Exercises 2: JML and FOL

TECHNISCHE
UNIVERSITÄT
DARMSTADT

The solutions to the exercises will be discussed on Monday, 4th May.

Problem 1 JML

Below you see the declarations for a Queue datatype. Specify the class and its operations using JML. The methods dequeue and enqueue shall throw an IndexOutOfBoundsException when removing an element from an empty queue or adding an element to a full queue respectively.

```
public class Queue {

    private Object[] arr;
    private int size;
    private int first;
    private int next;

    Queue( int max ) {
        // ...
    }

    public int size() {
        // ...
    }

    public void enqueue( Object x ) {
        // ...
    }

    public Object dequeue() {
        // ...
    }
}
```

Solution: See file `Queue.java`

Problem 2 FOL Formalisation

All members of the club of barbers adhere to the following rules:

1. If a member A shaves a member B (it is of no interest whether A and B are the same person or not) then all members also shave member A.
2. Four of the members are: Guido, Lorenzo, Petrucio and Cesare.
3. Guido shaves Cesare.

Show that then then the following statement is true:

4. Petrucio shaves Lorenzo

a) Formalise the items 1.-4. in first-order logic (choose suitable types, predicate and function symbols)

b) Prove using the sequent calculus that from 1.-3. the item 4. follows.

Solution (sketch):
a)

1. $\forall x, y((m(x) \land m(y) \land r(x,y)) \to \forall z(m(z) \to r(z,x)))$
2. $m(g) \land m(l) \land m(p) \land m(c)$
3. $r(g,c)$
4. $r(p,l)$

Some remarks:

- Try to use a type member instead of the predicate. (see file `barbersTypes.key`)
- According to our formalisation: Can g, c, p, l (Guido, Cesare et al.) be the same person? Why does it matter or does it not matter?

b)
To prove: $\Longrightarrow 1. \land 2. \land 3. \to 4.$ see files: `barbers.key` and `barbers.proof`

Problem 3 Soundness of the Calculus Rules

Prove the correctness of the rules: impRight and the rule for eliminating the existential quantifier on the right side (exRight).

Reminder: A rule is sound if from the validity of its premises the validity of their conclusion follows.
Solution (sketch):

$$\frac{\Gamma, \phi \Longrightarrow \psi, \Delta}{\Gamma \Longrightarrow \phi \to \psi, \Delta}$$

Proof. (outline) We have to show that from the validity of its premise the validity of the conclusions follows.

Let $S = (D, \delta, I)$ be an arbitrary first-order state and β an arbitrary variable assignment: We have to show that

$$val_{S,\beta}(\Gamma \Longrightarrow \phi \to \psi, \Delta) = \mathit{tt}$$

If $val_{S,\beta}(\Gamma) = \mathit{ff}$ or $val_{S,\beta}(\Gamma) = \mathit{ff}$ we are obviously done. Let's assume that neither of both cases hold, i.e., we have to show $val_{S,\beta}(\phi \to \psi) = \mathit{tt}$ from the validity of the premise we now that either $val_{S,\beta}(\phi) = \mathit{ff}$ or $val_{S,\beta}(\psi) = \mathit{tt}$. In both cases $val_{S,\beta}(\Gamma \Longrightarrow \phi \to \psi, \Delta) = \mathit{tt}$ follows directly from the definition of val for the implication. □

$$\frac{\Gamma \Longrightarrow [x/t']\phi,\ \exists \tau\, x;\ \phi, \Delta}{\Gamma \Longrightarrow \exists T\, x;\ \phi, \Delta} \ (t' \text{ is a variable-free term of compatible type})$$

Proof. (outline) The only interesting case is: Let $val_{S,\beta}([x/t']\phi) = \mathit{tt}$ for first-order states S, we show that then $val_{S,\beta}(\exists \tau\, x;\ \phi) = \mathit{tt}$.

$val_{S,\beta}(\exists \tau\, x;\ \phi) = \mathit{tt}$ iff. $val_{S,\beta_x^d}(\phi) = \mathit{tt}$ for at least one $d \in D^\tau$. Choose $d = val_{S,\beta_x^d}(t')$ (not t' is variable-free, i.e., does not depend on β). Then the validity follows directly from our assumption.

□

Problem 4 FOL Calculus: Application

Prove the following formula using the sequent calculus as presented in the lecture using pen-and-paper. (The type for bound variables is omitted for readability, assume the type $\top$).

a)

$$\Longrightarrow \big((\forall x; (q(x) \to p(x, f(x)))) \land (\forall x; (\neg p(x, f(x)) \lor p(f(x), x)))\big) \to (\forall x; (q(x) \to \exists y; p(y, x)))$$

b)

$$\Longrightarrow (\forall\ x; p(x))\ \to\ ((\forall\ x; \neg q(x)) \lor \exists\ x; (p(x) \land q(x)))$$

Redo your pen-and-paper proofs using the KeY theorem prover using manual steps only (KeYinput files: `folA.key` and `folB.key`).

Try now to use KeY's automatic proof search (clicking the green arrow button). KeYshould be able to close both problems automatically (check in the `Proof Search Strategy Tab` the following options are set: `Proof Splitting`—`Delayed`, `Arithmetic Treatment`—`DefOps`, `Quantifier Treatment`—`No Splits with Progs`).

Which other rules (not on the lecture slides) did KeY use? Can you explain them? Hint: When selecting an inner node, check the box below the proof tree to see more information about the applied rule.

Solution: See files `folA/B.proof`. Follow up questions as discussed in exercise session.