Interactive Proof Tools
Assignment 8

Hans de Nivelle, Patrick Maier

INFORMATIK

http://www.mpi-sb.mpg.de/~nivelle/teaching/intprooftools2003/main.html

The exercises 8.1 and 8.2 belong to our project of formalizing and verifying a propositional resolution calculus in PVS.

Exercise 8.1 Clause ordering.

1. Extend the `multisets` library with a theory defining the multiset extension $\succ_{\text{mul}}$ (see slide 2) of a partial order $\succ$ which is given as a parameter. Formalize the properties of $\succ_{\text{mul}}$: It is a partial order, which extends well-foundedness and totality of $\succ$ to multisets.
   Hint: Proving these properties is tedious; it suffices to formalize them as axioms.

2. Prove the following lemma:[1]

   For all multisets S, T and elements x,
   $$\text{if } x \in T \text{ and } \{x\} \succ_{\text{mul}} S \text{ then } T \succ_{\text{mul}} S \cup (T \setminus \{x\}).$$

   Point out where this lemma will be needed in the completeness proof.

3. Extend the `clauses` library with a theory defining the clause ordering $\succ$ (see slide 3). Prove that $\succ$ is a well-order.
   Hint: Assert the existence of a well-order on the propositional variables by an axiom.

Exercise 8.2 Candidate interpretation.

1. Formalize the ternary relation *a clause C produces a propositional variable A in an interpretation I* (see slide 4) in PVS.

2. Formalizing the inductive definition of $I_X(\Gamma)$ from slide 5 in PVS. and define the *candidate interpretation* $I(\Gamma)$.

3. Prove the following monotonicity lemma for all sets X and Y such that $I_X(\Gamma)$ and $I_Y(\Gamma)$ are defined:

   $$\text{If } X \subseteq Y \text{ and } I_X(\Gamma) \models C \text{ then } I_Y(\Gamma) \models C.$$

   Point out where this lemma will be needed in the completeness proof.

[1] The former statement $\forall R, S, T : R \succ_{\text{mul}} S \wedge R \succ_{\text{mul}} T \Rightarrow R \succ_{\text{mul}} S \cup T$ is wrong.

Exercise 8.3 Proof terms and proof normalization via the Curry-Howard correspondence.

1. Construct the proof terms for the two proofs of $\varphi \vdash \varphi \to \psi \to \psi$ from slide 22.

2. β-reduce the longer proof term into the shorter one. Is the shorter proof term in β-normal form? Why?

Exercise 8.4 Natural deduction proofs via the Curry-Howard correspondence.
Convert the type derivation trees of the combinator terms I, K, K* and S (see exercise 7.4) into natural deduction proofs of the combinators.

Exercise 8.5 Proof terms for minimal logic with conjunction and disjunction.
Construct proof terms (i. e., inhabitants) for the following formulas:

1. $A \wedge B \to B \wedge A$.

2. $A \vee B \to B \vee A$.

3. $A \wedge (B \wedge C) \to (A \wedge B) \wedge C$.

4. $(A \wedge B) \wedge C \to A \wedge (B \wedge C)$.

5. $A \vee (B \vee C) \to (A \vee B) \vee C$.

6. $A \vee (B \wedge C) \to (A \vee B) \wedge (A \vee C)$.

7. $(A \wedge B) \vee (A \wedge C) \to A \wedge (B \vee C)$.

Challenge: Construct an inhabitant of 4 using (repeated) proofs of 3 and 1. Normalize.