CTL Model Checking

Paul Jackson
Paul.Jackson@ed.ac.uk

University of Edinburgh

Formal Verification
Autumn 2023

CTL satisfaction using formula denotations

- In CTL model checking we ask the question: *does*

$$\mathcal{M}, s \models \phi$$

  hold for all initial states S_0?

- CTL model checking algorithms usually fix $\mathcal{M} = \langle S, \rightarrow, L \rangle$ and ϕ and compute

$$[\![\phi]\!]_{\mathcal{M}} \;=\; \{s \in S \mid \mathcal{M}, s \models \phi\}$$

  "The denotation of ϕ in model $\mathcal{M}$"

- The CTL model checking question now becomes:

$$S_0 \subseteq [\![\phi]\!]_{\mathcal{M}} \quad ?$$

- Often $\mathcal{M}$ is implicit and we write $[\![\phi]\!]$ rather than $[\![\phi]\!]_{\mathcal{M}}$

Denotational semantics for CTL

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

$$
\begin{array}{lcl}
[\![\top]\!] & = & S \\
[\![\bot]\!] & = & \emptyset \\
[\![p]\!] & = & \{s \in S \mid p \in L(s)\} \\
[\![\neg\phi]\!] & = & S - [\![\phi]\!] \\
[\![\phi \wedge \psi]\!] & = & [\![\phi]\!] \cap [\![\psi]\!] \\
[\![\phi \vee \psi]\!] & = & [\![\phi]\!] \cup [\![\psi]\!]
\end{array}
$$

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

Denotational semantics for CTL: temporal connectives

$$\begin{array}{rcl} [\![\mathbf{EX}\,\phi]\!] & = & \mathsf{pre}_{\exists}([\![\phi]\!]) \\ [\![\mathbf{AX}\,\phi]\!] & = & \mathsf{pre}_{\forall}([\![\phi]\!]) \end{array}$$

where

$$\begin{array}{rcl} \mathsf{pre}_{\exists}(Y) & \doteq & \{s \in S \mid \exists s' \in S.\, s \to s' \wedge s' \in Y\} \\ \mathsf{pre}_{\forall}(Y) & \doteq & \{s \in S \mid \forall s' \in S.\, s \to s' \Rightarrow s' \in Y\} \end{array}$$

These are computable.

But what about the rest? E.g.

$$[\![\mathbf{EF}\,\phi]\!] \;=\; \{s \in S \mid \exists \text{ path } \pi \text{ s.t. } s_0 = s.\ \exists i.\ s_i \models \phi\}$$

does not suggest how to compute $[\![\mathbf{EF}\,\phi]\!]$

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

Define

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

Then

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

$s \in [\![\mathbf{EF}_i\,\phi]\!]$ if there exists a finite path i states long starting from s such that ϕ holds at some point on the path.

Fix a model $\mathcal{M}$ and let $n = |S|$. If there is a finite path with $k > n$ states on which ϕ holds somewhere, then there also is a finite path of n states or fewer where ϕ holds somewhere. (*Proof: if ϕ occurs at position $\geq n$, repeatedly cut out segments between repeated states*)

Therefore, for all $k > n$, $[\![\mathbf{EF}_k\,\phi]\!] = [\![\mathbf{EF}_n\,\phi]\!]$

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

By a similar argument

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

Consider $[\![\mathbf{EF}_n]\!]$ when the definition of $\mathbf{EF}_n$ is expanded:

$$\begin{aligned} [\![\mathbf{EF}_0\,\phi]\!] &= \emptyset \\ [\![\mathbf{EF}_{i+1}\,\phi]\!] &= [\![\phi]\!] \cup \mathrm{pre}_{\exists}([\![\mathbf{EF}_i\,\phi]\!]) \end{aligned}$$

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

In general, we can stop computing the recurrence as soon as we find

$$[\![\mathbf{EF}_{k+1}\phi]\!] = [\![\mathbf{EF}_k\,\phi]\!]$$

for $k \leq n$.

For efficient computation $k << n$ is desirable.

Approximating $[\![\mathbf{EG}\,\phi]\!]$

Define

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

Then

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

$s \in [\![\mathbf{EG}_i\,\phi]\!]$ if there exists a finite path i states long starting from s such that ϕ holds at every point on the path.

One can show $\forall k > n.\quad [\![\mathbf{EG}_k\,\phi]\!] = [\![\mathbf{EG}_n\,\phi]\!] = [\![\mathbf{EG}\,\phi]\!]$ (exercise) and so we can compute $[\![\mathbf{EG}\,\phi]\!]$ using

$$\begin{aligned}[\![\mathbf{EG}_0\,\phi]\!] &= S \\ [\![\mathbf{EG}_{i+1}\,\phi]\!] &= [\![\phi]\!] \cap \mathrm{pre}_\exists([\![\mathbf{EG}_i\,\phi]\!])\end{aligned}$$

Fixed-point theory

What is happening here is that we are computing *fixed-points*.

A set $X \subseteq S$ is a fixed point of a function $F \in \mathcal{P}(S) \rightarrow \mathcal{P}(S)$ iff $F(X) = X$.

We have that

$$\begin{array}{rcl} [\![\mathbf{EF}_n\,\phi]\!] & = & [\![\mathbf{EF}_{n+1}\,\phi]\!] \\ & = & [\![\phi \vee \mathbf{EX}\,\mathbf{EF}_n\,\phi]\!] \\ & = & [\![\phi]\!] \cup \mathrm{pre}_{\exists}([\![\mathbf{EF}_n\,\phi]\!]) \end{array}$$

so $[\![\mathbf{EF}_n\,\phi]\!]$ is a fixed point of

$$F(Y) \doteq [\![\phi]\!] \cup \mathrm{pre}_{\exists}(Y) \quad .$$

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

Fixed-point theorem

A function $F \in \mathcal{P}(S) \to \mathcal{P}(S)$ is monotone iff $X \subseteq Y$ implies $F(X) \subseteq F(Y)$ of S.

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

Given a collection of sets $C \subseteq \mathcal{P}(S)$, a set $X \in C$ is

- the least element of C iff $\forall Y \in C.\ X \subseteq Y$,
- the greatest element of C iff $\forall Y \in C.\ X \supseteq Y$.

Knaster-Tarski Theorem (special case)
Let S be a set with n elements and $F \in \mathcal{P}(S) \to \mathcal{P}(S)$ 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

Proof: See p241 H&R

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 of temporal connectives

When $F \in \mathcal{P}(S) \to \mathcal{P}(S)$ is 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

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

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

Further CTL Equivalences

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

$$
\begin{aligned}
\mathbf{EF}\,\phi &\equiv \phi \lor \mathbf{EX}\,\mathbf{EF}\,\phi \\
\mathbf{EG}\,\phi &\equiv \phi \land \mathbf{EX}\,\mathbf{EG}\,\phi \\
\mathbf{AF}\,\phi &\equiv \phi \lor \mathbf{AX}\,\mathbf{AF}\,\phi \\
\mathbf{AG}\,\phi &\equiv \phi \land \mathbf{AX}\,\mathbf{EG}\,\phi \\
\mathbf{E}[\phi\,\mathbf{U}\,\psi] &\equiv \psi \lor (\phi \land \mathbf{EX}\,\mathbf{E}[\phi\,\mathbf{U}\,\psi]) \\
\mathbf{A}[\phi\,\mathbf{U}\,\psi] &\equiv \psi \lor (\phi \land \mathbf{AX}\,\mathbf{A}[\phi\,\mathbf{U}\,\psi])
\end{aligned}
$$

Fair CTL model checking

A fair version $\mathbf{E}_\psi\mathbf{G}\,\phi$ of $\mathbf{EG}\,\phi$ holds in a state *s* if there exists a path from *s* such that

1. ϕ holds in every state of the path, and
2. ψ holds infinitely often along the path.

We can define it using a greatest fixed-point operator ν

$$\mathbf{E}_\psi\mathbf{G}\,\phi \quad = \quad \nu Z.\, \phi \wedge \mathbf{EX}\,\mathbf{E}[\phi\,\mathbf{U}\,(\psi \wedge Z)]$$

How do we compute it?

- Its definition has nested fixed-points as there is a μ least fixed-point operator in the $\mathbf{E}[\_\mathbf{U}\_]$ definition
- In each iteration of the computation of the ν fixed-point, we have to complete a full set of iterations of the μ fixed-point computation.

Fair CTL model checking is useful both because of the extra expressivity it brings to CTL and because LTL model checking can be reduced to it.