LTL and CTL

Lecture Notes by Dhananjay Raju
draju@cs.utexas.edu

1 Linear Temporal Logic: LTL

Temporal logics are a convenient way to formalise and verify properties of reactive systems. LTL is an infinite sequence of states, where each state has a unique succesor. Therefore it establishes a total order on the set of states. Hence one can understand LTL formula's on a line.

LTL is built from the set of atomic propositions(AP),the logical operators $\neg$ and $\vee$, and the temporal modal operators $\mathbf{X}$ and $\mathbf{U}$. Formally, the set of LTL formulas over AP is inductively defined as follows:

- if $p \in AP$ then p is a valid LTL formula.
- if ψ, ϕ are valid LTL formulas, then $\neg\psi,\ \psi \vee \phi,\ \mathbf{X}\psi,\ \psi\mathbf{U}\phi$ are valid LTL formulas.

We have now defined the syntax for LTL. Note that we use only the $\mathbf{X}$ and $\mathbf{U}$ modalities for defining the valid formulas in LTL. We will define the sematics for LTL now. LTL formulas are interpreted over ω-words. More specifically they are interpreted over $(2^{AP})^{\omega}$. They can be viewed as a linear transition system where each state has a set of atomic propostions which are true. Formally, a model $\mathbf{M}, s \models \phi$ is defined inductively as follows:

- $M, s \models p$, if $p \in AP$ and $p \in w(s)$.
- $M, s \models \neg\phi$, if $M, s \not\models \phi$,.
- $M, s \models \psi \vee \phi$, if $M, s \models \phi$ or $M, s \models \psi$.
- $M, s \models \mathbf{X}\phi$, if $M, s^1 \models \phi$, where s^1 is the successor of s.
- $M, s \models \phi\mathbf{U}\psi$ if there $\exists i \geq 0$ such that $M, s^i \models \psi$ and $\forall k \in \{0 \ldots k\}$; $M, s^k \models \phi$, where s^i is the ith successor of s.

The other modalities like $\mathbf{F}$(future) $\mathbf{G}$(Globally), $\mathbf{R}$(Release) ... in LTL can be defined in terms of $\mathbf{X}$ and $\mathbf{U}$. Specifically $\mathbf{G}\psi \equiv \bot\mathbf{R}\psi \equiv \neg\mathbf{F}\neg\psi$; $\mathbf{F}\psi \equiv \top\mathbf{U}\psi$ and $\phi\mathbf{R}\psi \equiv \neg(\neg\phi\mathbf{U}\neg\psi)$. Figure. 1 is the list of modalities commonly used in LTL. Figure 2 are the equivalences commonly used.

When we want to prove that 2 formulas ϕ and ψ are equivalent in LTL we show that $\forall M,\ \forall s \in M\ M, s \models \phi$ iff $M, s \models \psi$.

Example Prove that $\neg\mathbf{G}\psi \equiv \mathbf{F}\neg\psi$

Textual	Symbolic†	Explanation	Diagram
Unary operators:			
X ϕ	$\bigcirc\phi$	ne**X**t: ϕ has to hold at the next state.	ϕ
G ϕ	$\Box\phi$	**G**lobally: ϕ has to hold on the entire subsequent path.	ϕ ϕ ϕ ϕ ϕ
F ϕ	$\Diamond\phi$	**F**inally: ϕ eventually has to hold (somewhere on the subsequent path).	ϕ
Binary operators:			
ψ **U** ϕ	$\psi\mathcal{U}\phi$	**U**ntil: ψ has to hold *at least* until ϕ, which holds at the current or a future position.	ψ ψ ψ ϕ
ψ **R** ϕ	$\psi\mathcal{R}\phi$	**R**elease: ϕ has to be true until and including the point where ψ first becomes true; if ψ never becomes true, ϕ must remain true forever.	ϕ ϕ ϕ ϕ,ψ ϕ ϕ ϕ ϕ ϕ

Figure 1: LTL operators

Proof. For any model M and some state $s \in M$.
$M, s \models \neg\mathbf{G}\psi \;\leftrightarrow\; M, s \not\models \mathbf{G}\psi \;\leftrightarrow\; \exists s^i \; s^i \geq s \; M, s^i \models \neg\psi \leftrightarrow \; M, s^i \models \mathbf{F}\neg\psi \;\leftrightarrow\; M, s \models \mathbf{F}\neg\psi$. □

Exercise Try proving the equivalences in figure 2.(One of them has been done for you)

REMARK LTL can be tought of as a pspace complete fragment of the classical first order logic. We just map each prepositon to a unary predicate in FOL. The following satisfyability preserving map holds.

- $p \rightsquigarrow p(t)$
- $\mathbf{X}p \rightsquigarrow p(t+1)$
- $\psi\mathbf{U}\phi \rightsquigarrow \exists t'(t' \geq t)\; \phi(t') \;\wedge\; \forall t"(t \leq t" < t')\; \psi(t")$

The following LTL formula expresses the property that the program always terminates ($start \implies \mathbf{F}\ terminate$). This is an example of a liveness propety. Something good will happen. There is another class of property that we are interested in, these capture the fact that nothing bad can ever happen. They are also called invariants. Not reaching a deadlocked state is one such property ($\mathbf{G}\ \neg deadlock$). Modelling systems and Model checking with LTL will be dealt with in the future.

Distributivity		
X (Φ ∨ ψ) ≡ (**X** Φ) ∨ (**X** ψ)	**X** (Φ ∧ ψ)≡ (**X** Φ) ∧ (**X** ψ)	**X** (Φ **U** ψ)≡ (**X** Φ) **U** (**X** ψ)
F (Φ ∨ ψ) ≡ (**F** Φ) ∨ (**F** ψ)	**G** (Φ ∧ ψ)≡ (**G** Φ) ∧ (**G** ψ)	
ρ **U** (Φ ∨ ψ) ≡ (ρ **U** Φ) ∨ (ρ **U** ψ)	(Φ ∧ ψ) **U** ρ ≡ (Φ **U** ρ) ∧ (ψ **U** ρ)	

Negation propagation		
¬**X** Φ ≡ **X** ¬Φ	¬**G** Φ ≡ **F** ¬Φ	¬**F** Φ ≡ **G** ¬Φ
¬ (Φ **U** ψ) ≡ (¬Φ **R** ¬ψ)	¬ (Φ **R** ψ) ≡ (¬Φ **U** ¬ψ)	

Special Temporal properties		
F Φ ≡ **F** **F** Φ	**G** Φ ≡ **G** **G** Φ	Φ **U** ψ ≡ Φ **U** (Φ **U** ψ)
Φ **U** ψ ≡ ψ ∨ (Φ ∧ **X**(Φ **U** ψ))	Φ **W** ψ ≡ ψ ∨ (Φ ∧ **X**(Φ **W** ψ))	Φ **R** ψ ≡ ψ ∧ (Φ ∨ **X**(Φ **R** ψ))
G Φ ≡ Φ ∧ **X**(**G** Φ)	**F** Φ ≡ Φ ∨ **X**(**F** Φ)	

Figure 2: LTL equivalences

2 Computational Tree Logic : CTL

LTL implicitly quantifies universally over paths. Properties that assert the existence of a path cannot be expressed. In particular, properties which mix existential and universal path quantifiers cannot be expressed. CTL was introduced to solve these problems. CTL explicitly introduces *path quantifiers*. Further CTL is the natural temporal logic defined over branching time structures.
The syntax of any well formed CTL formula adheres to the following grammar.

$$\phi ::= \bot|\top|p|(\neg\phi)|(\phi\wedge\psi)|\mathbf{A}[\phi\mathbf{U}\psi]|\mathbf{E}[\phi\mathbf{U}\psi]|\mathbf{A}[\mathbf{X}\phi]|\mathbf{E}[\mathbf{X}\phi].$$

$(\mathbf{X}, \mathbf{U})$ have the same meaning as in LTL. Where as $(\mathbf{A}, \mathbf{E})$ are quantified over path as follows.

- $\mathbf{A}\phi$ (All): ϕ has to hold on all paths starting from the current state.
- $\mathbf{E}\phi$ (Exists): there exists at least one path starting from the current state where ϕ holds.

Figure 3 illustrates the semantics of a CTL formula.

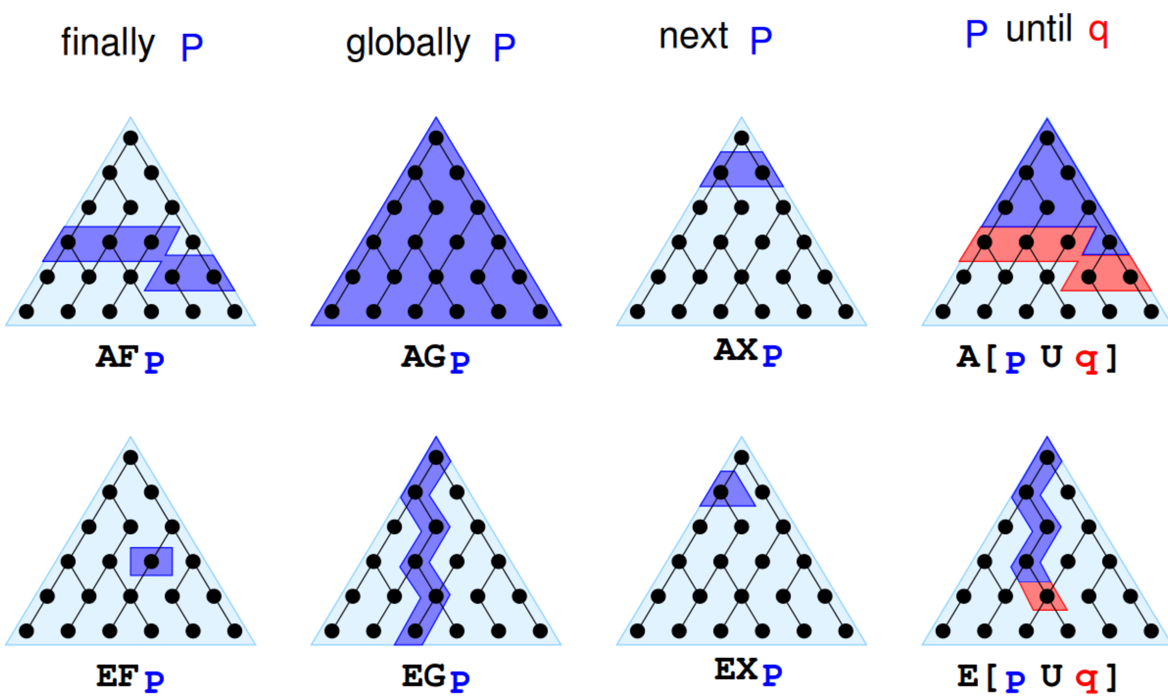

Figure 3: CTL Semantics

REMARK: $LTL \nsubseteq CTL$ and $CTL \nsubseteq LTL$

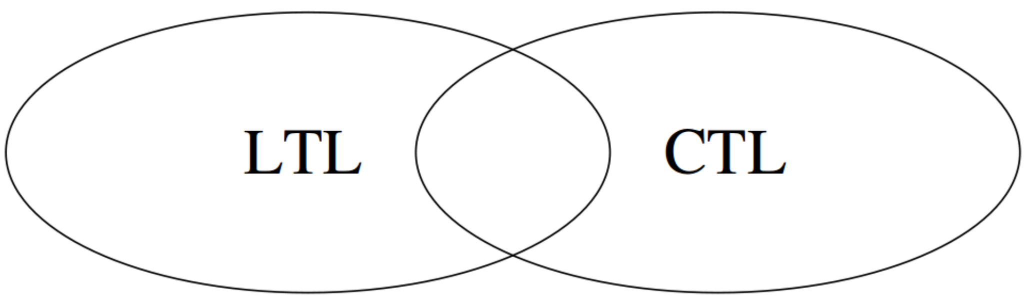

Figure 4: Relation between CTL and LTL

This means that there some formulae which can be expressed in CTL but cannot be expressed in LTL e.g. $\mathbf{AG}(p(\mathbf{EX}q\mathbf{EX}q))$. Similarly $\mathbf{F}(\mathbf{G}p)$ can be expressed in LTL but not in CTL.

Exercise Formally define the semantics for CTL. The intuitive meaning is illustrated in figure 3.

Exercise Give examples

1. $\psi \in LTL$, but $\psi \notin CTL$.
2. $\psi \in CTL$, but $\psi \notin LTL$.
3. $\psi \in LTL$ and $\psi \in CTL$.

Exercise Show that $\mathbf{A}$, $\mathbf{E}$ are duals. i.e that $\neg\mathbf{A}\phi \equiv \mathbf{E}\neg\phi$.

Exercise Show that $\{\top, \vee, \neg,\ \mathbf{EG},\ \mathbf{EU},\ \mathbf{EX}\}$ is one minimal set of operators for CTL. What it means is that other operators can be expressed in terms of these operators.

Just like LTL we have the following equivalences in CTL. These are used for expanding the formulae.

ExerciseProve the following equivalences

1. $AG\phi \equiv \phi \wedge AXAG\phi$
2. $EG\phi \equiv \phi \wedge EXEG\phi$
3. $AF\phi \equiv \phi \vee AXAF\phi$
4. $EF\phi \equiv \phi \vee EXEF\phi$
5. $A[\phi U\psi] \equiv \psi \vee (\phi \wedge AXA[\phi U\psi])$
6. $E[\phi U\psi] \equiv \psi \vee (\phi \wedge EXE[\phi U\psi])$