FMSE Exercise Course 3: Solutions

1.

SandT

$a, b : \mathbb{N}$

$a \leq b \land a \geq b$

The invariant can be simplified to $a = b$

SorT

$a, b : \mathbb{N}$

$a \leq b \lor a \geq b$

The invariant is trivial since it always holds for all a and b, so it can be removed.

SandU

$a, b : \mathbb{N}$
$c : \mathbb{P}\, \mathbb{N}$

$a \leq b \land a \in c$

2. Since in *HasColor* we have $\Xi InHand$, this implies $hand' = hand$. However, in *PlaysColor* we have $hand' \neq hand$.

3. (a)

$[PERSON, LOCKER]$
$MESSAGE ::= ok \mid ko \mid wait\_list \mid returned \mid to\_first$

Syst

$lockers : \mathbb{P}\, LOCKER$
$hire : LOCKER \pfun PERSON$
$wait : \mathrm{iseq}\, PERSON$

$\mathrm{dom}\, hire \subseteq lockers$
$\mathrm{ran}\, hire \cap \mathrm{ran}\, wait = \varnothing$
$\forall k1, k2 \in \mathrm{dom}\, hire \bullet k1 \neq k2 \Rightarrow hire(k1) \neq hire(k2)$
$\mathrm{dom}\, hire \neq lockers \Rightarrow wait = \varnothing$

Init

Syst

$lockers = \varnothing$
$wait = \varnothing$

(b)

HireAv

$\Delta Syst$
$p? : PERSON$
$l! : LOCKER$
$m! : MESSAGE$

$p? \notin \operatorname{ran} hire$
$\operatorname{dom} hire \neq lockers$
$l! \in lockers \setminus (\operatorname{dom} hire)$
$hire' = hire \oplus \{(l!, p?)\}$
$lockers' = lockers$
$wait' = wait$
$m! = ok$

Precondition:
$p? \notin \operatorname{ran} hire \land \operatorname{dom} hire \neq lockers$

HireNotAv

$\Delta Syst$
$p? : PERSON$
$m! : MESSAGE$

$p? \notin (\operatorname{ran} hire) \cup (\operatorname{ran} wait)$
$\operatorname{dom} hire = lockers$
$wait' = wait \frown \langle p? \rangle$
$lockers' = lockers$
$hire' = hire$
$m! = wait\_list$

Precondition:
$p? \notin (\operatorname{ran} hire) \cup (\operatorname{ran} wait) \land \operatorname{dom} hire = lockers$

HireKO

$\Xi Syst$
$p? : PERSON$
$m! : MESSAGE$

$p? \in (\operatorname{ran} hire) \cup (\operatorname{ran} wait)$
$m! = ko$

Precondition:
$p? \in (\operatorname{ran} hire) \cup (\operatorname{ran} wait)$

$$Hire \mathrel{\widehat=} HireAv \lor HireNotAv \lor HireKO$$

(c)

ReturnWait

$\Delta Syst$
$p? : PERSON$
$l? : LOCKER$
$m! : MESSAGE$

$(l?, p?) \in hire$
$wait \neq \varnothing$
$wait' = tail\ wait$
$hire' = hire \oplus \{(l?, head\ wait)\})$
$lockers' = lockers$
$m! = to\_first$

ReturnNoWait

$\Delta Syst$
$p? : PERSON$
$l? : LOCKER$
$m!MESSAGE$

$(l?, p?) \in hire$
$wait = \varnothing$
$wait' = wait$
$hire' = hire \setminus \{(l?, p?)\})$
$lockers' = lockers$
$m! = returned$

$Return \mathrel{\widehat=} ReturnWait \lor ReturnNoWait$

Note that *Return* is not robust (this was not explicitly asked in the exercise); ofcourse it is easy to make it robust by adding a schema for the case $(l?, p?) \notin hire$.

(d)

Remove

$\Delta Syst$
$ll? : \mathbb{P}\ LOCKER$
$pp! : \mathbb{P}\ PERSON$

$lockers' = lockers \setminus ll?$
$pp! = \{p : PERSON \mid \exists\, l : LOCKER \bullet$
$\qquad l \in ll? \land hire(l) = p\}$
$hire' = hire \setminus \{l : LOCKER, p : PERSON \mid l \in ll?\}$
$wait' = wait$