Exercise Sheet 5

General remarks:

- **Due date:** November 25th 12:30 (before the exercise class).
- Please submit your solutions via MOODLE. Remember to provide your matriculation number. It is necessary to hand in your solutions in groups of **three**. You may use the MOODLE forum to form groups.
- Solutions must be written in English.
- While we will 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, please use the forum in MOODLE.

Exercise 1 (Weakest pre-expectation calculus) $\boxed{\textbf{25P}}$

(a) [5P] Determine $wp(P,\, x^2)$ for program $P\colon \{\ x := 2\ \}\ [1/3]\ \{\ \texttt{diverge}\ \}$.

Solution:

$$
\begin{aligned}
& wp(P,\, x^2) \\
= \;& wp(\{\, x := 2\, [1/3]\, \texttt{diverge}\, \}, x^2) \\
= \;& 1/3 \cdot wp(x := 2,\, x^2) + 2/3 \cdot wp(\texttt{diverge},\, x^2) \\
= \;& 1/3 \cdot 4 + 2/3 \cdot 0 \\
= \;& 4/3.
\end{aligned}
$$

(b) [10P] In the present and the next exercise part, prove or disprove whether the programs P_1 and P_2 are equivalent w.r.t. the post-expectation $f = x$:

$P_1\colon \quad y := 5;\ \texttt{if}\ (y < 0)\ \{\ \texttt{skip}\ \}\ \texttt{else}\ \{\ \{\ x := 1\ \}\ [1/2]\ \{\ \texttt{skip}\ \}\ \}$

$P_2\colon \quad \{\ \{\ x := x + 3\ \}\ [1/3]\ \{\ x := x\ \}\ \}\ [1/2]\ \{\ x := 0\ \}$

Solution:

$$
\begin{aligned}
& k(x) = wp(x := 1\,[1/2]\,\texttt{skip},\, x) \\
=\ & 1/2 \cdot wp(x := 1,\, x) + 1/2 \cdot wp(\texttt{skip},\, x) \\
=\ & 1/2 \cdot x[x := 1] + 1/2 \cdot x \\
=\ & 1/2 \cdot (1 + x)
\end{aligned}
$$

$$
\begin{aligned}
& g(x) = wp(\{\texttt{if}(\, y < 0\,)\{\,\texttt{skip}\,\}\texttt{else}\,\{\, x := 1\,[1/2]\,\texttt{skip}\}\,\},\, x) \\
=\ & [y < 0] \cdot wp(\texttt{skip},\, x) + [y \geq 0] \cdot wp(x := 1\,[1/2]\,\texttt{skip},\, x) \\
=\ & [y < 0] \cdot x \ + \ [y \geq 0] \ \cdot k(x) \\
=\ & [y < 0] \cdot x + [y \geq 0] 1/2 \cdot (1 + x)
\end{aligned}
$$

$$
\begin{aligned}
& wp(P_1,\, x) \\
=\ & wp(y := 5, wp(\texttt{if}(y < 0)\{\,\texttt{skip}\,\}\texttt{else}\,\{\, x := 1\,[1/2]\,\texttt{skip}\,\},\, x)) \\
=\ & wp(y := 5, g(x)) \\
=\ & ([y < 0] \cdot x + [y \geq 0] \cdot 1/2 \cdot (1 + x))\,[y := 5] \\
=\ & [5 < 0] \cdot x + [5 > 0] \cdot 1/2(1 + x) \\
=\ & 1/2 \cdot (1 + x)
\end{aligned}
$$

$$
\begin{aligned}
& wp(P_2,\, x) \\
=\ & wp(\{\, x := x + 3\,[1/3]\, x := x\,\}\,[1/2]\,\{x := 0\},\, x) \\
=\ & 1/2 \cdot (\,wp(x := x + 3\,[1/3]\, x := x\},\, x)) + 1/2 \cdot wp(x := 0,\, x) \\
=\ & 1/2 \cdot (1/3 \cdot wp(x := x + 3,\, x) + 2/3 \cdot wp(x := x,\, x)) + 1/2 \cdot 0 \\
=\ & 1/2 \cdot (1/3 \cdot (x + 3) + 2/3 \cdot x) + 0 \\
=\ & 1/2 \cdot (x + 1)
\end{aligned}
$$

We observed that $wp(P_1,\, x) = wp(P_2,\, x) = 1/2 \cdot (\,x + 1\,)$. Therefore P_1 and P_2 are equivalent w.r.t. $f = x$.

(c) [10P]

P_1: $\texttt{while}\ (x \neq x)\ \{\ \{\ x := y + 1\ \}\ [1/2]\ \{\ x := y - 1\ \}\ \}$

P_2: $\texttt{while}\ (\mathit{true})\ \{\ \texttt{skip}\ \}$

Solution:

$$
\begin{aligned}
& wp(P_1, x) \\
= \;& wp(\texttt{while}(x \neq x)\{\, x := y+1\,[\nicefrac{1}{2}]\, x := y-1 \,\},\, x) \\
= \;& \mathrm{lfp}X.\,(([x \neq x] \cdot wp(x := y+1\,[\nicefrac{1}{2}]\, x := y-1, X)) + ([x = x] \cdot x)) \\
& \Phi(X) = (([x \neq x] \cdot wp(x := y+1\,[\nicefrac{1}{2}]\, x := y-1, X)) + ([x = x] \cdot x)) \\
= \;& 0 \cdot wp(x := y+1\,[\nicefrac{1}{2}]\, x := y-1,\, X) + 1 \cdot x \\
= \;& x \\
& \Phi^0(0) = x, \quad \Phi^1(0) = x, \cdots, \Phi^n(0) = x \\
& wp(P_1,\, x) = \mathrm{lfp}X.\Phi(X) = x
\end{aligned}
$$

$$
\begin{aligned}
& wp(P_2, x) \\
= \;& wp(\texttt{while}(\texttt{true})\{\, \texttt{skip} \,\},\, x) \\
= \;& \mathrm{lfp}X.\,([\texttt{true}] \cdot wp(\,\texttt{skip},\, X) + [\,\texttt{false}\,] \cdot x) \\
& \Phi(X) = ([\texttt{true}] \cdot wp(\,\texttt{skip}\,,\, X) + [\texttt{false}] \cdot x) \\
= \;& 1 \cdot X + 0 \cdot x = X \\
& \Phi^0(0) = 0, \Phi^1(0) = 0, \cdots, \Phi^n(0) = 0 \\
& wp(P_2,\, x) = \mathrm{lfp}X.\Phi(X) = 0
\end{aligned}
$$

We observed that $wp(P_1,\, x) \neq wp(P_2,\, x)$. Therefore P_1 and P_2 are not equivalent w.r.t the post-condition x.

Exercise 2 (Continuity of weakest pre-expectations) $\boxed{\textbf{25P}}$

Fix a pGCL loop $P = \texttt{while}\ (G)\ \{\ P'\ \}$. For all expectations $X, f \in \mathbb{E}$ we define

$$\Phi_{P,f}(X) = [G] \cdot wp(P', X) + [\neg G] \cdot f\ .$$

(a) [5P] Fix expectation $X \in \mathbb{E}$. Prove that $\Phi_{P,f}(X)$ is continuous *as a function in* f.
Hint: You can use without proof that the functions $\mu_g, \alpha_g \colon \mathbb{E} \to \mathbb{E}$ where $\mu_g(f) = g \cdot f$ and $\alpha_g(f) = g + f$ are continuous for all $g \in \mathbb{E}$.

Solution: Let $S \subseteq \mathbb{E}$ be a chain. We have to show that

$$\bigsqcup_{f \in S} \Phi_{P,f}(X) = \Phi_{P,\bigsqcup S}(X)\ .$$

We have

$$\begin{aligned}
\bigsqcup_{f\in S} \Phi_{P,f}(X) &= \bigsqcup_{f\in S} ([G]\cdot wp(P',X) + [\neg G]\cdot f) \\
&= [G]\cdot wp(P',X) + \bigsqcup_{f\in S} [\neg G]\cdot f \qquad \text{(because } \alpha_{[G]\cdot wp(P',X)} \text{ is continous)} \\
&= [G]\cdot wp(P',X) + [\neg G] \bigsqcup_{f\in S} \cdot f \ , \qquad \text{(because } \mu_{[\neg G]} \text{ is continous)} \\
&= \Phi_{P,\bigsqcup S}(X) \ .
\end{aligned}$$

We remark that this implies that $\Phi^n_{P,f}(X)$ is also continuous for all $n \in \mathbb{N}$ (this property is needed in part (b)). Formally and more generally, let φ be continuous on a complete lattice and let S be a chain. Then by monotonicity of φ, the set $\{\varphi^n(s) \mid s \in S\}$ is also a chain for all $n \in \mathbb{N}$. By induction on $n \in \mathbb{N}$,

$$\bigsqcup_{s\in S} \varphi^{n+1}(s) = \bigsqcup_{s\in S} \varphi(\varphi^n(s)) \overset{cont.}{=} \varphi\left(\bigsqcup_{s\in S} \varphi^n(s)\right) \overset{I.H.}{=} \varphi^{n+1}\left(\bigsqcup_{s\in S} s\right) \ .$$

(b) [20P] This time fix an arbitrary post-expectation f. Prove that $\Phi_{P,f}$ is continuous *as a function in X*.
Hint: We want you to focus on loops in this exercise. Therefore you can use all of the following without proof:

- For $P = \texttt{skip}$, $P = \texttt{diverge}$, $P = x := E$ it holds that $wp(P, f)$ is continuous.
- If P_1, P_2 are such that $wp(P_1, f)$ and $wp(P_2, f)$ are continuous, then $wp(P, f)$ is continuous for $P = P_1; P_2$, $P = \texttt{if}\ (H)\ \{\ P_1\ \}\ \texttt{else}\ \{\ P_2\ \}$ and $P = \{\ P_1\ \}\ [p]\ \{\ P_2\ \}$ for all guards H and probabilities $p \in [0, 1]$.

Solution: Let $S \subseteq \mathbb{E}$ be a chain. We have to show that

$$\bigsqcup_{X\in S} \Phi_{P,f}(X) = \Phi_{P,f}(\bigsqcup S) \ .$$

We have

$$\begin{aligned}
\bigsqcup_{X\in S} \Phi_{P,f}(X) &= \bigsqcup_{X\in S} ([G]\cdot wp(P',X) + [\neg G]\cdot f) \\
&= \bigsqcup_{X\in S} [G]\cdot wp(P',X) + [\neg G]\cdot f \qquad \text{(because } \alpha_{[\neg G]\cdot f} \text{ is continous)} \\
&= [G]\cdot \bigsqcup_{X\in S} wp(P',X) + [\neg G]\cdot f \ , \qquad \text{(because } \mu_{[G]} \text{ is continous)}
\end{aligned}$$

and so it remains to show that $wp(P', \cdot)\colon \mathbb{E} \to \mathbb{E}$ is continuous for general `pGCL` programs P'.

We now show by induction over the structure of P' that $wp(P', \cdot)$ is continuous. All cases of the induction except $P' = \texttt{while}\ (G')\ \{\ P''\ \}$ are already covered by the hint.
We now show that $wp(P', \cdot) = wp(\texttt{while}\ (G')\ \{\ P''\ \}, \cdot)$ is continuous:
First, for all post-expectations g it holds that

$$\Phi_{P',g}(X) = [G'] \cdot wp(P'', X) + [\neg G'] \cdot g$$

is continuous because by the I.H., we may assume that $wp(P'', \cdot)$ is continuous.

$$\begin{aligned}
\bigsqcup_{X \in S} wp(P', X) &= \bigsqcup_{X \in S} \text{lfp } Y.\ \Phi_{P',X}(Y) \\
&= \bigsqcup_{X \in S} \bigsqcup_{n \in \mathbb{N}} \Phi^n_{P',X}(0) && \text{(Kleene; } \Phi_{P',X} \text{ is continuous by I.H.)} \\
&= \bigsqcup_{n \in \mathbb{N}} \bigsqcup_{X \in S} \Phi^n_{P',X}(0) && \text{(suprema commute)} \\
&= \bigsqcup_{n \in \mathbb{N}} \Phi^n_{P',\bigsqcup S}(0) && \text{(part (a))} \\
&= \text{lfp } Y.\ \Phi_{P',\bigsqcup S}(Y) && \text{(Kleene)} \\
&= wp(P', \bigsqcup S)
\end{aligned}$$

This concludes the proof.

Exercise 3 (Reasoning with invariants) $\boxed{\textbf{25P}}$

Let P be a pGCL program, I an expectation, $s \in \mathbb{S}$ a state and x be a program variable. In this exercise, Φ_f (Ψ_f, resp.) denotes the wp(wlp, resp.)-characteristic function of P w.r.t. to a post-expectation f. For each of the colloquial specifications (1) – (5) below do the following: Either select at least one of the formal conditions (a) – (g) such that the specification holds if and only if the condition holds or indicate that no such condition exists!

Colloquial descriptions:

(1) P terminates almost-surely on input s.
(2) P diverges almost-surely on input state s.
(3) If P terminates almost-surely on input s, then expected value of x after termination is at most 1.
(4) P terminates with probability at least $1/2$ on all inputs.
(5) The probability that P on input s terminates in a state with $x = 1$ is zero.

Formal conditions:

(a) $I \sqsubseteq \Phi_x(I)$ and $I(s) = 1$.
(b) $I \sqsubseteq \Psi_1(I)$ and $I \geq 1/2$.
(c) $I \sqsubseteq \Psi_{[x \neq 1]}(I)$ and $I(s) = 1$.
(d) $\Phi_1(I) \sqsubseteq I$ and $I(s) = 0$.

(e) $I \sqsubseteq \Phi_1(I)$ and $I(s) = 1$.
(f) $I \sqsubseteq \Psi_0(I)$ and $I(s) = 1$.
(g) $\Phi_{[x\leq 1]}(I) \sqsubseteq I$ and $I(s) = s(x)$.

Solution: Since the expectation I is arbitrary but *fixed*, none of the "if and only if" relations holds. However, the following implications do hold (and the remaining implications from formal conditions to colloquial specifications are all false):

- (d) $\implies$ (2)
- (f) $\implies$ (2)
- (c) $\implies$ (5)

To see why e.g. (2) $\implies$ (d) does *not* hold consider the following: The fact that P diverges almost-surely on input s does not imply that condition (d) holds for an *arbitrary* I (e.g. it does not hold if $I = 1$). However, the following equivalences are true:

- $\exists I\colon$ (d) $\iff$ (2)
- $\exists I\colon$ (f) $\iff$ (2)
- $\exists I\colon$ (c) $\iff$ (5)

Exercise 4 (A syntax for expectations) **25P**

(a) [5P] Write the (semantic) expectation $f = \sqrt[3]{x}$ as a syntactic expectation in Exp.

Solution:
$$\mathsf{f} = \mathcal{S}y\colon [y \cdot y \cdot y < x] \cdot y$$

(b) [5P] Write the (semantic) expectation $f = \frac{2}{2\cdot x^2+7}$ as a syntactic expectation in Exp.

Solution:
$$\mathsf{f} = \mathcal{S}y\colon [y \cdot (2 \cdot x^2 + 7) < 2] \cdot y$$

(c) [7P] Let a be an arithmetic expression with a free variable x. We write $a(y)$ to mean a where x is substituted by y. Write a syntactic expectation $\mathsf{f} \in \mathsf{Exp}$ that evaluates to 1 if and only if a is constant in x.

Solution: We want to encode the following (semantic) expectation
$$[\forall y\colon \forall z\colon (a(y) \leq a(z))]$$

It evaluates to 1 if and only if for each pair of values y, z for x, a evaluates to the same value. We can see this using a case distinction:

- If a is constant in x, then for all y, z, we have $a(y) \leq a(z)$.
- If a is not constant in y, then there is a pair y, z such that $a(y) \not\leq a(z)$.

We need to encode this into our syntax. The correct result looks like this:

$$\mathsf{f} = \boldsymbol{\ell}\, y\colon \boldsymbol{\ell}\, z\colon [\neg(a(y) < a(z))] \cdot 1 \ .$$

We replaced $\forall$ by suprema and encoded the $\leq$ using $<$ and negation.
Why does the former transformation work? *(The following proof is not required to achieve full points, an informal argument suffices.)*
The crucial idea is that we can use infima to encode $\forall$ quantifiers inside the Iverson brackets. For all $s \in \mathbb{S}$ and Boolean expressions b:

$$(\ [\forall y\colon [\![b]\!]]\ )(s) = [\![\ \boldsymbol{\ell}_y [b]\ ]\!]^s \ .$$

Again, a proof by case distinction. Let $s \in \mathbb{S}$.

- If $[\![b]\!]^{s'}$ is true for all $s' \in \{\, s[y \mapsto r] \mid r \in \mathbb{Q}_{\geq 0} \,\}$, then

  $$[\forall y\colon [\![b]\!]](s) = 1$$

  and

  $$\begin{aligned} [\![\ \boldsymbol{\ell}_y [b]\ ]\!]^s &= \inf \{\, [\![[b]]\!]^{s[y \mapsto r]} \mid r \in \mathbb{Q}_{\geq 0} \,\} \\ &= \inf \{\, 1 \mid r \in \mathbb{Q}_{\geq 0} \,\} \\ &= 1 \end{aligned}$$

- If $[\![b]\!]^{s'}$ is not true for some $s' \in \{\, s[y \mapsto r] \mid r \in \mathbb{Q}_{\geq 0} \,\}$, then

  $$[\forall y\colon [\![b]\!]](s) = 0$$

  and

  $$\begin{aligned} [\![\ \boldsymbol{\ell}_y [b]\ ]\!]^s &= \inf \{\, [\![[b]]\!]^{s[y \mapsto r]} \mid r \in \mathbb{Q}_{\geq 0} \,\} \\ &= \inf \{\, [\![[b]]\!]^{s[y \mapsto r]} \mid r \in \mathbb{Q}_{\geq 0} \,\} \cup \{\, [\![[b]]\!]^{s'} \,\} \\ &= \inf \{\, [\![[b]]\!]^{s[y \mapsto r]} \mid r \in \mathbb{Q}_{\geq 0} \,\} \cup \{\, 0 \,\} \\ &= 0 \end{aligned}$$

(d) [8P] Let a be an arithmetic expression with a free variable x. We write $a(y)$ to mean a where x is substituted by y. Write a syntactic expectation $\mathsf{f} \in \mathsf{Exp}$ that evaluates to 1 if and only if a represents a monotonic function in x.

Solution: Using the operators $\leq$ and $\Rightarrow$, we can encode monotonicity as follows:

$$\mathsf{f}' = \curlywedge x\colon \curlywedge y\colon [(x \leq y) \Rightarrow (f(x) \leq f(y))] \cdot 1 \ .$$

Note that we used the trick from task c) to encode $\forall$ as infima again.
The comparison $(x \leq y)$ can be written as $\neg(y < x)$. The implication $\phi \Rightarrow \psi$ can be written as $\neg(\phi \wedge \neg\psi)$. Thus,

$$\mathsf{f} = \curlywedge x\colon \curlywedge y\colon [\neg(\neg(y < x) \wedge \neg\neg(f(y) < f(x)))] \cdot 1 \quad \in \mathsf{Exp} \ .$$

Eliminating double negations, we get the simplified version:

$$\mathsf{f} \equiv \curlywedge x\colon \curlywedge y\colon [\neg(\neg(y < x) \wedge (f(y) < f(x)))] \cdot 1 \ .$$