ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

J-R. Abrial, T.S. Hoang and M. Schmalz

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.

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

$$husband \in women \rightarrowtail men$$

$$mother \in PERSON \rightarrow \mathrm{dom}(husband)$$

$$father = mother ; husband$$

$$children = (mother \cup father)^{-1}$$

$$daughter = children \rhd women$$

$$sibling = (children^{-1} ; children) \setminus \mathrm{id}(PERSON)$$

Define New Concepts

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

$$brother = ?$$

$$sibling\_in\_law = ?$$

$$nephew\_or\_niece = ?$$

$$uncle\_or\_aunt = ?$$

$$cousin = ?$$

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

Prove Theorems

Define the following theorems and prove them.

$$mother = father ; wife$$

$$spouse = spouse^{-1}$$

$$sibling = sibling^{-1}$$

$$father ; father^{-1} = mother ; mother^{-1}$$

$$father ; mother^{-1} = \varnothing$$

$$mother ; father^{-1} = \varnothing$$

$$father ; children = mother ; children$$

Hints: The following strategy is good:

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

Prove a Difficult Theorem (Challenge Exercise)

Define the following theorem and prove.

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

Hint:

- The following lemma will be helpful

$$sibling\_in\_law = sibling\_in\_law^{-1} .$$

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

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.

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.

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.

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*.

- 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.