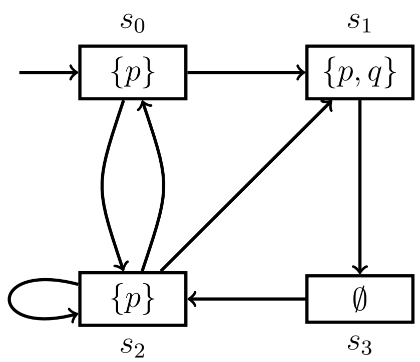
Model Checking – Exercise sheet 10

Exercise 10.1
Create a NuSMV model for the following Kripke structure over $AP = \{p, q\}$:



Use NuSMV to model check each of the following formulas. Explain in word if the formula holds, or give a counterexample otherwise.

(a) $\mathbf{EG}\ p$,

(b) $\mathbf{AX}\ \mathbf{AF}\ \mathbf{EG}\ p$,

(c) $p\ \mathbf{AU}\ q$,

(d) $\mathbf{AG}(p \rightarrow \mathbf{AX}\ p)$,

(e) $\mathbf{EX}(\neg q \wedge (\neg p\ \mathbf{EU}\ q))$.

Exercise 10.2
Model the following stack system in NuSMV:

> The stack system consists of three input interfaces: `push`, `pop`, `in_val`; and one output interface: `out_val`. The values of `push` and `pop` can be either `true` or `false`, while `in_val` and `out_val` can take any number between 0 and 9.
>
> When `push` is `true`, the system takes the input from `in_val` and pushes it onto its internal stack. When `pop` is `true`, the system removes the value on the top of the stack and outputs it via `out_val`. It is forbidden to call `push` and `pop` at the same time. The size of the stack is 5, i.e. the stack is full if there are 5 pushes without a pop. When the stack is full, it ignores `push` and `in_val`. Similarly, the system ignores `pop` when the stack is empty. The value of `out_val` is undefined if the stack is empty or `pop` is `false`.

Write the following properties in CTL and use `NuSMV` to model check the formulas:

(a) The stack cannot be empty and full at the same time.

(b) There exists a path along which the stack is eventually always full.

(c) From any given point of time, there always exists a path in which the stack will be full.

(d) The stack cannot be empty after a push.

(e) The internal stack is correctly updated after a push or pop.

(f) Whenever the stack is full, there exists a path in which the stack stays full forever or it remains full until a pop.

(g) For every push, there exists a path that pops the value without pushing another value.

(h) After every pop, `out_val` holds the correct value.

Exercise 10.3
Let $\mathcal{K} = (S, \rightarrow, r, AP, \nu)$ be a Kripke structure. For every $X \subseteq S$, $i \in \mathbb{N}$ and CTL formulas φ and ψ, let

$$\begin{aligned}\xi^0_{\varphi,\psi}(X) &= X,\\ \xi^{i+1}_{\varphi,\psi}(X) &= [\![\psi]\!] \cup \left([\![\varphi]\!] \cap \text{pre}(\xi^i_{\varphi,\psi}(X))\right).\end{aligned}$$

(a) Show that if $[\![\varphi]\!] \subseteq [\![\varphi']\!]$, $[\![\psi]\!] \subseteq [\![\psi']\!]$ and $X \subseteq X'$, then $\xi^i_{\varphi,\psi}(X) \subseteq \xi^i_{\varphi',\psi'}(X')$ for every $i \in \mathbb{N}$.

(b) Show that if $(\varphi \Rightarrow \varphi') \wedge (\psi \Rightarrow \psi')$, then $(\varphi \; \mathbf{EU} \; \psi) \Rightarrow (\varphi' \; \mathbf{EU} \; \psi')$, $\mathbf{EF}\varphi \Rightarrow \mathbf{EF}\varphi'$ and $\mathbf{AG}\varphi \Rightarrow \mathbf{AG}\varphi'$.