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

$a, b: \mathbb{N}$		
$a \leq b \lor a \geq b$		

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 $\exists InHand$, this implies hand' = hand. However, in PlaysColor we have hand' \neq hand.

3. (a)

 $[PERSON, LOCKER] \\ MESSAGE ::= ok \mid ko \mid wait_list \mid returned \mid to_first$

Init		
Syst		
$lockers = \emptyset$		
$wait = \emptyset$		

(b)

```
 \begin{array}{l} HireAv \\ \Delta Syst \\ p? : PERSON \\ l! : LOCKER \\ m! : MESSAGE \\ \hline 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 \\ \end{array}
```

```
Precondition:
```

 $p?\notin\operatorname{ran}\mathit{hire}\wedge\operatorname{dom}\mathit{hire}\neq\mathit{lockers}$

HireNotAv
$\Delta Syst$
p?: PERSON
m!: MESSAGE
$p? \notin (\operatorname{ran} hire) \cup (\operatorname{ran} wait)$
dom $hire = lockers$
$wait' = wait \cap \langle p? \rangle$
lockers' = lockers
hire' = hire
$m! = wait_list$

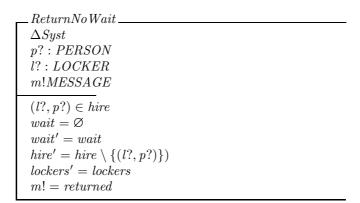
Precondition:

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

HireKO
$\Xi Syst$
p?: PERSON
m!: MESSAGE
$p? \in (\operatorname{ran} hire) \cup (\operatorname{ran} wait)$ $m! = ko$

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

$$Hire \cong HireAv \lor HireNotAv \lor HireKO$$



 $Return \cong Return Wait \lor Return No Wait$

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

(d)

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

(c)