Specification et Verification Formelle

Chapter 04: CTL Model Checking

Dr. Hichem Debbi

hichem.debbi@gmail.com

April 25, 2022

CTL semantics

We use the Computation Tree Logic (CTL) to specify properties of systems described using Kripke Structures. The CTL formulas are evaluated over infinite computations produced by Kripke structure K. A computation of a Kripke structure is an infinite sequence of states $s_0 s_1, ...$ such that $s_i, s_{i+1} \in R$ for all $i \in \mathbb{N}$. We denote by $Paths(s)$ the set of all paths starting at s. The syntax of CTL state formula over the set AP is given as follows:

$$\phi ::= true|a|\neg\phi|\phi_1 \wedge \phi_2|\exists\varphi|\forall\varphi$$

where $a \in AP$ is an atomic proposition and φ is a path formula. The path formulas are formed according to the following grammar:

$$\varphi ::= \bigcirc\phi|\phi_1 U \phi_2$$

CTL semantics

We denote by $K, s \models \phi$ the satisfaction of CTL formula at a state s of K. The semantics defined by the satisfaction relation for a state formula is given as follows

$$
\begin{aligned}
& K, s \models true \Leftrightarrow true \\
& K, s \models a \Leftrightarrow a \in L(s) \\
& K, s \models \neg\phi \Leftrightarrow s \not\models \phi \\
& K, s \models \phi_1 \wedge \phi_2 \Leftrightarrow s \models \phi_1 \wedge s \models \phi_2 \\
& K, s \models \exists\varphi \Leftrightarrow \text{for some } \pi \in Paths(s), \pi \models \varphi \\
& K, s \models \forall\varphi \Leftrightarrow \text{for all } \pi \in Paths(s), \pi \models \varphi
\end{aligned}
$$

Given a path $\pi = s_0 s_1 \ldots$ and an integer $i \geq 0$, where $\pi[i] = s_i$, the semantics of path formulas is given as follows:

$$
\begin{aligned}
& K, \pi \models \bigcirc\phi \Leftrightarrow \pi\,[1] \models \phi \\
& K, \pi \models \phi_1 \mathbf{U} \phi_2 \Leftrightarrow \exists j \geq 0 . \pi\,[j] \models \phi_2 \wedge (\forall 0 \leq k < j . \pi\,[k] \models \phi_1)
\end{aligned}
$$

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

CTL satisfaction

The temporal operators in branching temporal logic allow the expression of properties of some or all computations that start in a state. To that end, it supports an existential path quantifier (denoted $\exists$) and a universal path quantifier (denoted $\forall$). For instance, the property $\exists\lozenge\varphi$ denotes that there exists a computation along which $\lozenge\varphi$ holds, whereas $\forall\lozenge\varphi$ denotes that for all computations $\lozenge\varphi$ holds.

Frequent CTL Formulae

- $\forall\Box a$**:** along All paths *a* holds Globally
- $\exists\Box a$**:** there Exists a path where *a* holds Globally
- $\forall\Diamond a$**:** along All paths *a* holds at some state in the Future
- $\exists\Diamond a$**:** there Exists a path where *a* holds at some state in the Future

Frequent CTL Formulae

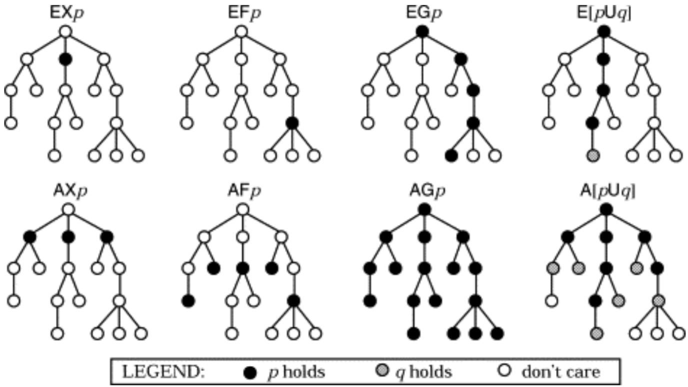
- $\forall \bigcirc a$**:** along All paths, p holds in the neXt state
- $\exists \bigcirc a$**:** there Exists a path where p holds in the neXt state
- $\forall[aUb]$**:** along All paths, p holds Until q holds
- $\exists[aUb]$**:** there Exists a path where p holds Until q holds

Basic CTL Equivalences

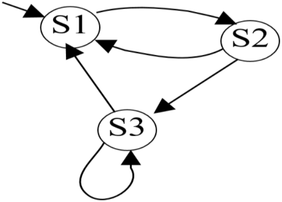
$$\begin{aligned}
AXp &\equiv \neg EX\neg p \\
AFp &\equiv \neg EG\neg p \\
AGp &\equiv \neg EF\neg p \\
A(pRq) &\equiv \neg E(\neg pU\neg q) \\
A(pUq) &\equiv \neg E(\neg pR\neg q)
\end{aligned}$$

$$\begin{aligned}
EFp &\equiv E(\text{true } U \ p) \\
E(pRq) &\equiv E(qU(p\wedge q))\vee EGq
\end{aligned}$$

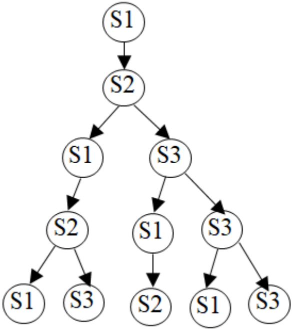
جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila



Université Mohamed Boudiaf - M'sila

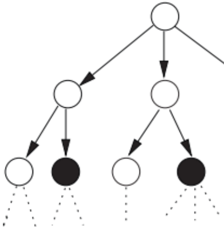


Kripke Structure

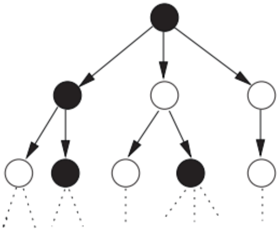


Tree of Computations

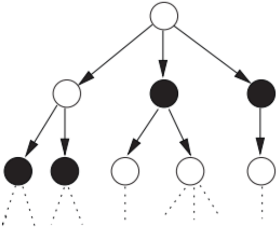
Basic CTL Formulae



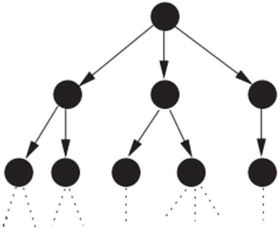
$\exists\Diamond\, black$



$\exists\Box\, black$

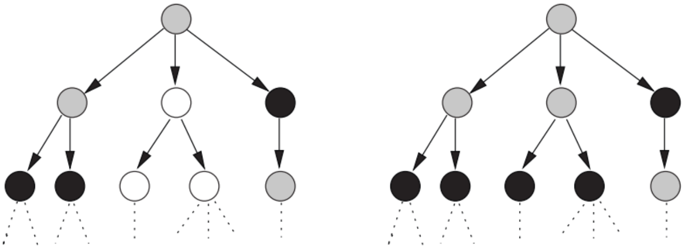


$\forall\Diamond\, black$



$\forall\Box\, black$

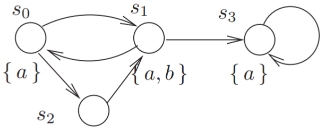
Basic CTL Formulae



$\exists(gray \, \mathsf{U} \, black)$ $\quad$ $\forall(gray \, \mathsf{U} \, black)$

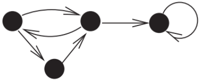
Basic CTL Formulae

TS

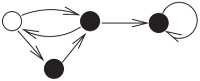


(a)

$\exists \bigcirc a$

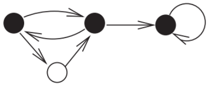


$\forall \bigcirc a$

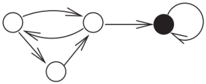


Basic CTL Formulae

$\exists\Box\, a$



$\forall\Box\, a$



Basic CTL Formulae

- The formula $\exists \bigcirc a$ is valid for all states since all states have some direct successor state that satisfies a.
- $\forall \bigcirc a$ a is not valid for state s0, since a possible path starting at s0 goes directly to state s2 for which a does not hold. Since the other states have only direct successors for which a holds, $\forall \bigcirc a$ is valid for all other states.
- For all states except state s2, it is possible to have a computation that leads to state s3 (such as $s0s1s3^{\omega}$ when starting in s0) for which a is globally valid. Therefore, $\exists$ a is valid in these states. Since $a \notin L(s2)$ there is no path starting at s2 for which a is globally valid.
- $\forall \Box a$ is only valid for s3 since its only path, $s3^{\omega}$, always visits a state in which a holds. For all other states it is possible to have a path which contains s2 that does not satisfy a. So for these states $\forall \Box a$ is not valid.

Equivalence rules for CTL– duality laws

$$\forall\bigcirc\Phi \equiv \neg\exists\bigcirc\neg\Phi \qquad \exists\bigcirc\Phi \equiv \neg\forall\bigcirc\neg\Phi$$

$$\forall\Diamond\Phi \equiv \neg\exists\Box\neg\Phi \qquad \exists\Diamond\Phi \equiv \neg\forall\Box\neg\Phi$$

$$\begin{aligned}
\forall(\Phi\,\mathsf{U}\,\Psi) &\equiv \neg\exists(\neg\Psi\,\mathsf{U}\,(\neg\Phi\wedge\neg\Psi)) \;\wedge\; \neg\exists\Box\neg\Psi \\
&\equiv \neg\exists((\Phi\wedge\neg\Psi)\,\mathsf{U}\,(\neg\Phi\wedge\neg\Psi)) \;\wedge\; \neg\exists\Box(\Phi\wedge\neg\Psi) \\
&\equiv \neg\exists((\Phi\wedge\neg\Psi)\,\mathsf{W}\,(\neg\Phi\wedge\neg\Psi))
\end{aligned}$$

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

Equivalence rules for CTL–Expansion laws

$$
\begin{aligned}
\forall(\Phi \, \mathsf{U} \, \Psi) &\equiv \Psi \lor (\Phi \land \forall \bigcirc \forall(\Phi \, \mathsf{U} \, \Psi)) \\
\forall \Diamond \Phi &\equiv \Phi \lor \forall \bigcirc \forall \Diamond \Phi \\
\forall \Box \Phi &\equiv \Phi \land \forall \bigcirc \forall \Box \Phi
\end{aligned}
$$

$$
\begin{aligned}
\exists(\Phi \, \mathsf{U} \, \Psi) &\equiv \Psi \lor (\Phi \land \exists \bigcirc \exists(\Phi \, \mathsf{U} \, \Psi)) \\
\exists \Diamond \Phi &\equiv \Phi \lor \exists \bigcirc \exists \Diamond \Phi \\
\exists \Box \Phi &\equiv \Phi \land \exists \bigcirc \exists \Box \Phi
\end{aligned}
$$

Equivalence rules for CTL– Distributuve laws

$$\forall\Box(\Phi \wedge \Psi) \equiv \forall\Box\Phi \wedge \forall\Box\Psi$$

$$\exists\Diamond(\Phi \vee \Psi) \equiv \exists\Diamond\Phi \vee \exists\Diamond\Psi$$