

Temporal Logic and State Systems

Prof. Dr. Fred Kröger

Verification of Finite State Systems: Model Checking

Finite State Systems

Definition (Finite State System):

A **finite state system** (briefly: FSS) $\Psi = (V, S, T)$ is given by

- a finite set V of **system** (or **state**) **variables**,
- a set S of **(system) states** $\eta : V \rightarrow \{\text{ff}, \text{tt}\}$,
- a total **transition relation** $T \subseteq S \times S$.

An adequate temporal logic for FSS is a propositional one (LTL, CTL, ...).

Verification Methods

Methods for verifying a property A for a specification \mathcal{F}_Ψ of an FSS $\Psi = (V, S, T)$:

1. Show $\mathcal{F}_\Psi \vdash A$ as for "infinite" systems (verification by deduction).
2. Show that " A holds in all runs of Ψ " (model checking).

This means:

- In linear temporal logics: Check whether all temporal structures W_Ψ induced by Ψ satisfy A .
- In branching time logics: Check whether A is valid in K_Ψ .

(K_Ψ is the temporal structure (S, ρ) with $i\rho j$ given by $(\eta_i, \eta_j) \in T$ for $\eta_i, \eta_j \in S$.)

Verification of Finite State Systems: Basics of CTL Model Checking

CTL Model Checking

Definition (Satisfactory Set):

Let $\Psi = (V, S, T)$ be an FSS and F a formula of $\mathcal{L}_{\text{CTL}}(V)$. The **satisfactory set** $\llbracket F \rrbracket$ of F (in Ψ) is the set $\llbracket F \rrbracket = \{\eta \in S \mid \eta \models F\}$.

(Notation: $\eta \models F$ for $K_{\Psi}^{(\eta)}(F) = \text{tt.}$)

CTL Model checking means:

For Ψ and F : Determine $\llbracket F \rrbracket$.

(Then: F is valid in $K_{\Psi} \Leftrightarrow \llbracket F \rrbracket$ contains all states of Ψ .)

Determination of $\llbracket F \rrbracket$

$\llbracket F \rrbracket$ can be recursively defined according to the form of F :

$$\llbracket v \rrbracket = \{\eta \in S \mid \eta \models v\}.$$

$$\llbracket \mathbf{false} \rrbracket = \emptyset.$$

$$\begin{aligned} \llbracket A \rightarrow B \rrbracket &= \{\eta \in S \mid \eta \models A \rightarrow B\} \\ &= \{\eta \in S \mid K_{\Psi}^{(\eta)}(A) = \mathbf{ff} \text{ or } K_{\Psi}^{(\eta)}(B) = \mathbf{tt}\} \\ &= (S \setminus \llbracket A \rrbracket) \cup \llbracket B \rrbracket. \end{aligned}$$

(additionally: $\llbracket \neg A \rrbracket = S \setminus \llbracket A \rrbracket$.)

$$\llbracket A \vee B \rrbracket = \llbracket A \rrbracket \cup \llbracket B \rrbracket.$$

$$\llbracket A \wedge B \rrbracket = \llbracket A \rrbracket \cap \llbracket B \rrbracket.$$

$$\llbracket \mathbf{true} \rrbracket = S.)$$

$$\begin{aligned} \llbracket \exists \circ A \rrbracket &= \{\eta \in S \mid \text{there is some } \eta' \in S \text{ with } (\eta, \eta') \in T \text{ and } \eta' \models A\} \\ &= \{\eta \in S \mid \text{there is some } \eta' \in S \text{ with } (\eta, \eta') \in T \text{ and } \eta' \in \llbracket A \rrbracket\}. \end{aligned}$$

The cases $\exists\Box A$ and $A \exists$ **until** B are non-trivial and need some preparations:
 Let $\Psi = (V, S, T)$ be an FSS, $\mathcal{P}(S)$ the power set of S and $\mathcal{P} \subseteq \mathcal{P}(S)$ with $\emptyset \in \mathcal{P}$ and $S \in \mathcal{P}$.

Definition (Monotonicity, Fixpoint):

A mapping $\pi : \mathcal{P} \rightarrow \mathcal{P}$ is called **monotone** if for all $P, Q \in \mathcal{P}$:

$$P \subseteq Q \Rightarrow \pi(P) \subseteq \pi(Q).$$

$P \in \mathcal{P}$ is called **fixpoint** of π , if $\pi(P) = P$.

Lemma:

If $\pi : \mathcal{P} \rightarrow \mathcal{P}$ is monotone then for all $i \in \mathbb{N}$:

- a) $\pi^i(\emptyset) \subseteq \pi^{i+1}(\emptyset)$.
- b) $\pi^i(S) \supseteq \pi^{i+1}(S)$.

Lemma:

Let $\pi : \mathcal{P} \rightarrow \mathcal{P}$ be monotone, $LFP(\pi) = \bigcup_{i \in \mathbb{N}} \pi^i(\emptyset)$, $GFP(\pi) = \bigcap_{i \in \mathbb{N}} \pi^i(S)$.

Then: $LFP(\pi) \in \mathcal{P}$, $GFP(\pi) \in \mathcal{P}$, and $LFP(\pi)$ and $GFP(\pi)$ are fixpoints of π .

Let $\Psi = (V, S, T)$ be an FSS and $\mathcal{P}_\Psi = \{\llbracket F \rrbracket \mid F \text{ formula of } \mathcal{L}_{\text{CTL}}(V)\}$ be the set of all satisfactory sets of formulas of $\mathcal{L}_{\text{CTL}}(V)$. (Then: $\mathcal{P}_\Psi \subseteq \mathcal{P}(S)$, $\emptyset = \llbracket \mathbf{false} \rrbracket \in \mathcal{P}_\Psi$, $S = \llbracket \mathbf{true} \rrbracket \in \mathcal{P}_\Psi$.) Let A and B be formulas of $\mathcal{L}_{\text{CTL}}(V)$ and the mappings

$\pi_1, \pi_2 : \mathcal{P}_\Psi \rightarrow \mathcal{P}_\Psi$ be defined by:

$$\pi_1(\llbracket F \rrbracket) = \llbracket A \wedge \exists \circ F \rrbracket,$$

$$\pi_2(\llbracket F \rrbracket) = \llbracket B \vee (A \wedge \exists \circ F) \rrbracket.$$

Lemma:

π_1 and π_2 are monotone.

Theorem:

$$\llbracket \exists \square A \rrbracket = \text{GFP}(\pi_1).$$

Theorem:

$$\llbracket A \exists \text{until } B \rrbracket = \text{LFP}(\pi_2).$$

Construction of $\llbracket \exists \square A \rrbracket$:

Let the formulas C_0, C_1, C_2, \dots be given by

$$C_0 \equiv \mathbf{true}, \quad C_{i+1} \equiv A \wedge \exists \bigcirc C_i \quad \text{for } i = 0, 1, 2, \dots$$

Construct $\llbracket C_i \rrbracket$ for $i = 0, 1, 2, \dots$ until $\llbracket C_{k+1} \rrbracket = \llbracket C_k \rrbracket$ for some k . Then

$$\llbracket \exists \square A \rrbracket = \llbracket C_k \rrbracket.$$

Construction of $\llbracket A \exists \mathbf{until} B \rrbracket$:

Let the formulas D_0, D_1, D_2, \dots be given by

$$D_0 \equiv \mathbf{false},$$

$$D_{i+1} \equiv B \vee (A \wedge \exists \bigcirc D_i) \quad \text{for } i = 0, 1, 2, \dots$$

Construct $\llbracket D_i \rrbracket$ for $i = 0, 1, 2, \dots$ until $\llbracket D_{k+1} \rrbracket = \llbracket D_k \rrbracket$ for some k .

Then $\llbracket A \exists \mathbf{until} B \rrbracket = \llbracket D_k \rrbracket$.