)$ TRUE
3. $M \models AX\neg q$ FALSE
4. $M \models AGAF\neg p$ TRUE

We can loop in S_0 only a finite amount of time due to the fairness conditions.

Fair CTL Model Checking Consider the following fair Kripke Model M insert figure For each of the following facts, say if it is true or false in CTL.

1. $M \models EF(p \wedge q)$ TRUE
2. $M \models AGAFp$ FALSE
3. $M \models AF\neg q$ TRUE
4. $M \models AG(\neg p \vee \neg q)$ FALSE

We can loop in S_0 only a finite amount of time due to the fairness conditions.