Exercise Sheet 5: Interactive Proofs in the Predicate Calculus

1 Introduction

1.1 Purpose

The purpose of this exercise is to make you familiar with the practice of interactive proofs with the Rodin Platform on the Predicate Calculus.

1.2 Your Task

We distribute to you a Rodin development named "05_pred": it contains 8 contexts, each of which with one theorem. You will be asked to prove these theorems by using 3 successive *tactic profile*: "pred_profile_1", "pred_profile_2", and "pred_profile_3". Each of them is a slight extension of the previous one.

1.3 Grading

The grading of this exercise will be made on the basis of the proofs of the 8 theorems *using the second tactic profile* "pred_profile_2" only. Hand out your proofs in a corresponding renamed export of the development: "05_pred_XXX".

In the last section, we give some hints to help discharging some of the proofs with the profile "pred_profile_2".

2 Some Red Operator Buttons

In this section we present two more red operator buttons besides the ones we introduced in the previous exercise. We also present the very important notion of instantiation of existential goal and universal hypotheses.

2.1 Another Goal Red Operators (as labeled in the Rodin Platform)

Forall Instantiation

$$\frac{\mathbf{H} \vdash \mathbf{P(x)}}{\mathbf{H} \vdash \forall \mathbf{x} \cdot \mathbf{P(x)}} \qquad \text{where } \mathbf{x} \text{ is not free in } \mathbf{H}$$

When **x** is free in **H**, a change of variable is automatically performed.

2.2 Another Hypotheses Red Operator (as labeled in the Rodin Platform)

Free Existential Variables

$$\frac{\mathbf{H}, \mathbf{P(x)} \vdash \mathbf{G}}{\mathbf{H}, \exists \mathbf{x} \cdot \mathbf{P(x)} \vdash \mathbf{G}} \qquad \text{where } \mathbf{x} \text{ is not free in } \mathbf{H} \text{ and in } \mathbf{G}$$

When **x** is free in **H** or **G**, a change of variable is automatically performed.

2.3 Existential Instantiation in the Goal

$$\frac{\mathbf{H} \vdash \mathbf{P}(\mathbf{E})}{\mathbf{H} \vdash \exists \mathbf{x} \cdot \mathbf{P}(\mathbf{x})}$$

For doing this, write the instantiation **E** (there might be several of them in case there are several quantified variables) in the yellow box and then press the red operator $\exists$.

2.4 Universal Instantiation in the Hypotheses

$$\frac{\mathbf{H}, \mathbf{P}(\mathbf{E}) \vdash \mathbf{G}}{\mathbf{H}, \forall \mathbf{x} \cdot \mathbf{P}(\mathbf{x}) \vdash \mathbf{G}}$$

For doing this, write the instantiation **E** (there might be several of them in case there are several quantified variables) in the yellow box. Then there are two cases:

1. In the case where the hypothesis has the following shape:

   $$\forall x \cdot P(x) \Rightarrow Q(x)$$

   press the red operator $\Rightarrow$ and, in the coming menu, press the button "Instantiate universal followed by modus ponens" or the button "Instantiate universal followed by modus tollens".

2. In the case where the hypothesis has NOT the previous shape, press the red operator $\forall$.

3 Tactic Profile 1

The tactic profile "pred_profile_1" is a slight extension of the tactic profile "prp_profile_4" used in the previous exercise. It contains the following additional elementary tactic:

True Goal

$$\frac{}{\mathbf{H} \vdash \top}$$

When using this tactic profile, the user will be asked to depress the additional red operator button in the goal (section 2.1) and then the additional red operator button in the hypotheses (section 2.2) . Some instantiations of existential goal (section section 2.3) or universal hypothesis (section 2.4) will also be necessary.

Use Profile 1 for the proofs of the theorems in contexts "pred0" and "pred1". For the other theorems, use directly Profile 2 and then later again with Profile 3.

4 Tactic Profile 2

This profile extends Profile 1 by adding an elementary tactics for the goal and an elemenary tactic for the hypotheses. The added elementary tactics are the following:

Forall Goal (Forall Instantiation)

$$\frac{\mathbf{H} \vdash \mathbf{P}(\mathbf{x})}{\mathbf{H} \vdash \forall \mathbf{x} \cdot \mathbf{P}(\mathbf{x})} \qquad \text{where } \mathbf{x} \text{ is not free in } \mathbf{H}$$

When **x** is free in **H**, a change of variable is automatically performed.

Exists Hypothesis (Free Existential Variables)

$$\frac{\mathbf{H}, \mathbf{P}(\mathbf{x}) \vdash \mathbf{G}}{\mathbf{H}, \exists \mathbf{x} \cdot \mathbf{P}(\mathbf{x}) \vdash \mathbf{G}} \qquad \text{where } \mathbf{x} \text{ is not free in } \mathbf{H} \text{ and in } \mathbf{G}$$

When **x** is free in **H** or **G**, a change of variable is automatically performed.

As a consequence, it is now not necessary to depress the red operator in the goal (section 2.1) and the red operator in the hypotheses (section 2.2). The user is still asked to perform some proof by cases and, more difficult, some instantiations in the goal (section 2.3) or in the hypotheses (section 2.4).

5 Tactic Profile 3

This profile extends Profile 2 by adding a call to the automatic prover P0. All proofs are now discharged automatically

6 Hints

6.1 For the theorem in context "pred4"

1. At some point , you have to prove the following sequent (there are more hypotheses):

   $$\begin{array}{l} \forall x, y, z \cdot x \mapsto z \in R \land y \mapsto z \in R \Rightarrow x \mapsto y \in R \\ x \mapsto y \in R \\ \vdash \\ x \mapsto z \in R \end{array}$$

   Try to figure out what the right instantiations for x, y, and z should be.

   WARNING: After doing this instantiation, you will see that the hypothesis

   $$\forall x, y, z \cdot x \mapsto z \in R \land y \mapsto z \in R \Rightarrow x \mapsto y \in R$$

   disappeared. You can get it back again by pressing the "Show cache hypotheses" button in the "Proof Control" pannel and then select this hypothesis on the window appearing on the right part of the screen.

2. For your instantiation to be accepted you need to prove the following (there are more hypotheses):

   $$\begin{array}{l} \forall x, y, z \cdot x \mapsto z \in R \land y \mapsto z \in R \Rightarrow x \mapsto y \in R \\ y \mapsto z \in R \\ \vdash \\ z \mapsto y \in R \end{array}$$

   Try to figure out what the right instantiations for x, y, and z should be.

3. For your instantiation to be accepted you need to prove the following (there are more hypotheses):

   $$\begin{array}{l} \forall x \cdot \exists y \cdot x \mapsto y \in R \\ \forall x, y, z \cdot x \mapsto z \in R \land y \mapsto z \in R \Rightarrow x \mapsto y \in R \\ y \mapsto z \in R \\ \vdash \\ z \mapsto z \in R \end{array}$$

   Instantiate x in the first hypothesis with z and then figure out what the right instantiations for x, y, and z should be in the second hypothesis.

6.2 For the theorem in context "pred5"

Instantiate x with x in the existential goal and then try to figure out how to instantiate the universal hypotheses.

6.3 For the theorem in context "pred6"

1. Remove the useless hypotheses
2. Instantiate the first universal hypothesis with x
3. Instantiate the new first universal hypothesis with x
4. Terminate the proof by cases (last hypothesis)

6.4 For the theorem in context "pred7"

1. Instantiate x with a in the existential goal
2. Try to figure out how to instantiate x in hypothesis $\forall x \cdot x \in Q \lor x \in R$
3. Terminate the proof by cases