

Theorem:

For every (r)fSTS Γ the following axioms are Γ -valid (for every $\lambda \in Act_\Gamma$):

(action) $exec\ \lambda \rightarrow enabled_\lambda$

(fair) $\Box\Diamond\ enabled_\lambda \rightarrow \Diamond\ exec\ \lambda$

From this theorem, the following formula can be derived:

(progress) $enabled_\lambda \rightarrow \neg nil_\Gamma$ for every $\lambda \in Act_\Gamma$

Specification and Verification of State Systems: Verification

Verification of State Systems

Specification of (the set of execution sequences of) an (f)(r)(l)STS Γ : $(\mathcal{L}_{T\Gamma}, \mathcal{A}_\Gamma)$

Verification: Formal proof of “properties” of Γ (described by formulas F) by deriving

$$\mathcal{A}_\Gamma \vdash F$$

Note: The choice of an adequate language \mathcal{L}_T depends on:

- the type of Γ ,
- which properties are to be considered.

Classification of Properties

Simple classification according to the form of the specifying formulas.

Invariance properties: $A \rightarrow \square B$

Precedence properties: $A \rightarrow B$ **atnext** C

$A \rightarrow B$ **unless** C

⋮

Eventuality properties: $A \rightarrow \diamond B$

(A, B, C are state formulas of the system in question.)

In the following: Basic proof rules for these classes (only for (r)lSTS or (r)fSTS).

Proof Rules for Invariance Properties

(inv) $A \rightarrow B, B \mathbf{invof} Act_{\Gamma} \vdash A \rightarrow \Box B$ (invariance rule)

(inv') $start_{\Gamma} \rightarrow A, A \mathbf{invof} Act_{\Gamma} \vdash \Box A$

Remark: (inv) is mostly applied in the form:

$$A \rightarrow B', B' \mathbf{invof} Act_{\Gamma}, B' \rightarrow B \vdash A \rightarrow \Box B$$

Proof Rules for Precedence Properties

(atnext) $exec \lambda \wedge A \rightarrow \circ(C \rightarrow B) \wedge \circ(\neg C \rightarrow A)$ for every $\lambda \in Act_{\Gamma}$,
 $nil_{\Gamma} \wedge A \rightarrow (C \rightarrow B)$
 $\vdash A \rightarrow B$ **atnext** C if A, B , and C are state formulas of Γ

Analogously for **unless**, **before**, ..., e.g.:

(unless) $exec \lambda \wedge A \rightarrow \circ C \vee \circ(A \wedge B)$ for every $\lambda \in Act_{\Gamma}$,
 $nil_{\Gamma} \wedge A \rightarrow B \vee C$
 $\vdash A \rightarrow B$ **unless** C if A, B , and C are state formulas of Γ

A Proof Rule for Eventuality Properties

$$\begin{aligned}
 \text{(well)} \quad & exec\lambda \wedge H_\lambda \wedge A \rightarrow \bigcirc(B \vee \exists \bar{z}(\bar{z} \prec z \wedge A_z(\bar{z}))) \quad \text{for every } \lambda \in Act_\Gamma, \\
 & exec\lambda \wedge \neg H_\lambda \wedge A \rightarrow \bigcirc(B \vee \exists \bar{z}(\bar{z} \preceq z \wedge A_z(\bar{z}))) \quad \text{for every } \lambda \in Act_\Gamma, \\
 & \square A \rightarrow \diamond(B \vee E_\Gamma) \\
 & \vdash \exists z A \rightarrow \diamond B \quad \text{if } A \text{ and } B \text{ are state formulas of } \Gamma
 \end{aligned}$$

where: $Act_\Gamma = \{\lambda_1, \dots, \lambda_m\}$,

$H_{\lambda_1}, \dots, H_{\lambda_m}$ formulas of $\mathcal{L}_{T\Gamma}$ without flexible symbols,

$E_\Gamma \equiv (H_{\lambda_1} \wedge enabled_{\lambda_1}) \vee \dots \vee (H_{\lambda_m} \wedge enabled_{\lambda_m})$.

(Assume given an appropriate signature with well-founded ordering.)