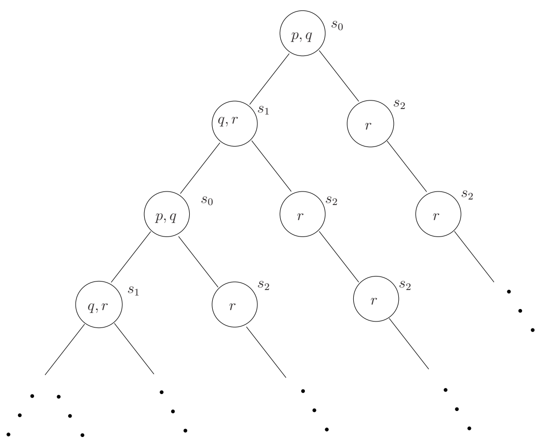
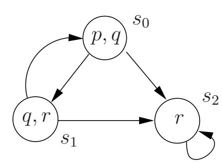
Aula 4

Contents

1 Branching-time Logic CTL

Branching-time Logic





The evolution of a transition system is a infinite computation tree. LTL implicitly quantifies universally over paths of that tree CTL (*Computation Tree Logic*) allows the existencial quantification over paths of that tree

Computation Tree Logic, CTL

AP, set of propositional variiables, $p, q, r, s, \ldots$

Syntax

$$\begin{aligned}\varphi \quad ::= \quad & \mathsf{true} \mid \mathsf{false} \mid p \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \rightarrow \varphi) \mid (\mathrm{AX}\varphi) \mid \\ & (\mathrm{EX}\varphi) \mid (\mathrm{AF}\varphi) \mid (\mathrm{EF}\varphi) \mid (\mathrm{AG}\varphi) \mid (\mathrm{EG}\varphi) \mid \mathrm{A}[\varphi \mathrm{U} \varphi] \mid \mathrm{E}[\varphi \mathrm{U} \varphi]\end{aligned}$$

Temporal Connectives

A means *along all paths* (from a state)

E means *along at least one path* (from a state)

F,G,X and U as in LTL

Formulae are interpreted in a state (state formulae)

Computation Tree Logic, CTL

Connectives A and E can only appear together with LTL temporal connectives.

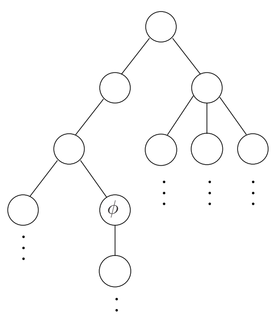
Priority bindings

- Unary connective($\neg$, AX,EX, AF,EF,AG and EG) has high priority
- Next $\wedge$ and $\vee$.
- Next $\rightarrow$, AU and EU (which are written in prefix and infix notation)

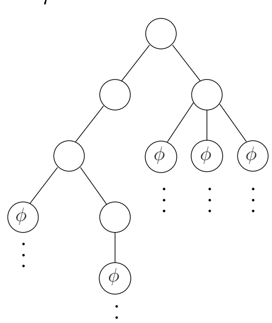
Examples

$$\mathrm{AG}(p \rightarrow \mathrm{EG}r)$$
$$\mathrm{EFE}[r\mathrm{U}q]$$
$$\mathrm{E}[\mathrm{A}[r\mathrm{U}p]\mathrm{U}q]$$
$$\mathrm{A}[\mathrm{AX}\neg p\mathrm{UE}[\mathrm{EX}(p \wedge q)\mathrm{U}\neg p]]$$

Semantics of CTL

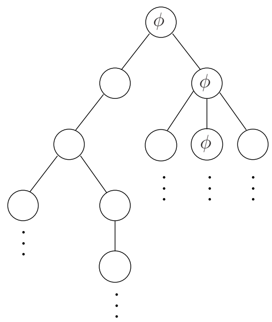


EFφ

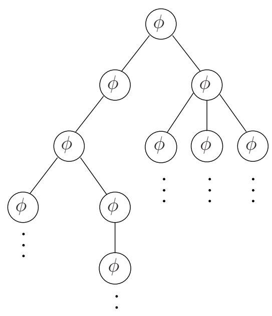


AFφ

Semântica do CTL



EGφ



AGφ

Always and Potentially

- $\mathrm{EF}\varphi = \mathrm{E}\mathsf{true}\mathrm{U}\varphi$, φ *potentially holds*
- $\mathrm{AF}\varphi = \mathrm{A}\mathsf{true}\mathrm{U}\varphi$, φ *is inevitable*
- $\mathrm{EG}\varphi = \neg\mathrm{AF}\neg\varphi$, φ *holds potentially always*
- $\mathrm{AG}\varphi = \neg\mathrm{EF}\neg\varphi$, φ *invariantly holds*
- $\mathrm{AGAF}\varphi$, φ *holds infinitely often in all paths*

Examples

- *Safety*: Mutual exclusion

$$\mathrm{AG}(\neg c_1 \vee \neg c_2)$$

- *Liveness* : P_1 and P_2 access the critical section infinitely often

$$\mathrm{AGAF}c_1 \wedge \mathrm{AGAF}c_2$$

- *Starvation freedom*:

$$(\mathrm{AGAF}w_1 \rightarrow \mathrm{AGAF}c_1) \wedge (\mathrm{AGAF}w_2 \rightarrow \mathrm{AGAF}c_2)$$

Semantics of CTL

Satisfiability

Given a transition system (model) $\mathcal{M} = (S, \longrightarrow, L)$ (without terminal states), a state $s \in S$, for $\pi \in Paths(s)$ let $\pi = s_1 s_2 s_3 \cdots$, $s_1 = s$ and $\pi[i] = s_i$ be i state in π.

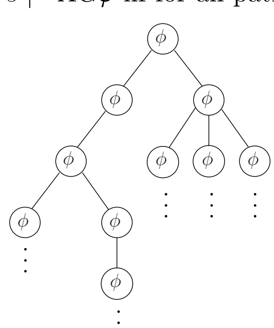
Given a formula φ and a state s, the satisfaction relation $s \models \varphi$ is defined inductively in the structure of φ:

1. $s \models \mathsf{true}$ and $s \not\models \mathsf{false}$
2. $s \models p$ iff $p \in L(s)$
3. $s \models \neg\varphi$ iff $s \not\models \varphi$
4. $s \models \varphi \wedge \psi$ iff $s \models \varphi$ and $s \models \psi$
5. $s \models \varphi \vee \psi$ iff $s \models \varphi$ or $s \models \psi$
6. $s \models \varphi \rightarrow \psi$ iff if $s \models \varphi$ then $s \models \psi$
7. $s \models \mathrm{AX}\varphi$ iff for all $\pi \in Paths(s)$, $\pi[2] \models \varphi$
8. $s \models \mathrm{EX}\varphi$ iff exists $\pi \in Paths(s)$, $\pi[2] \models \varphi$

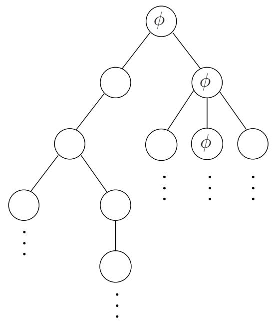
Semantics of CTL

Satisfiability

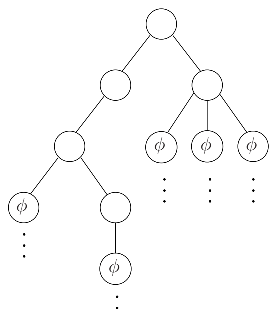
9. $s \models \mathrm{AG}\varphi$ iff for all paths $\pi \in Paths(s)$, we have for all $i \geq 1$ $\pi[i] \models \varphi$



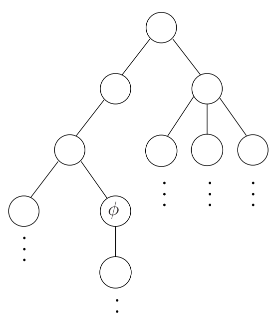
10. $s \models \mathrm{EG}\varphi$ iff exists a path $\pi \in \mathit{Paths}(s)$ such that for all $i \geq 1$, $\pi[i] \models \varphi$



11. $s \models \mathrm{AF}\varphi$ iff for all paths $\pi \in \mathit{Paths}(s)$, exists $i \geq 1$ such that $\pi[i] \models \varphi$



12. $s \models \mathrm{EF}\varphi$ iff exists one path $\pi \in \mathit{Paths}(s)$ such that exists $i \geq 1$ such that $\pi[i] \models \varphi$



13. $\mathcal{M}, s \models \mathrm{A}[\varphi_1 \mathrm{U} \varphi_2]$ iff for all paths $\pi \in \mathit{Paths}(s)$, we have that $\varphi_1 \mathrm{U} \varphi_2$ holds, i.e. exists $i \geq 1$ $\pi[i] \models \varphi_2$, and for $1 \leq j < i$ $\pi[j] \models \varphi_1$

14. $s \models \mathrm{E}[\varphi_1 \mathrm{U} \varphi_2]$ iff exists one path $\pi \in \mathit{Paths}(s)$, such that $\varphi_1 \mathrm{U} \varphi_2$ holds, i.e. exists $i \geq 1$ $\pi[i] \models \varphi_2$, and for $1 \leq j < i$ $\pi[j] \models \varphi_1$.

Specification Patterns

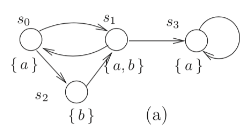
- There exists a reachable state where p holds. EFp
- From all reachable states where p holds it is possible to hold p true until there is a state where q holds. $AG(p \rightarrow EpUq)$
- Whenever there is a state where p holds, it is possible to have q true forevermore.$AG(p \rightarrow EGq)$
- There is a reachable state from which p holds in all reachable states. $EFAGp$

CTL Semantics for transition systems

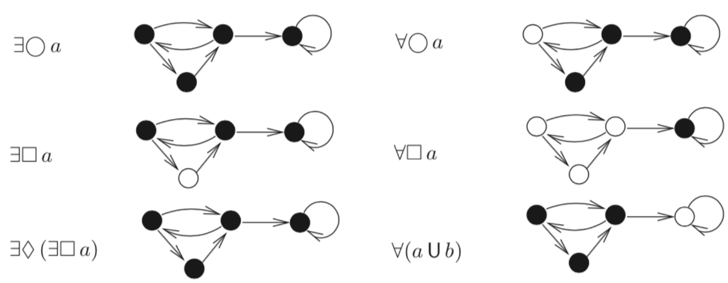
- Given $T = (S, Act, \longrightarrow, AP, I, L)$ and a CTL formula φ,
- $Sat(\varphi) = \{\ s \in S \mid s \models \varphi\ \}$
- T satisfies φ i.e $T \models \varphi$ iff $\forall s_0 \in I, s_0 \models \varphi$ (i.e $I \subseteq Sat(\varphi)$)

Exemple

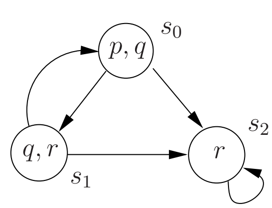
Give $Sat(\varphi)$ for the following formulae EXa, AXa, EGa, AGa, EFEGa e A[aUb],



(a)



Example



1. $s_0 \models p \land q$
2. $s_0 \models \mathrm{EX}r$
3. $s_0 \models \neg\mathrm{AX}(q \land r)$
4. $s_0 \models \neg\mathrm{EF}(p \land r)$
5. $s_0 \models \mathrm{EG}r$
6. $s_0 \models \mathrm{A}[p\mathrm{U}r]$

Property Specifications

- It is possible to get a state where `started` holds, but `ready` is false. $EF(started \land \neg ready)$
- For any state, if `trying`, then there exists a path where `critical` holds in the future (non-blocking).$AG(trying \to EF\, critical)$
- A process is `enabled` infinitely often on every computation path. $AG(AF\, enabled)$
- If a process is `enabled` infinitely often, then it `runs` infinitely often *Not possible*. It is not $AGAF\, enabled \to AGAF\, running$
- From any state it is possible to get to a `restart` state.$AGEF\, restart$

Property Specification

- For any state, if `request` occurs, then it will eventually be acknowledged, `ack`. $AG(\texttt{request} \to AF\, \texttt{ack})$
- A process will eventually be permanently `deadlock`ed. $AF(AG\, \texttt{deadlock})$

Equivalence of CTL Formulae

Two CTL formulae (over AP) are semantically equivalent, $\varphi \equiv \psi$, if any state in any model which satisfies one of them also satisfies the other.

It holds that:

$$\begin{aligned} \neg\mathrm{AF}\varphi &\equiv \mathrm{EG}\neg\varphi \\ \neg\mathrm{EF}\varphi &\equiv \mathrm{AG}\neg\varphi \\ \neg\mathrm{AX}\varphi &\equiv \mathrm{EX}\neg\varphi \\ \mathrm{AF}\varphi &\equiv \mathrm{A}[\mathsf{true}\mathrm{U}\varphi] \\ \mathrm{EF}\varphi &\equiv \mathrm{E}[\mathsf{true}\mathrm{U}\varphi] \\ \mathrm{A}[\varphi\mathrm{U}\psi] &\equiv \neg(\mathrm{E}[\neg\psi\mathrm{U}(\neg\varphi \land \neg\psi)]) \land \neg\mathrm{EG}\neg\psi \quad (*) \end{aligned}$$

Complete Sets of Connectives

Teorema 4.1. *The following sets of temporal connectives are complete* $\{AU, EU, EX\}$ *and* $\{EG, EU, EX\}$.

More equivalences

$$
\begin{array}{rcl}
\mathrm{AG}\varphi & \equiv & \varphi \,\wedge\, \mathrm{AXAG}\varphi \\
\mathrm{EG}\varphi & \equiv & \varphi \,\wedge\, \mathrm{EXEG}\varphi \\
\mathrm{AF}\varphi & \equiv & \varphi \,\vee\, \mathrm{AXAF}\varphi \\
\mathrm{EF}\varphi & \equiv & \varphi \,\vee\, \mathrm{EXEF}\varphi \\
\mathrm{A}[\varphi \mathrm{U} \psi] & \equiv & \psi \vee (\varphi \wedge \mathrm{AXA}[\varphi \mathrm{U} \psi] \\
\mathrm{E}[\varphi \mathrm{U} \psi] & \equiv & \psi \vee (\varphi \wedge \mathrm{EXE}[\varphi \mathrm{U} \psi]
\end{array}
$$

LTL and CTL

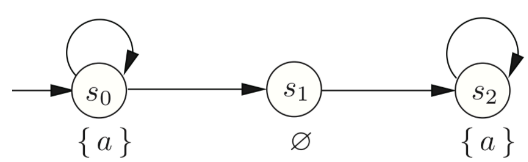
CTL is not strictly more expressive than LTL. For instance

$$\mathrm{F}p \to \mathrm{F}q$$

cannot be expressed in CTL. It means

All paths where p holds, q also holds.

Note that AF $p \to$ AF q or AG$(p \to \mathrm{AF}q)$ have different meanings.
FGφ is not AFAGφ



$$s_0 \models \mathrm{FG}a$$

but

$$s_0 \not\models \mathrm{AFAG}a$$

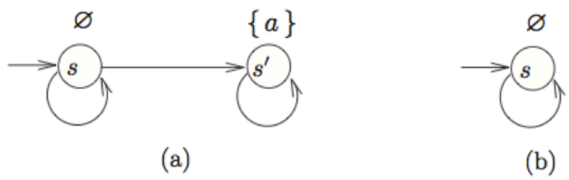
(show that for $\pi = s_0 s_0 s_0 \cdots$ exists a state (s_0) and $s_0 \not\models \mathrm{AG}a$.)

But

$$\mathrm{AGEF}\mathtt{a}$$

cannot be expressed in LTL:

From every state it is possible to reach a state where $\mathtt{a}$ holds.



AGEF$\mathtt{a}$ has no equivalent in LTL

There is no LTL formula φ that is equivalent to AGEF$\mathtt{a}$. Suppose that there exists such a formula. As $\mathcal{M}_{(a)}, s \models$ AGEF$\mathtt{a}$ then $\mathcal{M}_{(a)}, s \models \varphi$ and for all $\pi \in Paths(s)$, $\pi \models \varphi$. In particular for $\pi = sss\cdots$ then $\pi \models \varphi$. Then, we also have $\mathcal{M}_{(b)}, s \models \varphi$ .But $\mathcal{M}_{(b)}, s \not\models$ AGEFa, because $s \not\models$ EFa. This is a contradiction.

Also, we have FX$\mathtt{a} \equiv$ XF$\mathtt{a} \equiv$ AXAF$\mathtt{a}$ but

$$\mathrm{FX}\mathtt{a} \not\equiv \mathrm{AFAX}\mathtt{a}.$$

Teorema 4.2. *Let ψ a CTL formula and φ the LTL formula that is obtained by eliminating all path quantifiers A and E in ψ. Then either*

$$\psi \equiv \varphi$$

or there does not exists any LTL formula that is equivalent to ψ.

LTL versus CTL

Teorema 4.3. *a) There exist LTL formulas for which there is no equivalent CTL formula. For instance, FGa.*

b) There exist CTL formulas for which there is no equivalent LTL formula. For instance, AGEFa.

LTL versus CTL

Aspect	*Linear time*	*Branching time*
"behavior" in a state s	path-based: $trace(s)$	state-based: computation tree of s
temporal logic	LTL: path formulae φ $s \models \varphi$ iff $\forall \pi \in Paths(s). \pi \models \varphi$	CTL: state formulae existential path quantification $\exists\varphi$ universal path quantification: $\forall\varphi$
complexity of the model checking problems	PSPACE–complete $\mathcal{O}(\lvert TS\rvert \cdot \exp(\lvert\varphi\rvert))$	*PTIME* $\mathcal{O}(\lvert TS\rvert \cdot \lvert\Phi\rvert)$
implementation-relation	trace inclusion and the like (proof is PSPACE-complete)	simulation and bisimulation (proof in polynomial time)
fairness	no special techniques needed	special techniques needed

2 Logic CTL*

CTL*

CTL*

Extension of CTL, where it is not mandatory that an LTL operator {X, G,F,U} has an associated operador A or E.

- $\mathrm{A}[(p\mathrm{U}r) \ \vee \ (q\mathrm{U}r)]$,
- $\mathrm{E}(\mathrm{GF}\varphi)$
- $\mathrm{A}[\mathrm{X}p \ \vee \ \mathrm{XX}p]$

CTL* is strictly more expressive than both LTL and CTL, and much less efficient.

Syntax of CTL*

State Formulas

Evaluated in a state

$$\varphi \quad ::= \quad \mathsf{true} \mid p \mid (\neg\varphi) \mid (\varphi \ \wedge \ \varphi) \mid (\mathrm{A}[\alpha]) \mid (\mathrm{E}[\alpha])$$

Path Formulas

Evaluated in a path

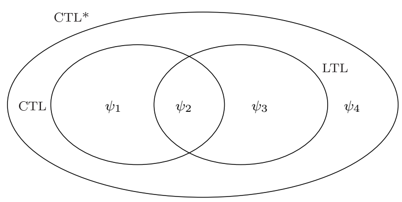
$$\alpha \quad ::= \quad \varphi \mid (\neg\alpha) \mid (\alpha \ \wedge \ \alpha) \mid (\alpha \mathrm{U} \alpha) \mid (\mathrm{G}\alpha) \mid (\mathrm{F}\alpha) \mid (\mathrm{X}\alpha)$$

Here we consider only a complete set of Boolean connectives ($\{\neg, \wedge\}$).

LTL, CTL and CTL*

A LTL formula α corresponds to A[α] in CTL*. CTL is a fragment of CTL* where

$$\alpha \quad ::= \quad (\alpha \mathrm{U} \alpha) \mid (\mathrm{G}\alpha) \mid (\mathrm{F}\alpha) \mid (\mathrm{X}\alpha)$$



$$\begin{array}{lcr} \psi_1 & = & \mathrm{AGEF}p \\ \psi_2 & = & \mathrm{AG}(p \rightarrow AFq) \\ \psi_3 & = & \mathrm{A}[\mathrm{GF}p \rightarrow Fq] \\ \psi_4 & = & \mathrm{E}[\mathrm{GF}p] \end{array}$$

$\mathbf{A}[\varphi\mathbf{U}\psi] \equiv \neg\mathbf{E}[\neg\psi\mathbf{U}(\neg\varphi \wedge \neg\psi)] \wedge \neg\mathbf{EG}\neg\psi$

Using CTL^*,

$$\begin{array}{rcl} \mathrm{A}[\varphi \mathrm{U} \psi] & \equiv & \mathrm{A}[\neg(\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)) \wedge \mathrm{F}\psi] \\ & \equiv & \neg\mathrm{E}\neg[\neg(\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)) \wedge \mathrm{F}\psi] \\ & \equiv & \neg\mathrm{E}[\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi) \vee \mathrm{G}\neg\psi] \\ & \equiv & \neg(\mathrm{E}[\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)] \vee \mathrm{EG}\neg\psi) \\ & \equiv & \neg\mathrm{E}[(\neg\psi \mathrm{U}(\neg\varphi \wedge \neg\psi)]) \wedge \neg\mathrm{EG}\neg\psi) \end{array}$$