Probabilistic Programming (WS16/17)
Prof. Dr. Ir. Joost-Pieter Katoen
Christoph Matheja Dr. Federico Olmedo

Lehrstuhl für Informatik 2 Softwaremodellierung und Verifikation | RWTH AACHEN UNIVERSITY

Exercise Sheet 2

General remarks:

- **Due date:** December 16$^{\text{th}}$ (before the exercise class).
- Solutions must be written in English.
- While we *might* publish sketches of exercise solutions, we do *not* guarantee that these sketches contain all details that are necessary to properly solve an exercise. Hence, it is recommended to attend the exercise classes.
- If you have any questions regarding the lecture or the exercise, feel free to write us an email or visit us at the chair.

Exercise 1 (Properties of Weakest Preconditions) — 35%

Let c be a GCL program and f, g be predicates.

(a) [10%] Show that $\mathsf{wp}[c](0) = 0$.

(b) [15%] Show that $f \Rightarrow g$ implies $\mathsf{wp}[c](f) \Rightarrow \mathsf{wp}[c](g)$.

(c) [10%] Does $\mathsf{wp}[c](f) \vee \mathsf{wp}[c](g)$ imply $\mathsf{wp}[c](f \vee g)$? If yes, why? If not, find special cases for which this law holds.

Exercise 2 (Calculation of Weakest Pre–conditions) — 20%

Consider the program c given by

$$x := X \,;\, z := 0 \,;\, \mathsf{while}\,(y \leq x)\,\{z := z + 1 \,;\, x := x - y\}.$$

with respect to postcondition $z = X \operatorname{div} y$, where div denotes integer division.

(a) [10%] Provide an invariant I for the loop of c w.r.t. postcondition $z = X \operatorname{div} y$.

(b) [10%] Prove that your proposed invariant is correct.

Exercise 3 (Alternative Semantic Characterization for Loops) — 24%

Recall that

$$\mathsf{wp}[\mathsf{while}\,(G)\,\{c\}](f) \;=\; \boldsymbol{\mu} F \;=\; \sup_n F^n(\mathbf{0})\ ,$$

where F is the expectation transformer $X \mapsto [G] \cdot \mathsf{wp}[c](X) + [\neg G] \cdot f$ and F^n denotes the composition of F with itself n times, i.e. $F^0 = id$ and $F^{n+1} = F \circ F^n$.

Prove by induction on n that

$$\forall n.\ F^n(\mathbf{0}) \;=\; \mathsf{wp}[\mathsf{while}_n\,(G)\,\{c\}](f)\ ,$$

where $\mathsf{while}_n\,(G)\,\{c\}$ represents the n^{th}*–unrolling* of the loop given by

$$\begin{aligned} \mathsf{while}_0\,(G)\,\{c\} &= \mathsf{abort} \\ \mathsf{while}_{n+1}\,(G)\,\{c\} &= \mathsf{ite}\,(G)\,\{c;\, \mathsf{while}_n\,(G)\,\{c\}\}\,\{\mathsf{skip}\}\ . \end{aligned}$$

Exercise 4 (Program Specifications) — 21%

UPDATE 13.12.2016: Since the weakest liberal precondition (wlp) calculus has not been introduced in the lecture yet, you can ignore part (a), (d), and (e) of task 4.

Match each of the following formal specifications of program c

(a) [3%] $[P] = \mathsf{wlp}[c](\mathbf{1})$
(b) [3%] $[P] = \mathsf{wp}[c](\mathbf{1})$
(c) [3%] $[P] \leq \mathsf{wp}[c](\mathbf{1})$
(d) [3%] $\mathbf{1} = \mathsf{wlp}[c](\mathbf{0})$
(e) [3%] $\mathbf{1} \leq \mathsf{wlp}[c](\mathbf{0})$
(f) [3%] $\mathbf{1} = \mathsf{wp}[c](\mathbf{0})$
(g) [3%] $\mathbf{0} \leq \mathsf{wp}[c]([Q])$

with their corresponding colloquial description from 1–7. (There may be more than one formal specification in (a)-(g) with the same colloquial description in 1–7. There may also be "unmatched" colloquial interpretations.)

1. Program c diverges almost surely for all initial states.
2. The program never finishes in a final state satisfying Q.
3. The specification does not say anything about program c; it is logically equivalent to true.
4. The specification is logically equivalent to false.
5. None of the above. Provide yourself the interpretation of the specification.
6. Program c terminates almost surely whenever executed in an initial state that satisfies P.
7. Program c terminates almost surely when executed in an initial state that satisfies P and diverges almost surely when executed in an initial state that satisfies $\neg P$.