

Model Checking Computation Tree Logic (CTL)

Didier Buchs

University of Geneva

from CTL Model Checking, Paul Jackson , University of Edinburgh .

Programme for the upcoming lectures

- Introducing CTL
- Basic Algorithms for CTL
- Basic Decision Diagrams

The denotation of a CTL formula

- Before, we defined a satisfaction relation $M, s \models \phi$.
- CTL model checking algorithms usually fix $M = \langle S, \rightarrow, AP, \nu \rangle$ and ϕ and compute $\llbracket \phi \rrbracket_M = \{s \in S \mid M, s \models \phi\}$
- $\llbracket \phi \rrbracket_M$ read as the denotation of ϕ in model M.
- The relationship between satisfaction and denotation is $M, s \models \phi$ iff $s \in \llbracket \phi \rrbracket_M$
- Often M is implicit and we write $\llbracket \phi \rrbracket$ rather than $\llbracket \phi \rrbracket_M$

CTL satisfaction for multiple initial states

- In NuSMV, CTLSPEC ϕ asks whether ϕ is satisfied in the given model which has a set of initial states
- The NuSMV definition of CTL satisfaction with a set of initial states S_0 is : $M, S_0 \models \phi$ iff $\forall s \in S_0, M, s \models \phi$
- We then have $M, S_0 \models \phi$ iff $S_0 \subseteq \llbracket \phi \rrbracket_M$

Denotational semantics for CTL

Instead of defining $\llbracket \phi \rrbracket$ in terms of $\models \phi$, we can define it directly recursively on the structure of ϕ , ψ and $p \in AP$

$$\begin{aligned}\llbracket t \rrbracket &= S \\ \llbracket f \rrbracket &= \emptyset \\ \llbracket p \rrbracket &= \nu(p) \\ \llbracket \neg \phi \rrbracket &= S - \llbracket \phi \rrbracket \\ \llbracket \phi \wedge \psi \rrbracket &= \llbracket \phi \rrbracket \cap \llbracket \psi \rrbracket \\ \llbracket \phi \vee \psi \rrbracket &= \llbracket \phi \rrbracket \cup \llbracket \psi \rrbracket\end{aligned}$$

Since $\llbracket \phi \rrbracket$ is always a finite set, these are computable.

Denotational semantics for CTL : temporal operators

$$\begin{aligned}\llbracket \mathbf{EX} \phi \rrbracket &= pre_{\exists}(\llbracket \phi \rrbracket) \\ \llbracket \mathbf{AX} \phi \rrbracket &= pre_{\forall}(\llbracket \phi \rrbracket)\end{aligned}$$

where

$$pre_{\exists}(Y) = \{s \in S \mid \exists s' \in S, s \rightarrow s' \wedge s' \in Y\}$$

$$pre_{\forall}(Y) = \{s \in S \mid \forall s' \in S, s \rightarrow s' \Rightarrow s' \in Y\}$$

These are computable if we have the whole transition system, but what about the rest E.g.

$\llbracket \mathbf{EF} \phi \rrbracket = \{s \in S \mid \exists path \pi \text{ s.t. } \pi(0) = s, \exists i \pi(i) \models \phi\}$ does not suggest how to compute $\llbracket \mathbf{EF} \phi \rrbracket$

Considering fixing path length as approximation of $\llbracket \mathbf{EF} \phi \rrbracket$

Define

$$\begin{aligned}\mathbf{EF}_0 \phi &= f \\ \mathbf{EF}_{i+1} \phi &= \phi \vee \mathbf{EX} \mathbf{EF}_i \phi\end{aligned}$$

Then have

$$\begin{aligned}\mathbf{EF}_1 \phi &= \phi \\ \mathbf{EF}_2 \phi &= \phi \vee \mathbf{EX} \phi \\ \mathbf{EF}_3 \phi &= \phi \vee \mathbf{EX}(\phi \vee \mathbf{EX} \phi)\end{aligned}$$

$s \in \llbracket \mathbf{EF}_i \phi \rrbracket$ if there exists a finite path of length $i - 1$ from s and ϕ holds at some point on that path.

For a given model M , let $n = |S|$, If there is a path of length $k > n$ on which ϕ holds somewhere, there also will be path of length n . (Proof : take the k -length path and repeatedly cut out segments between repeated states)

Therefore, $\forall k > n, \llbracket \mathbf{EF}_k \phi \rrbracket = \llbracket \mathbf{EF}_n \phi \rrbracket$

Computing $\llbracket \mathbf{EF} \phi \rrbracket$

By a similar argument

$$\llbracket \mathbf{EF} \phi \rrbracket = \llbracket \mathbf{EF}_n \phi \rrbracket$$

$$\begin{aligned} \llbracket \mathbf{EF}_0 \phi \rrbracket &= \emptyset \\ \llbracket \mathbf{EF}_{i+1} \phi \rrbracket &= \llbracket \phi \rrbracket \cup \text{pre}_{\exists}(\llbracket \mathbf{EF}_i \phi \rrbracket) \end{aligned}$$

We have here an effective way of computing $\llbracket \mathbf{EF} \phi \rrbracket$

Approximation of $\llbracket \mathbf{EG} \phi \rrbracket$

Define

$$\begin{aligned}\mathbf{EG}_0 \phi &= t \\ \mathbf{EG}_{i+1} \phi &= \phi \wedge \mathbf{EX} \mathbf{EG}_i \phi\end{aligned}$$

Then have

$$\begin{aligned}\mathbf{EG}_1 \phi &= \phi \\ \mathbf{EG}_2 \phi &= \phi \wedge \mathbf{EX} \phi \\ \mathbf{EG}_3 \phi &= \phi \wedge \mathbf{EX}(\phi \wedge \mathbf{EX} \phi)\end{aligned}$$

$s \in \llbracket \mathbf{EG}_i \phi \rrbracket$ if there exists a finite path of length $i - 1$ from s and ϕ holds at every point on that path.

As with $\llbracket \mathbf{EF} \phi \rrbracket$, we have $\forall k > n, \llbracket \mathbf{EG}_k \phi \rrbracket = \llbracket \mathbf{EG}_n \phi \rrbracket = \llbracket \mathbf{EG} \phi \rrbracket$ and so we can compute $\llbracket \mathbf{EG} \phi \rrbracket$. Similarly we can compute the denotation of the other temporal connectives .

Fixed-Point theory

- In general, what's happening here is that we are computing fixed-points.
- A set $X \subseteq S$ is a fixed point of a function $F \subseteq P(S) \rightarrow P(S)$ iff $X = F(X)$.
- We have that

$$\begin{aligned}\llbracket \mathbf{EF}_n \phi \rrbracket &= \llbracket \mathbf{EF}_{n+1} \phi \rrbracket \\ &= \llbracket \phi \vee \mathbf{EX} \mathbf{EF}_n \phi \rrbracket \\ &= \llbracket \phi \rrbracket \cup \text{pre}_{\exists}(\llbracket \mathbf{EF}_n \phi \rrbracket)\end{aligned}$$

so $\llbracket \mathbf{EF}_n \phi \rrbracket$ is a fixed point of $F = \lambda Y. \llbracket \phi \rrbracket \cup \text{pre}_{\exists}(Y)$

- Also $\llbracket \mathbf{EF} \phi \rrbracket$ is a fixed-point of F , since $\llbracket \mathbf{EF}_n \phi \rrbracket = \llbracket \mathbf{EF} \phi \rrbracket$.
- More specifically, $\llbracket \mathbf{EF}_n \phi \rrbracket$ and $\llbracket \mathbf{EF} \phi \rrbracket$ are the least fixed point of F .

Fix point theorem

A function $F \in P(S) \rightarrow P(S)$ is monotone iff $X \subseteq Y$ implies $F(X) \subseteq F(Y)$ for all subsets X and Y of S .

Let $F^i(X) = F(F^{i-1}(X))$ for $i > 0$ and $F^0(X) = X$.

Given a collection of sets $C \subseteq P(S)$, a set $X \in C$ is the least element of C iff $\forall Y \in C, X \subseteq Y$, and X is the greatest element of C iff $\forall Y \in C, Y \subseteq X$.

Theorem (Knaster-Tarski Theorem (special case))

Let S be a set with n elements and $F \in P(S) \rightarrow P(S)$ be a monotone function. Then

- $F^n(\emptyset)$ is the least fixed point of F , and
- $F^n(S)$ is the greatest fixed point of F

This theorem justifies $F^n(\emptyset)$ and $F^n(S)$ being fixed points of F without the need, as before, to appeal to further details about F .

Denotational semantics for CTL temporal operator

When $F \in P(S) \rightarrow P(S)$ a monotone function, let us write $\mu Y.F(Y)$ for the least fixed point of F , and $\nu Y.F(Y)$ for the greatest fixed point of F .

With this notation, we can make the definitions

$$\begin{aligned} \llbracket \mathbf{EF} \phi \rrbracket &= \mu Y. \llbracket \phi \rrbracket \cup \text{pre}_{\exists}(Y) \\ \llbracket \mathbf{EG} \phi \rrbracket &= \nu Y. \llbracket \phi \rrbracket \cap \text{pre}_{\exists}(Y) \\ \llbracket \mathbf{AF} \phi \rrbracket &= \mu Y. \llbracket \phi \rrbracket \cup \text{pre}_{\forall}(Y) \\ \llbracket \mathbf{AG} \phi \rrbracket &= \nu Y. \llbracket \phi \rrbracket \cap \text{pre}_{\forall}(Y) \\ \llbracket \mathbf{E}[\phi U \psi] \rrbracket &= \mu Y. \llbracket \psi \rrbracket \cup (\llbracket \phi \rrbracket \cap \text{pre}_{\exists}(Y)) \\ \llbracket \mathbf{A}[\phi U \psi] \rrbracket &= \mu Y. \llbracket \psi \rrbracket \cup (\llbracket \phi \rrbracket \cap \text{pre}_{\forall}(Y)) \end{aligned}$$

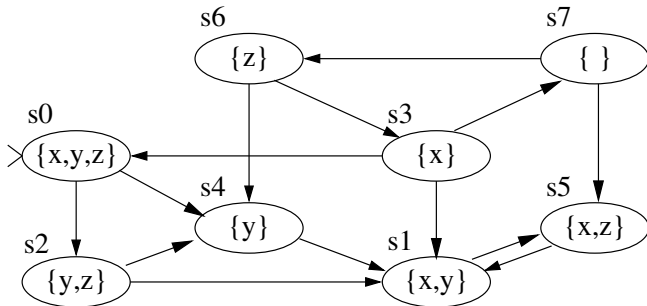
In every case the $F(Y)$ is monotone, so the KT theorem assures us the fixed point exists and can be computed.

Fixed-point identities

The fixed-point characterisations of the CTL temporal operators justify the CTL identities

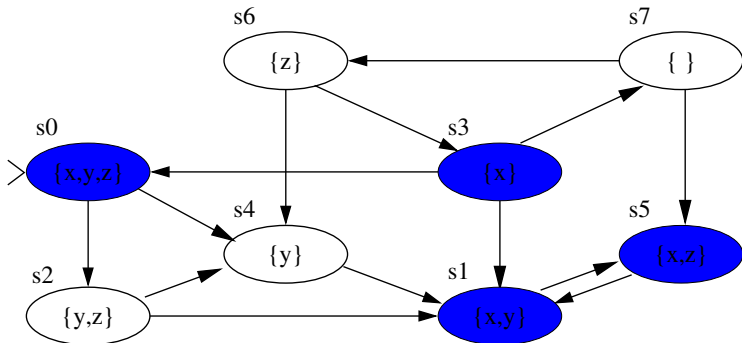
$$\begin{aligned}\mathbf{EF} \phi &= \phi \vee \mathbf{EX}(\mathbf{EF} \phi) \\ \mathbf{EG} \phi &= \phi \wedge \mathbf{EX}(\mathbf{EG} \phi) \\ \mathbf{AF} \phi &= \phi \vee \mathbf{AX}(\mathbf{AF} \phi) \\ \mathbf{AG} \phi &= \phi \wedge \mathbf{AX}(\mathbf{AG} \phi) \\ \mathbf{E}[\phi \mathbf{U} \psi] &= \psi \vee (\phi \wedge \mathbf{EX}(\mathbf{E}[\phi \mathbf{U} \psi])) \\ \mathbf{A}[\phi \mathbf{U} \psi] &= \psi \vee (\phi \wedge \mathbf{AX}(\mathbf{A}[\phi \mathbf{U} \psi]))\end{aligned}$$

Solving nested formulas : Is $s_0 \in \llbracket \mathbf{AF\ AG\ x} \rrbracket$?



- To compute the semantics of formulas with nested operators, we first compute it recursively as imbrication of fix-point computations.
- In this example, we compute
$$\llbracket \mathbf{AF\ AG\ x} \rrbracket = \mu Y. \llbracket \mathbf{AG\ x} \rrbracket \cup \text{pre}_\forall(Y)$$
$$\llbracket \mathbf{AG\ x} \rrbracket = \nu Y. \llbracket x \rrbracket \cap \text{pre}_\forall(Y)$$
$$\llbracket x \rrbracket = ? \text{ in that order.}$$

Fix-point method (1) : Compute $\llbracket x \rrbracket$



We have here the result of $\nu(x) = \{s_0, s_1, s_3, s_5\} = \llbracket x \rrbracket$

Fix-point method (2) : Compute $\llbracket \mathbf{AG} x \rrbracket$

$$\llbracket \mathbf{AG} x \rrbracket = \nu Y. \llbracket x \rrbracket \cap \text{pre}_V(Y)$$

$$(1) \{s_0, s_1, s_3, s_5\} \cap \text{pre}_V(\{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7\})$$

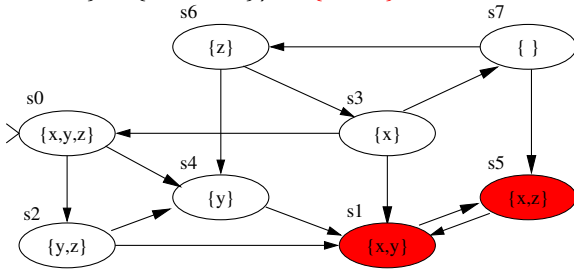
$$(1') \{s_0, s_1, s_3, s_5\} \cap \{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7\} = \{s_0, s_1, s_3, s_5\}$$

$$(2) \{s_0, s_1, s_3, s_5\} \cap \text{pre}_V(\{s_0, s_1, s_3, s_5\})$$

$$(2') \{s_0, s_1, s_3, s_5\} \cap \{s_4, s_5, s_1\} = \{s_1, s_5\}$$

$$(3) \{s_0, s_1, s_3, s_5\} \cap \text{pre}_V(\{s_1, s_5\})$$

$$(3') \{s_0, s_1, s_3, s_5\} \cap \{s_4, s_5, s_1\} = \{s_1, s_5\} \text{ fixpoint reached}$$



Fix-point method (3) : Compute $\llbracket \mathbf{AF\ AG\ }x \rrbracket$

$$\llbracket \mathbf{AF\ AG\ }x \rrbracket = \mu Y. \llbracket \mathbf{AG\ }x \rrbracket \cup \text{pre}_V(Y)$$

$$(1) \{s_1, s_5\} \cup \text{pre}_V(\emptyset) = \{s_1, s_5\}$$

$$(2) \{s_1, s_5\} \cup \text{pre}_V(\{s_1, s_5\})$$

$$(2') \{s_1, s_5\} \cup \{s_1, s_4, s_5\} = \{s_1, s_4, s_5\}$$

$$(3) \{s_1, s_5\} \cup \text{pre}_V(\{s_1, s_4, s_5\})$$

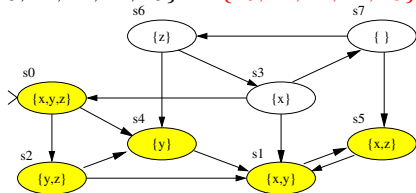
$$(3') \{s_1, s_5\} \cup \{s_1, s_2, s_4, s_5\} = \{s_1, s_2, s_4, s_5\}$$

$$(4) \{s_1, s_5\} \cup \text{pre}_V(\{s_1, s_2, s_4, s_5\})$$

$$(4') \{s_1, s_5\} \cup \{s_0, s_1, s_2, s_4, s_5\} = \{s_0, s_1, s_2, s_4, s_5\}$$

$$(5) \{s_1, s_5\} \cup \text{pre}_V(\{s_0, s_1, s_2, s_4, s_5\})$$

$$(5') \{s_1, s_5\} \cup \{s_0, s_1, s_2, s_4, s_5\} = \{s_0, s_1, s_2, s_4, s_5\} \text{ fixpoint}$$



Conclusion

- *Conclusion* : The model checking principles are stated as fix-point computations.
- Complexity issues are difficult to master. Next chapter will show some techniques for this.
- *Remark* : The *pre* function is fundamental for computing fix-points but it is not always necessary to memorize it with the transition system. It can be computed as the inverse of the firing functions (for instance in P/T).