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() {
        // ...
    }
}
```

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.

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.

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)

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

b)

$$\Rightarrow (\forall\ x; p(x)) \ \rightarrow\ ((\forall\ x; \neg q(x)) \lor \exists\ x; (p(x) \land q(x)))$$

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

Try now to use KeY's automatic proof search (clicking the green arrow button). KeY should 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.