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 $\boxed{M, s \models \phi.}$
- CTL model checking algorithms usually fix $M = \langle S, \rightarrow, AP, \nu\rangle$ and ϕ and compute $[\![\phi]\!]_M = \{s \in S | M, s \models \phi\}$
- $[\![\phi]\!]_M$ read as the denotation of ϕ in model M.
- The relationship between satisfaction and denotation is $M, s \models \phi$ iff $s \in [\![\phi]\!]_M$
- Often M is implicit and we write $[\![\phi]\!]$ rather than $[\![\phi]\!]_M$

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 $S_0 \subseteq [\![\phi]\!]_M$

Denotational semantics for CTL

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

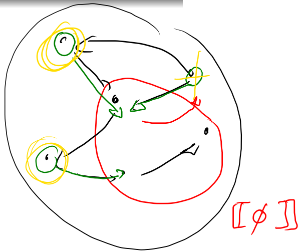
$$\begin{array}{rcl}
[\![t]\!] & = & S \\
[\![f]\!] & = & \varnothing \\
[\![p]\!] & = & \nu(p) \\
[\![\neg\phi]\!] & = & S - [\![\phi]\!] \\
[\![\phi \wedge \psi]\!] & = & [\![\phi]\!] \cap [\![\psi]\!] \\
[\![\phi \vee \psi]\!] & = & [\![\phi]\!] \cup [\![\psi]\!]
\end{array}$$

logique classiqu

Since $[\![\phi]\!]$ is always a finite set, these are computable.

Denotational semantics for CTL : temporal operators

$$\begin{array}{rcl} [\![\textbf{EX}\ \phi]\!] & = & pre_{\exists}([\![\phi]\!]) \\ [\![\textbf{AX}\ \phi]\!] & = & pre_{\forall}([\![\phi]\!]) \end{array}$$



where

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

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

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

i est un entier positif inconnu

$[\![\textbf{EF}\ \phi]\!] = \{s \in S | \exists path\ \pi \text{ s.t. } \cancel{\pi(0) =} s, \exists i\ \pi(i) \models \phi\}$ does not suggest how to compute $[\![\textbf{EF}\ \phi]\!]$

(ensemble infini de chemins)

Considering fixing path length as approximation of $[\![\mathbf{EF}\,\phi]\!]$

indice indique la longueur du chemi

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

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

$s \in [\![\mathbf{EF}_i\,\phi]\!]$ 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, $\forall k > n$, $[\![\mathbf{EF}_k\,\phi]\!] = [\![\mathbf{EF}_n\,\phi]\!]$

Computing $[\![\mathbf{EF}\,\phi]\!]$

By a similar argument

$$[\![\mathbf{EF}\,\phi]\!] = [\![\mathbf{EF}_n\,\phi]\!]$$

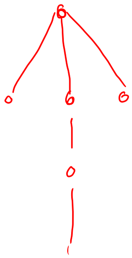
$$\begin{array}{rcl} [\![\mathbf{EF}_0\,\phi]\!] & = & \varnothing \\ [\![\mathbf{EF}_{i+1}\,\phi]\!] & = & [\![\phi]\!] \cup pre_{\exists}([\![\mathbf{EF}_i\,\phi]\!]) \end{array}$$

We have here an effective way of computing $[\![\mathbf{EF}\,\phi]\!]$

Approximation of $[\![\mathbf{EG}\,\phi]\!]$

Define

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



Then have

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

$s \in [\![\mathbf{EG}_i\,\phi]\!]$ if there exists a finite path of length $i-1$ from s and ϕ holds at every point on that path.
As with $[\![\mathbf{EF}\,\phi]\!]$, we have $\forall k > n$, $[\![\mathbf{EG}_k\,\phi]\!] = [\![\mathbf{EG}_n\,\phi]\!] = [\![\mathbf{EG}\,\phi]\!]$ and so we can compute $[\![\mathbf{EG}\,\phi]\!]$. Similarly we can compute the denotation of the other temporal connectives .

Fixed-Point theory

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

$$
\begin{aligned}
[\![\mathbf{EF}_n\,\phi]\!] &= [\![\mathbf{EF}_{n+1}\,\phi]\!] \\
&= \boxed{[\![\phi \lor \mathbf{EX}\,\mathbf{EF}_n\,\phi]\!]} \\
&= [\![\phi]\!] \cup pre_{\exists}([\![\mathbf{EF}_n\,\phi]\!])
\end{aligned}
$$

$F(y) = [\![\phi]\!] \cup pre_E(y)$

so $\boxed{[\![\mathbf{EF}_n\,\phi]\!]}$ is a fixed point of $F = \lambda Y.[\![\phi]\!] \cup pre_{\exists}(Y)$

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

Fix point theorem

A function $F \in P(S) \to P(S)$ 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 $F \in P(S) \to P(S)$ be a monotone function. Then

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

This theorem justifies $F^n(\varnothing)$ 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 $F \in P(S) \to P(S)$ 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

$$
\begin{array}{rcl}
[\![\mathbf{EF}\,\phi]\!] & = & \mu Y.[\![\phi]\!] \cup pre_{\exists}(Y) \\
[\![\mathbf{EG}\,\phi]\!] & = & \nu Y.[\![\phi]\!] \cap pre_{\exists}(Y) \\
[\![\mathbf{AF}\,\phi]\!] & = & \mu Y.[\![\phi]\!] \cup pre_{\forall}(Y) \\
[\![\mathbf{AG}\,\phi]\!] & = & \nu Y.[\![\phi]\!] \cap pre_{\forall}(Y) \\
[\![\mathbf{E}[\phi U \psi]]\!] & = & \mu Y.[\![\psi]\!] \cup ([\![\phi]\!] \cap pre_{\exists}(Y)) \\
[\![\mathbf{A}[\phi U \psi]]\!] & = & \mu Y.[\![\psi]\!] \cup ([\![\phi]\!] \cap pre_{\forall}(Y))
\end{array}
$$

?

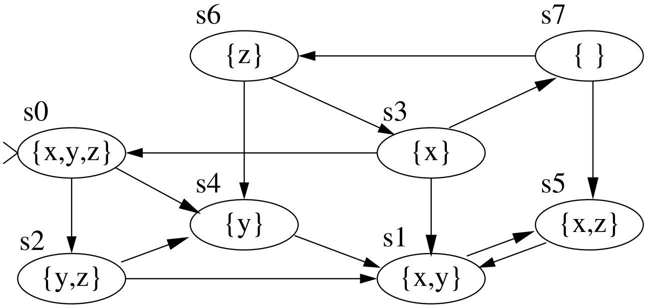
In every case the $F(Y)$ is monotone, so the KT theorem assures us the fixed point exists and can be computed.

Fixed-point identities

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

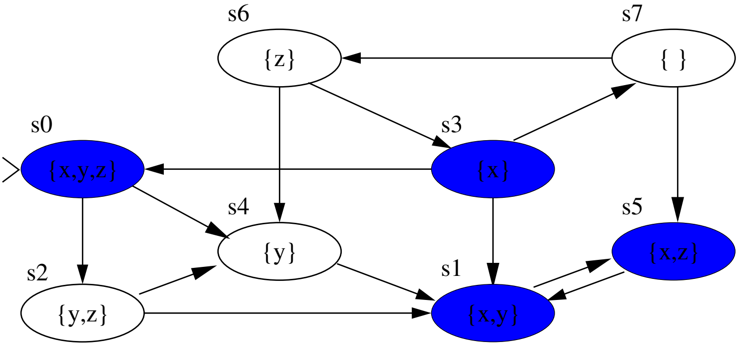
$$
\begin{array}{rcl}
\mathbf{EF}\,\phi & = & \phi \vee \mathbf{EX}(\mathbf{EF}\,\phi) \\
\mathbf{EG}\,\phi & = & \phi \wedge \mathbf{EX}(\mathbf{EG}\,\phi) \\
\mathbf{AF}\,\phi & = & \phi \vee \mathbf{AX}(\mathbf{AF}\,\phi) \\
\mathbf{AG}\,\phi & = & \phi \wedge \mathbf{AX}(\mathbf{AG}\,\phi) \\
\mathbf{E}[\phi\,\mathbf{U}\,\psi]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

Solving nested formulas : Is $s_0 \in [\![\mathbf{AF\,AG}\,x]\!]$?



- 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
  $[\![\mathbf{AF\,AG}\,x]\!] = \mu Y.[\![\mathbf{AG}\,x]\!] \cup pre_{\forall}(Y)$
  $[\![\mathbf{AG}\,x]\!] = \nu Y.[\![x]\!] \cap pre_{\forall}(Y)$
  $[\![x]\!] =?$ in that order.

Fix-point method (1) : Compute$[\![x]\!]$



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

Fix-point method (2) : Compute$[\![\mathbf{AG}\, x]\!]$

$[\![\mathbf{AG}\, x]\!] = \nu Y . [\![x]\!] \cap pre_{\forall}(Y)$

(1) $\{s_0, s_1, s_3, s_5\} \cap pre_{\forall}(\{\overbrace{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7}^{S}\})$

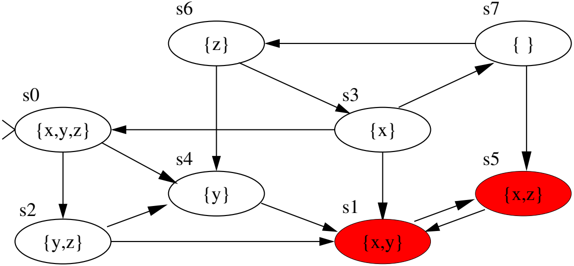
(1') $\{s_0, s_1, s_3, s_5\} \cap \{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7\} = \{s_0, s_1, s_3, s_5\}$

(2) $\{s_0, s_1, s_3, s_5\} \cap pre_{\forall}(\{s_0, s_1, s_3, s_5\})$

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

(3) $\{s_0, s_1, s_3, s_5\} \cap pre_{\forall}(\{s_1, s_5\})$

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



Fix-point method (3) : Compute$[\![$**AF AG** $x]\!]$

$[\![\textbf{AF AG } x]\!] = \mu Y.[\![\textbf{AG } x]\!] \cup pre_\forall(Y)$

(1) $\{s_1, s_5\} \cup pre_\forall(\emptyset) = \{s_1, s_5\}$

(2) $\{s_1, s_5\} \cup pre_\forall(\{s_1, s_5\})$

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

(3) $\{s_1, s_5\} \cup pre_\forall(\{s_1, s_4, s_5\})$

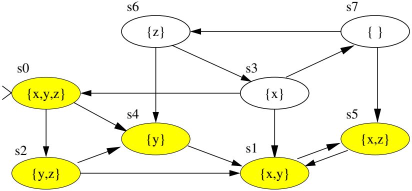
(3') $\{s_1, s_5\} \cup \{s_1, s_2, s_4, s_5\} = \{s_1, s_2, s_4, s_5\}$

(4) $\{s_1, s_5\} \cup pre_\forall(\{s_1, s_2, s_4, s_5\})$

(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) $\{s_1, s_5\} \cup pre_\forall(\{s_0, s_1, s_2, s_4, s_5\})$

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