Workshop Testing and Formal Methods, Week 2

```haskell
> module Workshop2 where
> import Data.List

> infix 1 -->

> (-->) :: Bool -> Bool -> Bool
> p --> q = (not p) || q

> forall = flip all
```

This workshop is about understanding fundamental concepts in formal specifications. The focus is on pre- and postcondition specifications.

1.

A sudoku is a 9×9 matrix of numbers in $\{1, \ldots, 9\}$, possibly including blanks, satisfying certain constraints. A sudoku problem is a sudoku containing blanks, but otherwise satisfying the sudoku constraints. The sudoku solver transforms the problem into a solution.

Note: Here you should make sure to explain what you consider a correct sudoku problem: do you assume correctness means it has at least one solution, or do you assume that the corresponding matrix complies to the uniqueness rules?

Give a Hoare triple for a sudoku solver. If the solver is called P, the Hoare triple consists of

$$\{ \text{ precondition } \} \text{ P } \{ \text{ postcondition } \}$$

The **precondition** of the sudoku solver is that the input is a correct sudoku problem.

The **postcondition** of the sudoku solver is that the transformed input is a solution to the initial problem.

State the pre- and postconditions as clearly and formally as possible.

2.

Suppose $\{p\}\ f\ \{q\}$ holds for some function $f : a \to a$ and a pair of properties p and q.

Recall the meaning of $\{p\}\ f\ \{q\}$:

For every possible argument x for f it is the case that if x has property p then $f(x)$ has property q.

- If p' is stronger that p, does it follow that $\{p'\}\ f\ \{q\}$ still holds?
- If p' is weaker that p, does it follow that $\{p'\}\ f\ \{q\}$ still holds?
- If q' is stronger that q, does it follow that $\{p\}\ f\ \{q'\}$ still holds?
- If q' is weaker that q, does it follow that $\{p\}\ f\ \{q'\}$ still holds?

3.

Which of the following properties is stronger, left side or right side? assume domain [1..10]

- `(\ x -> even x && x > 3) or even`
- `(\ x -> even x || x > 3) or even`
- `(\ x -> (even x && x > 3) || even x) or even`
- `even or  (\ x -> (even x && x > 3) || even x)`

4.

Which of the following properties is stronger?

- $\lambda x \mapsto x = 0$ and $\lambda x \mapsto x \geq 0$
- $\lambda x \mapsto x \neq 0$ and $\lambda x \mapsto x > 3$
- $\lambda x \mapsto x \neq 0$ and $\lambda x \mapsto x < 3$
- $\lambda x \mapsto x^3 + 7x^2 \geq 3$ and $\lambda x \mapsto \bot$
- $\lambda x \mapsto x \geq 2 \lor x \leq 3$ and $\lambda x \mapsto x \geq 2$
- $\lambda x \mapsto x \geq 2 \land x \leq 3$ and $\lambda x \mapsto x \geq 2$

5.

Implement all properties from the previous question as Haskell functions of type `Int -> Bool`. **Note**: this is a pen and paper exercise: just write out the definitions. Using code, you can check your answers to the previous exercise, on some small domain like $[(-10)..10]$.

Weakest precondition

Now that we know what weaker and stronger mean, we can talk about the weakest property p for which

$$\{p\}\ f\ \{q\}$$

holds, for a given function f and a given postcondition property q.

Example: the weakest p for which

$$\{p\}\lambda x \mapsto 2 * x + 4 \ \ \{\lambda x \mapsto 0 \le x < 8\}$$

holds is $\lambda x \mapsto -2 \le x < 2$.

Note: To find the weakest p, we need to find the input domain for f such that the output domain for f is given by $\lambda x \mapsto 0 \le x < 8$. The recipe for finding out when that is the case is as follows.

Use the function $\lambda x \mapsto 2 * x + 4$ as a substitution: substitute the right-hand side $2 * x + 4$ for x in the postcondition q to get the weakest precondition, and simplify.

6.

Work out the weakest preconditions for the following triples. You may assume that the variables range over integers.

- $\{\cdots\}\ \lambda x \mapsto x{+}1\ \{\,\lambda x \mapsto 2x - 1 = A\,\}$
- $\{\cdots\}\ \lambda x \mapsto x * x + 1\ \{\,\lambda x \mapsto x = 10\,\}$
- $\{\cdots\}\ \lambda x \mapsto x{+}y\ \{\,\lambda x \mapsto x{-}y = 7\,\}$
- $\{\cdots\}\ \lambda x \mapsto x{+}y\ \{\,\lambda x \mapsto x \ge y\,\}$
- $\{\cdots\}\ \lambda x \mapsto -x\ \{\,\lambda x \mapsto x \ge 0\,\}$

7.

Show the following (again, you may assume that the variables range over integers):

- $\{\,\lambda n \mapsto x = n^2\,\}\ \lambda n \mapsto n{+}1\ \{\,\lambda n \mapsto x = (n{-}1)^2\,\}$
- $\{\,\lambda x \mapsto A = x\,\}\ \lambda x \mapsto x{+}1\ \{\,\lambda x \mapsto A = x{-}1\,\}$
- $\{\,\lambda x \mapsto x \ge 0\,\}\ \lambda x \mapsto x{+}y\ \{\,\lambda x \mapsto x \ge y\,\}$

- $\{\, \lambda x \mapsto 0 \le x < 100 \,\}\ \lambda x \mapsto x{+}1\ \{\, \lambda x \mapsto 0 \le x \le 100 \,\}$
- $\{\, \lambda n \mapsto x = (n{+}1)^2 \wedge n = A \,\}\ \lambda n \mapsto n{+}1\ \{\, \lambda n \mapsto x = n^2 \wedge n = A{+}1 \,\}$

Strongest postcondition

How would you find the strongest postcondition q for which

$$\{p\}\ f\ \{q\}$$

holds, for a given function f and a given precondition property p?

8.

For each triple in Exercise 7 find the strongest postconditions.
