5.2 Automata-based model checking

Given a T.S. TS and φ, decide whether

$$TS \models \varphi$$

If φ is refuted, provide an error trace.

Note: TS is assumed finite and without terminal states

First we make some observations

$$\begin{aligned} TS \models \varphi &\text{ iff } Traces(TS) \subseteq words(\varphi) \\ &\text{iff } Traces(TS) \cap (2^{AP})^\omega \setminus words(\varphi) = \emptyset \\ &\text{iff } Traces(TS) \cap words(\neg\varphi) = \emptyset \\ &\text{iff } traces(TS) \cap \mathcal{L}_\omega(A_{\neg\varphi}) = \emptyset \end{aligned}$$

How do we algorithmically check that

$$Traces(TS) \cap \mathcal{L}_\omega(A_{\neg\varphi}) = \emptyset \quad ?$$

Combine the T.S. TS and the NBA $A_{\neg\varphi}$ into a new, extended T.S. and check that there are no paths that are simultaneously

Traces of TS and acceptance of Aφ.
This last property can be expressed by a formula stating that eventually no states in F are visited.

Def (4.62)

Let $TS = (S, Act, \to, I, AP, L)$ be a T.S. without terminal states and $A = (Q, 2^{AP}, \delta, Q_0, F)$ a non-blocking NBA. Then $TS \otimes A$ is the following T.S.:

$$TS \otimes A = (S \times Q, Act, \to', I', AP', L')$$

where $\to'$ is the smallest relation satisfying

$$\frac{s \xrightarrow{\alpha} t \text{ and } q \xrightarrow{L(t)} p}{(s,q) \to' (t,p)}$$

and

$$I' = \{(s_0, q) \mid s_0 \in I \text{ and } \exists q_0 \in Q_0 . q_0 \xrightarrow{L(s_0)} q\}$$

$$AP' = Q$$

$L' : S \times Q \to 2^Q$ is given by $L'((s,q)) = \{q\}$

Let $P_{pers}(A)$ be the formula

$$\Diamond\Box \neg F$$

where $\neg F$ denotes the formula $\bigwedge_{q \in F} \neg q$ over $AP' = Q$.

Thm 4.63

$$Traces(TS) \cap L_\omega(A) = \emptyset$$

iff

$$TS \otimes A \not\models P_{pers}(A)$$

We are thus left with the task of how to establish whether $TS \otimes A \not\models P_{pers}(A)$.

Formulas such as $P_{pers}(A)$ are called persistence properties. For such formulas this problem can be resolved as follows:

Thm 4.64 $P_{pers} = \Diamond\Box\varphi$

$TS \not\models P_{pers}$ iff There exists a reachable $\neg\varphi$ state s which belongs to a cycle. That is

$\exists s \in Reach(TS).\ s \not\models \varphi \wedge s$ is on a cycle in $G(TS)$.