SOEN331: Introduction to Formal Methods for Software Engineering
Assignment 3 on extended finite state machines

Instructor: C. Constantinides

March 28, 2017

Exercise 1: Home heating system

The EFSM of the home heating system is the tuple $S = (Q, \Sigma_1, \Sigma_2, q_0, V, \Lambda)$, where t_r is the desired room temperature, T is the limit temperature and

$Q = \{furnace\_on \ \& \ fan\_off,\ fan\_on \ \& \ furnace\_off,\ fan\_off \ \& \ furance\_off\}$
$\Sigma_1 = \{room\ temperature\ <= t_r - 2,\ room\ temperature >= t_r + 2,$
$\quad furnace\ temperature >= T\}$
$\Sigma_2 = \{turn\ furnace\ on,\ turn\ furnace\ off,\ turn\ furnace\ off\ and\ fan\ on,\ turn\ fan\ off\}$
$q_0 : fan\_off \ \& \ furance\_off$
$V : Desired\ room\ temperature,\ limit\ temperature\ (T) : \mathbb{N}$
Λ: Transition specifications

1. $\rightarrow fan\_off \ \& \ furance\_off$
2. $fan\_off \ \& \ furance\_off \xrightarrow{\text{(room temperature <} \ t_r - 2\text{) / (turn furnace on)}} fan\_off \ \& \ furnace\_on$
3. $fan\_off \ \& \ furnace\_on \xrightarrow{\text{(room temperature >= } t_r + 2\text{) / (turn furnace off)}} fan\_off \ \& \ furance\_off$
4. $fan\_off \ \& \ furnace\_on \xrightarrow{\text{(furnace temperature >= T) / (turn furnace off and fan on)}} fan\_on \ \& \ furnace\_off$
5. $fan\_on \ \& \ furnace\_off \xrightarrow{\text{(furnace temperature <= T - 5) / (turn fan off)}} fan\_off \ \& \ furance\_off$
6. $fan\_on \ \& \ furnace\_off \xrightarrow{\text{(room temperature >= } t_r + 2\text{) / (turn fan off)}} fan\_off \ \& \ furance\_off$

Exercise 2: Arbiter

The EFSM of the arbiter is the tuple $S = (Q, \Sigma_1, \Sigma_2, q_0, V, \Lambda)$, where

$Q = \{idle,\ S1\ (State1),\ S2\ (State2)\}$
$\Sigma_1 = \{Rq1\ (P\ requests\ the\ resource),\ Rq2\ (Q\ requests\ the\ resource),\ after\ (t_r\ time)\}$
$\Sigma_2 = \{allocate,\ return,\ t_{max} = t + t_r\}$
$q_0 : idle$

V : *Maximum utilization time* (t_r), *time* (t), *maximum time* $(t_{max}) : \mathbb{N}$

Λ: Transition specifications

1. $\rightarrow idle$
2. $idle \xrightarrow{\text{Rq1 / (allocate; } t_{max} = t + t_r)} S1$
3. $idle \xrightarrow{\text{Rq2 / (allocate; } t_{max} = t + t_r)} S2$
4. $S1 \xrightarrow{\text{Return}} idle$
5. $S2 \xrightarrow{\text{Return}} idle$
6. $S1 \xrightarrow{after\ (t_r\ time)\ /\ \text{release resource}} idle$
7. $S2 \xrightarrow{after\ (t_r\ time)\ /\ \text{release resource}} idle$