



J. Hoenicke
J. Christ

15.01.2013

Hand in solutions via email to
christj@informatik.uni-freiburg.de
until 22.01.2013 (only Java sources and
PDFs accepted).

Paper submissions possible after the lecture.

Tutorials for “Formal methods for Java” Exercise sheet 10

Exercise 1: Jahob Integrated Proof Language

Consider the following class:¹

```
class Ex11 {  
    /*:  
        public ghost specvar P :: "obj => bool";  
        public ghost specvar Q :: "obj => bool";  
    */  
  
    public static void test()  
    /*:  
        requires "ALL x. P x --> Q x"  
        ensures "ALL u v. P u & v=u --> Q v"  
    */  
    {  
        {  
            /*: pickAny u::obj, v::obj suchThat cond: "P u & v=u";  
            /*: noteThat p1: "P v" from cond;  
            /*: noteThat p2: "Q v" from Precondition forSuch u, v;  
        }  
    }  
}
```

- Which formula does this class try to prove?
- Explain why the proof does not succeed.
- Fix the proof.

¹This is a slightly modified version of a test class that comes with the Jahob distribution.

Exercise 2: Logical operators

From the logical operators **false**, \rightarrow and \forall , all other logical operators are definable. For example $\neg F$ can be defined as $\neg F := F \rightarrow \mathbf{false}$. Find formulas defining

- (a) $\neg F$
- (b) **true**,
- (c) $F \vee G$
- (d) $F \wedge G$
- (e) $\exists x F$

in terms of **false**, \rightarrow and \forall . Prove the validity of these definitions in sequent calculus, e.g. $\neg F \implies F \rightarrow \mathbf{false}$ and $F \rightarrow \mathbf{false} \implies \neg F$.