Formal Methods in Software Development
Exercise 8 (January 17)

Wolfgang Schreiner
Wolfgang.Schreiner@risc.jku.at

December 13, 2010

The result is to be submitted by the deadline stated above *via the Moodle interface* of the course as a *.zip or .tgz* file which contains

1. a PDF file with
   - a cover page with the course title, your name, Matrikelnummer, and email address,
   - the deliverables requested in the description of the exercise,
2. the RISC ProofNavigator (.pn) file(s) used in the exercise;
3. the proof directories generated by the RISC ProofNavigator.

Exercise 8: Dining Philosophers

Let S be the model of a system described by initial state condition $I \subseteq State$ and state relation $R \subseteq State \times State$ for some state space $State$. To show that S cannot run into a deadlock, it suffices to show for some state condition Inv

- $\forall s \in State : I(s) \Rightarrow Inv(s)$
- $\forall s, s' \in State : Inv(s) \land R(s, s') \Rightarrow Inv(s')$
- $\forall s \in State : Inv(s) \Rightarrow \exists s' \in State : R(s, s')$

In other words, *Inv* must be an invariant of the system (*Inv* holds on every state) and, always when *Inv* holds, the system can make another transition (thus the system can always make a transition).

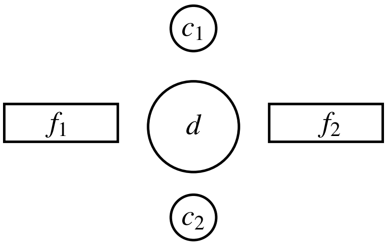
Let us consider a system of two philosophers sitting on the opposites side of a desk each with a plate of spaghetti. Each philosopher wants to talk ("philosophize") a bit and then to eat a bit; the philosophers repeat this behavior forever.

The problem is that on the desk there are only two forks positioned between the philosophers. In order to eat, a philosopher has to grab one fork and then another fork before she can start eating. However, if both philosophers at the same time grab e.g. their respective left forks, they cannot grab their right forks any more and no one can start to eat (so they starve).

To overcome the problem, the philosophers place a coin on the table. Before grabbing a fork, a philosopher has to grab the coin. Then she grabs one fork (randomly the left or the right one), then the other fork, and finally starts to eat. When she is done, she returns the forks and the coin.

The goal of this exercise is to show that the philosophers will indeed not starve.

The state of the system can be described by five integer variables f_1, f_2, c_1, c_2, d where f_i is set to 0, if fork i is on the table, respectively to 1 or 2, if it is grabbed by the corresponding philosopher. Furthermore, c_i is set to 1 respectively 0 indicating whether philosopher i holds the coin or not, and d is set to 1 respectively 0 indicating whether the coin is on the table or not[1].



- (35P) Let a state s be denoted by a tuple $\langle f_1, f_2, c_1, c_2, d\rangle$. Define *State*, *I*, and *R* correspondingly. Decompose *R* into four named transitions for grabbing the coin, grabbing the left fork, grabbing the right fork, and returning the coin and both forks, where each transition is parameterized over the number of the philosopher performing the transition (i.e., define $R(\ldots, \ldots) :\Leftrightarrow \exists i \in \mathbb{Z} : (i = 1 \lor i = 2) \land (Coin(i, \ldots, \ldots) \lor \ldots))$. Show a trace of the variables for a (part of a) system run where at least five transitions are performed. Based on the trace, define a suitable system invariant (hint: the core of the invariant is based on the sum of c_1, c_2, and d).

[1] The model is chosen more general than necessary such that it can be easily adapted to n philosophers.

- (30P) Formalize the system in the RISC ProofNavigator using the type INT for the system variables. Prove that the system maintains the invariant and that the invariant ensures that the philosophers do not starve.

  Hints: to preserve an intuitive proof structure, expand the definitions of the individual transitions as late as possible. In the last proof, perform a suitable case distinction on the state space and then manually instantiate the existentially quantified variables.

- (35P) Generalize the model to n philosophers with $n - 1$ coins being placed on the table. Model the forks as an array $f : \mathbb{N}_n \to \mathbb{Z}$ and the grabbed tokens as an array $c : \mathbb{N}_n \to \mathbb{Z}$ where $\mathbb{N}_n = \{0, \ldots, n - 1\}$. Define the transition relation $R(\ldots, \ldots) :\Leftrightarrow \exists i \in \mathbb{Z} : 1 \leq i \leq n \land \ldots$. Generalize the invariant correspondingly. You need *not* formalize this model in the RISC ProofNavigator and not perform the proofs.

  Hint: you may use the notation $f[i \mapsto a]$ to indicate that version of f where i is mapped to a new value a.

The results of the exercise are the requested models in mathematical notation, the RISC ProofNavigator formalization, screenshots of the constructed proof trees with an explicit indications whether you succeeded or not, and, if not, where you failed and the probable reason of the failure.