

DEPLOY Blocked Course

(ETH Zurich 9-11 April, 2008)

Exercise Sheet 2: A Small Society and Development of Patterns

Description of Work

The exercise has two parts.

The aim of the first part is:

- to use set theoretical notation to do some modeling.
- to do the proofs using the Rodin Tool.

The example that we use in this part is the “family” example used in the slides “Summary of Mathematical Notation”.

The aim of the second part of this exercise is to see how failed proof attempts help us to improve our model. The example chosen here is the development of the patterns as mentioned in the lecture of the “Mechanical Press”. An important point to notice here is the difference between invariants and guards.

A Small Society

Enter the Basic Concepts

Create a new Rodin project and then a context to enter the following basic definitions of a simple society using constants and axioms.

$$\begin{aligned} \textit{men} &\subseteq \textit{PERSON} \\ \textit{women} &= \textit{PERSON} \setminus \textit{men} \\ \textit{husband} &\in \textit{women} \rightsquigarrow \textit{men} \\ \textit{mother} &\in \textit{PERSON} \rightarrow \text{dom}(\textit{husband}) \end{aligned}$$

$$\begin{aligned}
\text{father} &= \text{mother}; \text{husband} \\
\text{children} &= (\text{mother} \cup \text{father})^{-1} \\
\text{daughter} &= \text{children} \triangleright \text{women} \\
\text{sibling} &= (\text{children}^{-1}; \text{children}) \setminus \text{id}(\text{PERSON})
\end{aligned}$$

Solution:

See context *c0* in the development in the Rodin Platform archive within *family_sol.zip*.

Define New Concepts

Defining the following concepts and enter them as in a new context which “extends” the one defined in the previous exercise.

$$\begin{aligned}
\text{brother} &= ? \\
\text{sibling_in_law} &= ? \\
\text{nephew_or_niece} &= ? \\
\text{uncle_or_aunt} &= ? \\
\text{cousin} &= ?
\end{aligned}$$

Here we assume that the son of my brother in law is my nephew.

Solution:

$$\begin{aligned}
\text{brother} &= \text{sibling} \triangleright \text{men} \\
\text{sibling_in_law} &= (\text{spouse}; \text{sibling}) \cup (\text{sibling}; \text{spouse}) \\
\text{nephew_or_niece} &= (\text{sibling} \cup \text{sibling_in_law}); \text{children} \\
\text{uncle_or_aunt} &= \text{nephew_or_niece}^{-1} \\
\text{cousin} &= \text{uncle_or_aunt}; \text{children}
\end{aligned}$$

Prove Theorems

Define the following theorems and prove them.

$$\begin{aligned}
\text{mother} &= \text{father}; \text{wife} \\
\text{spouse} &= \text{spouse}^{-1} \\
\text{sibling} &= \text{sibling}^{-1} \\
\text{father}; \text{father}^{-1} &= \text{mother}; \text{mother}^{-1} \\
\text{father}; \text{mother}^{-1} &= \emptyset \\
\text{mother}; \text{father}^{-1} &= \emptyset \\
\text{father}; \text{children} &= \text{mother}; \text{children}
\end{aligned}$$

Hints: The following strategy is good:

- Expanding the definitions. (This usually done automatically by post-tactics).
- Removing redundant hypotheses.
- Apply external prover “p0”.

Solution:

See the development in the Rodin Platform archive within *family_sol.zip*.

Prove a Difficult Theorem (Challenge Exercise)

Define the following theorem and prove.

$$\text{cousin} = \text{cousin}^{-1}$$

Hint:

- The following lemma will be helpful

$$\text{sibling_in_law} = \text{sibling_in_law}^{-1} .$$

- Also you might want to disable the “Use Equals Hypotheses” tactic from the set of post-tactics.

Solution:

See the development in the Rodin Platform archive within *family_sol.zip*.

Development of Patterns

First you need to import the development in *pattern_poor.zip* into your Rodin workspace.

The Weak-synchronization Pattern

In the specification of the weak-synchronization pattern (namely **weak**), there is one remaining proof obligation ($r_on/pat0_5/INV$). Open the obligation in your interactive proving interface. Can you prove the obligation? Otherwise, suggest a way to improve our model to fix the inconsistency.

Solution:

Add $r = 0 \wedge a = 1 \Rightarrow cr < ca$ as an invariant.

The Strong-synchronization Pattern

This is a refinement of the weak-synchronization pattern. There is one remaining proof obligation ($a_on/pat1_1/INV$). Following the description of the pattern in the slides to improve the model in order to fix the problem.

Solution:

- Add $r = 1$ as a guard of the event a_on .
- Add $r = 1 \wedge a = 0 \Rightarrow cr = ca$ as an invariant.
- Add $r = 0$ as a guard of the event a_off .

Strong-Weak Pattern (Challenge Exercise)

There are two undischarged proof obligations, namely $r_off/dbl1_1/INV$ and $s_on/dbl1_1/INV$ in the strong-weak pattern. Follow the description of the pattern in the slides to fix the remaining problem in the strong-weak pattern development.

Solution:

- Add $b = 1 \Rightarrow r = 1$ as an invariant.
- Add $a = 0 \Rightarrow s = 0$ as an invariant.
- Add $r = 1$ as a guard of event b_on .
- Add $a = 0 \Rightarrow b = 0$ as an invariant.
- Add $s = 0$ as a guard of event a_off .
- Add $b = 0$ as a guard of event a_off .
- Add $a = 1$ as a guard of event b_on .

Strong-Strong Pattern (Challenge Exercise)

This is a refinement of the Strong-weak pattern in the previous exercise. Once you finish correcting the Strong-weak pattern, there should be 6 undischarged proof obligations. Follow the description of the pattern on the slides to fix the problem.

- Prove the obligations $thm1$, $thm2$, $a_on/dbl2_2/INV$, $r_on/dbl2_5/INV$.

Solution:

See the development within the Rodin Platform archive in *pattern_rich.zip*.

- Follow the description of the pattern to fix the problem related to the obligations $r_off/dbl2_5/INV$, $s_off/dbl2_4/INV$

Hints: You only need to add some missing invariants relating m with the original variables a, b, r, s .

Solution:

Add invariants:

- $r = 1 \wedge a = 0 \Rightarrow m = 0$
- $m = 1 \Rightarrow s = 0$