Interactive Proof Tools
Assignment 7

Hans de Nivelle, Patrick Maier

INFORMATIK

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

The exercises 7.1 and 7.2 belong to our project of formalizing and verifying a propositional resolution calculus in PVS.

Exercise 7.1 From formulas to sets of clauses:

1. Formalize propositional formulas (constructed from propositional variables, negation, conjunction, disjunction, implication and equivalence), and define the predicates `true?`, `satisfiable?` and `valid?` for formulas.
   Hint: Define formulas as an abstract datatype.

2. Define an equivalence transformation from formulas to finite sets of clauses, i. e., a transformation that converts a propositional formula φ into an equivalent finite set of clauses Γ. Prove, for all interpretations I, that $I \models \varphi$ iff $I \models \Gamma$.
   Hints:
   - Implement the 3 transformations from slide 4 (in the right order).
   - For each transformation, formalize its range (and the domain of the next transformation) as predicate subtype of the type of formulas.
   - For each transformation, define the transformation as a recursive function and establish that the transformation preserves truth. Note that termination of the recursion may be rather tricky for the transformation from NNF to CNF.
   - Transform a CNF formula to a finite set of clauses and prove that this transformation preserves truth.
   - Compose all 4 transformations.

Exercise 7.2 The resolution calculus Res:

1. Formalize the inferences rules **Resolution** and **Factoring**.
   Hint: An inference rule with n premises can be viewed as an $n+1$-ary relation.

2. For all (not necessarily finite) clause sets Γ, define the sets $\mathrm{Res}(\Gamma)$ and $\mathrm{Res}^*(\Gamma)$.
   Hint: Use an inductive definition for $\mathrm{Res}^*(\Gamma)$.

3. Prove the soundness of Res.

Exercise 7.3 Show (on paper) that $\mathrm{Res}^*(\Gamma)$ need not be finite for finite clause sets Γ.[1]
Hint: It suffices to consider a satisfiable Γ containing 2 clauses only.

Exercise 7.4 Formally check (on paper) the types of the combinator terms I, K, K^* and S (see slide 18) by building their type derivation trees.

[1]Contrary to what I told you in the lecture.