Prof. Dr. A. Poetzsch-Heffter
Mathias Weber, M.Sc.

University of Kaiserslautern
Department of Computer Science
Software Technology Group

Advanced Aspects of Object-Oriented Programming (SS 2013)

Practice Sheet 8 (Hints and Comments)

Exercise 1 Assertions for JML using Method Calls

a)
```
public class C {
  private int f = 0;

  public void m(O o) {
    assert f >= 0 : "invariant";
    f++;

    assert f >= 0 : "invariant";
    o.notify();
    assert f >= 0 : "invariant";

    f--;
    assert f >= 0 : "invariant";
  }
```

b) The invariant also has to hold when leaving method m. This is also the case when calling o.notify(). Therefore the invariant has to be checked before the call to o.notify() after incrementing. If the invariant would be `f == 0` the check would not be successfull.

Exercise 2 Abstraction

a) Model fields form a model state, which can be different from the implemented state. The model state may be better suited for specifying the behavior of an object, because it can be more abstract than the real state. For interfaces this is the only possibility to express something about the state of the objects that implement the interfaces. The model fields (model state) has to be related by the specification to the real state.

b)
```
//@ model import org.jmlspecs.models.*;

public interface Queue {
  // FIFO Datastructure, extract at front, insert at the end

  //@ public model JMLObjectSequence elements;
  //@ initially elements != null && elements.isEmpty()

  /*@
    @ public normal_behavior
    @   requires !isEmpty();
    @   ensures \result == elements.first();
    @
    @ also
    @
    @ public exceptional_behavior
    @   requires isEmpty();
    @   signals(EmptyQueueException);
    @*/
  /*@ pure @*/ Object peek() throws EmptyQueueException;

  /*@
    @ public normal_behavior
    @   requires !isEmpty();
    @   assignable elements;
    @   ensures elements.equals(\old(elements).removeItemAt(0)) &&
    @           \result == \old(peek()) &&
    @           size()==\old(size())-1;
    @
    @ also
    @
    @ public exceptional_behavior
    @   requires isEmpty();
    @   assignable \nothing;
```

```
    @   signals(EmptyQueueException);
    @*/
  Object dequeue() throws EmptyQueueException;

  /*@   requires item != null;
    @   assignable elements;
    @   ensures elements.equals(\old(elements).insertBack(item)) &&
    @           size()==\old(size())+1;
    @*/
  void enqueue(Object item);

  /*@
    @   ensures \result==elements.isEmpty();
    @*/
  /*@ pure @*/ boolean isEmpty();

  /*@
    @   ensures \result==elements.size();
    @*/
  /*@ pure @*/ int size();
}

class EmptyQueueException extends Exception {}
```

c) The method implementation are straightforward, mainly delegate the calls to `e`. To relate specification and implementation use depends- and represents-clauses.

```
public abstract class Queue {

  private LinkedList<Object> e = new LinkedList<Object>();
  //@ private depends elements <- e
  //@ private represents elements <- JMLObjectSequence.convertFrom(e)

  //@ public model JMLObjectSequence elements;
  ...
}
```

d) Interfaces can not have fields in Java. This is the reason why model fields can not directly be modeled as fields in all cases. Each implementation (class) would have to implement the model field and its representation as a field. The representation gives the expression that has to be executed whenever a component of the representation is changed.

Exercise 3 Behavioral Subtyping I

a) JML specifications are inherited by subclasses and classes implementing interfaces. A class inherits the visible invariants of its superclasses (-interfaces). See JML Reference Manual 8.2.4

b) *The also keyword indicates that the current specification is refining the specification inherited either from the superclass or from the previous declaration of the method in a refinement sequence. Therefore, it is an error if the specification of a non-refining method begins with also (unless it overrides an inherited method).* JML Reference Manual 16.4

c) Use the rules to construct the pre- and postconditions for subclasses.

```
public class Child extends Parent {
    //@ requires    i >= 0 || i <= 0
    //@ ensures     (\old(i>=0) => \result >= i)
                 && (\old(i<=0) => \result <= i);
    int m(int i){ ... }
}
```

A call to Child.m with `i = 0`, means that both parts of the precondition are fulfilled and therefor both parts of the postcondition have to be fulfilled too. As i is not assignable, pre- and post-values of i are the same and we get as only possible result 0.

d)
- Class A + Class B: ok
- Class C + Class D: No behavioural subtyping. The complete precondition of D.set() is `a > 0 || a > 10`, and the complete postcondition of D.get() is `(true => result > 10) && (true => result > 0)`.

```
D d = new D();
d. set (5); // ok
... d.get();    // not ok, because of the conjunction.
```

The invariant changes nothing.

- Class E + Class F: No behavioural subtyping, due to a possible overflow in F.increment(). The overflow breaks the part of the postcondition, that is inherited from E.increment().

Exercise 4 Behavioral Subtyping II

Works analogously to the Reader example of the lecture.