Formal methods - Temporal logic

Francesco Penasa

March 10, 2020

2020 03 10

1 Summary

We have seen the behaviour of Kripke structure as **infinite set of computation paths** and **infinite computation tree**.

LTL extension of boolean logic with X(next) U(until) G(globally) F(finally) R(releases, give the permission to be false). LTL properties are evaluated over single paths. $G\phi$ is stronger than anyone.

1.1 LTL tableaux rules

Let ϕ_1 and ϕ_2 be LTL formulae:

$$G\phi_1 \Leftrightarrow (\phi_1 \vee XF\phi_1)$$
$$F\phi_1 \Leftrightarrow (\phi_1 \wedge XG\phi_1)$$
$$\phi_1 U\phi_2 \Leftrightarrow (\phi_2 \vee (\phi_1 \wedge X(\phi_1 U\phi_2)))$$
$$\phi_1 R\phi_2 \Leftrightarrow (\phi_2 \wedge (\phi_1 \vee X(\phi_1 R\phi_2)))$$

If appllied recursively, rewrite an LTL formula in terms of atomic and X-formulas:

$$(pUq) \wedge (G\neg p) \Rightarrow (q \vee (p \wedge X(pUq))) \wedge (\neg p \wedge XG\neg p)$$

Extremely important.

1.2 Some property

1. Fairness

$$G(T \rightarrow)$$

2 Computation Tree Logic CTL

2.1 Syntax

An atomic proposition is a CTL formula, as all his combinations plus the combination with the 8 temporal operators in CTL, AX, AU, AG, AF, EX, EU, EG, EF.
A = Necessarily, it applies to all path starting from the current point E = Possibly, it applies to at least one path starting from the current point. **Remember** that in this case we thinking in tree, when we say every possible successor we consider all the successors of a certain node.

1. AX necessarily next
2. EX possibly next
3. AF necessarily in the future (inevitably)
4. EF possibly in the future (possibly)
5. AG always true in all paths
6. $EG\phi$ there is at least one path where ϕ is always true.
7. $A(\phi U \psi)$ no matter what sooner or later in every path ϕ will hold.
8. $E(\phi U \psi)$

The figure is clearly self explaining. 03 60/108 While in LTL we use a state in a given path for the definition, here we usa a given state s_i and a given model M (situation). To sum up CTL properties are evaluated over trees. Universal modalities(AF,AG,AX,AU), Existential modalities(EF,EG,EX,EU). **It is based on the pair M, s_i called also a "situation".**
The CTL model checking problem $M \models \phi$ $M, s \models \phi$ **for every initial state** $s \in l$ of the Kripke structure.

2.2 CTL tableaux rules

Let ϕ_1 and ϕ_2 be CTL formulae:

1. $AF\phi_1 \Leftrightarrow (\phi_1 \vee AXAF\phi_1)$
2. $AG\phi_1 \Leftrightarrow (\phi_1 \wedge AXAG\phi_1)$
3. $A(\phi_1 U \phi_2) \Leftrightarrow (\phi_2 \vee (\phi_1 \wedge AXA(\phi_1 U \phi_2))$
4. $EF\phi_1 \Leftrightarrow (\phi_1 \vee EXEF\phi_1)$
5. $EG\phi_1 \Leftrightarrow (\phi_1 \wedge EXEG\phi_1)$
6. $E(\phi_1 U \phi_2) \Leftrightarrow (\phi_2 \vee (\phi_1 \wedge EXE(\phi_1 U \phi_2))$

Recursive definitions of AF, AG, AU, EF, EG, EU. If appllied recursively, rewrite a CTL formula in terms of atomic, AX- and EX- formulas:

$$A(pUq) \wedge (EG\neg p) \Rightarrow (q \vee (p \wedge AXA(pUq))) \wedge (\neg p \wedge EXEG\neg p)$$

2.3 Examples

TODO: add the figure
Mutual exclusion

$$M \models AG\neg(C_1 \wedge C_2)?$$

YES

Liveness

$$M \models AG(T_1 \rightarrow AF\ C_1)?$$

YES

Fairness

$$M \models AGAF\ C_1?$$

NO

Fairness(2)

$$M \models AGAF\ turn = 0?$$

NO

Blocking

$$M \models AG(N_1 \rightarrow EF\ T_1)?$$

YES

Blocking(2)

$$M \models AG(N_1 \rightarrow AF\ T_1)?$$

NO

example 6

$$M \models EG\ N_1?$$

YES

example 7

$$M \models AFEG\ N_1?$$

YES

If we use E we can observe that there is not a corresponding LTL formula.