

Exercise Sheet 7

General remarks:

- **Due date:** February 10th (before the exercise class). You can either hand your solutions in at the beginning of the exercise class or submit them via email to

`prop1617@i2.informatik.rwth-aachen.de`

- Solutions must be written in English.
- 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 (Computing the expected runtime)

20%

Compute the expected runtime of the following pGCL program c :

```
1 :    {b := true} [1/2] {b := false};
2 :    if (b) {
3 :        s := true
4 :    } else {
5 :        {b := true} [1/2] {b := false};
6 :        ite(b) {s := true} {s := false}
7 :    }
```

Solution: We write c_{ij} to denote the program starting in line i and ending in line j . Further note that we start with continuation $\mathbf{0}$ as we are interested in *the* runtime of c .

$$\begin{aligned}
& \text{ert}[c](\mathbf{0}) \\
&= \text{ert}[c_{11}](\text{ert}[c_{27}](\mathbf{0})) \\
&= \text{ert}[c_{11}](1 + [b] \cdot \text{ert}[s := \text{true}](\mathbf{0}) + [\neg b] \cdot \text{ert}[c_{56}](\mathbf{0})) \\
&= \text{ert}[c_{11}] \left(1 + [b] \cdot (1 + \mathbf{0}) + [\neg b] \cdot \underbrace{\text{ert}[c_{55}](1 + [b] \cdot (1 + \mathbf{0}) + [\neg b] \cdot (1 + \mathbf{0}))}_{=2} \right) \\
&= \text{ert}[c_{11}](1 + [b] + [\neg b] \cdot (1 + 1/2 \cdot \text{ert}[b := \text{true}](\mathbf{2}) + 1/2 \cdot \text{ert}[b := \text{false}](\mathbf{2}))) \\
&= \text{ert}[c_{11}](1 + [b] + [\neg b] \cdot 4) \\
&= 1 + 1/2 \cdot (1 + 1 + [b](b \mapsto \text{true})) + 1/2 \cdot (1 + 1 + [\neg b](b \mapsto \text{false}) \cdot 4) \\
&= 1 + 3/2 + 6/2 = 5 + 1/2
\end{aligned}$$

Exercise 2 (Relation between ert and wp)

30%

Prove that for any runtime $t \in \mathbb{T}$ and pGCL program c ,

$$\text{ert}[c](t) = \text{ert}[c](\mathbf{0}) + \text{wp}[c](t) .$$

Hint. In order to use an inductive argument (on the program structure) it will be necessary to appropriately strengthen the claim.

Solution: We prove by induction on the structure of c that

$$\text{ert}[c](t_1 + t_2) = \text{ert}[c](t_1) + \text{wp}[c](t_2) .$$

By setting $t_1 = \mathbf{0}$ we recover the original claim.

The (base) cases of **skip**, **abort** and assignments are straightforward. For the remaining cases we have:

Conditional Branching:

$$\begin{aligned} & \text{ert}[\text{ite}(G) \{c_1\} \{c_2\}](t_1 + t_2) \\ = & \quad \{\text{def. of ert}\} \\ & \mathbf{1} + [G] \cdot \text{ert}[c_1](t_1 + t_2) + [\neg G] \cdot \text{ert}[c_2](t_1 + t_2) \\ = & \quad \{\text{I.H. on } c_1, c_2\} \\ & \mathbf{1} + [G] \cdot (\text{ert}[c_1](t_1) + \text{wp}[c_1](t_2)) + [\neg G] \cdot (\text{ert}[c_2](t_1) + \text{wp}[c_2](t_2)) \\ = & \quad \{\text{algebra}\} \\ & \mathbf{1} + [G] \cdot \text{ert}[c_1](t_1) + [\neg G] \cdot \text{ert}[c_2](t_1) + [G] \cdot \text{wp}[c_1](t_2) + [\neg G] \cdot \text{wp}[c_2](t_2) \\ = & \quad \{\text{def. of ert, wp}\} \\ & \text{ert}[\text{ite}(G) \{c_1\} \{c_2\}](t_1) + \text{wp}[\text{ite}(G) \{c_1\} \{c_2\}](t_2) \end{aligned}$$

Sequential Composition:

$$\begin{aligned} & \text{ert}[c_1; c_2](t_1 + t_2) \\ = & \quad \{\text{def. of ert}\} \\ & \text{ert}[c_1](\text{ert}[c_2](t_1 + t_2)) \\ = & \quad \{\text{I.H. on } c_2\} \\ & \text{ert}[c_1](\text{ert}[c_2](t_1) + \text{wp}[c_2](t_2)) \\ = & \quad \{\text{I.H. on } c_1\} \\ & \text{ert}[c_1](\text{ert}[c_2](t_1)) + \text{wp}[c_1](\text{wp}[c_2](t_2)) \\ = & \quad \{\text{def. of ert, wp}\} \\ & \text{ert}[c_1; c_2](t_1) + \text{wp}[c_1; c_2](t_2) \end{aligned}$$

Loop We have to prove that

$$\text{ert}[\text{while}(G) \{c\}](t_1 + t_2) = \text{ert}[\text{while}(G) \{c\}](t_1) + \text{wp}[\text{while}(G) \{c\}](t_2) ,$$

which reduces to

$$\lim_{n \rightarrow \infty} F_{t_1+t_2}^n(\mathbf{0}) = \lim_{n \rightarrow \infty} F_{t_1}^n(\mathbf{0}) + \lim_{n \rightarrow \infty} G_{t_2}^n(\mathbf{0}) , \quad (1)$$

where

$$\begin{aligned} F_t(X) & \triangleq \mathbf{1} + [G] \cdot \text{ert}[c](X) + [\neg G] \cdot t \\ G_t(X) & \triangleq [G] \cdot \text{wp}[c](X) + [\neg G] \cdot t \end{aligned}$$

Equation (1) follows from

$$\forall n. F_{t_1+t_2}^n(\mathbf{0}) = F_{t_1}^n(\mathbf{0}) + G_{t_2}^n(\mathbf{0}) ,$$

which we prove by induction on n . The base case $n = 0$ is immediate as it reduces to $\mathbf{0} = \mathbf{0} + \mathbf{0}$. For the inductive case we reason as follows:

$$\begin{aligned}
& F_{t_1+t_2}^{n+1}(\mathbf{0}) \\
= & \quad \{\text{def. of } F_t^{n+1}\} \\
& \mathbf{1} + [G] \cdot \text{ert}[c](F_{t_1+t_2}^n(\mathbf{0})) + [\neg G] \cdot (t_1 + t_2) \\
= & \quad \{\text{I.H. on } n\} \\
& \mathbf{1} + [G] \cdot \text{ert}[c](F_{t_1}^n(\mathbf{0}) + G_{t_2}^n(\mathbf{0})) + [\neg G] \cdot (t_1 + t_2) \\
= & \quad \{\text{I.H. on } c\} \\
& \mathbf{1} + [G] \cdot \left(\text{ert}[c](F_{t_1}^n(\mathbf{0})) + \text{wp}[c](G_{t_2}^n(\mathbf{0})) \right) + [\neg G] \cdot (t_1 + t_2) \\
= & \quad \{\text{algebra}\} \\
& \left(\mathbf{1} + [G] \cdot \text{ert}[c](F_{t_1}^n(\mathbf{0})) + [\neg G] \cdot t_1 \right) + \left([G] \cdot \text{wp}[c](G_{t_2}^n(\mathbf{0})) + [\neg G] \cdot t_2 \right) \\
= & \quad \{\text{def. of } F_t^{n+1}, G_t^{n+1}\} \\
& F_{t_1}^{n+1}(\mathbf{0}) + G_{t_2}^{n+1}(\mathbf{0})
\end{aligned}$$

Exercise 3 (Basic properties of ert)**30%**

Decide whether each of the following statements are true or false, justifying your answer. (For true statements, provide a formal proof). Assume $t, t_1, t_2 \in \mathbb{T}$, $k \in \mathbb{R}^{>0}$ and c is a pGCL program.

1. $\text{ert}[c](k \cdot t) = k \cdot \text{ert}[c](t)$;
2. $\text{ert}[c](t_1 + t_2) = \text{ert}[c](t_1) + \text{ert}[c](t_2)$;
3. $\text{ert}[c](t) \succeq t$.

Solution:

1. False.

$$\underbrace{\text{ert}[x := E](2 \cdot \mathbf{0})}_{= 1} \neq 2 \cdot \underbrace{\text{ert}[x := E](\mathbf{0})}_{= 1}$$

2. False.

$$\underbrace{\text{ert}[c](\mathbf{0} + \mathbf{0})}_{= 1} \neq \underbrace{\text{ert}[c](\mathbf{0})}_{= 1} + \underbrace{\text{ert}[c](\mathbf{0})}_{= 1}$$

3. False

$$\text{ert}[\text{abort}](\mathbf{1}) = \mathbf{0} \prec \mathbf{1}$$

Exercise 4 (Calculating runtimes with wp)

20%

Let c be a pGCL program and $t \in \mathbb{T}$ be a runtime. Formally define a program transformation, i.e., a pGCL program c' and an expectation f , such that

$$\text{ert}[c](t) = \text{wp}[c'](f).$$

Explain why your construction is correct (a formal proof is not required).

Solution: Main idea: introduce a fresh variable *counter* that is incremented before executing a statement with a non-zero runtime. Then, after execution of the whole program, the expected value of *counter* corresponds to the expected runtime of *c*. Thus, the runtime *t* is represented by the expectation $f = \text{counter} + t$.

The transformation $\text{trans} : \text{pGCL} \rightarrow \text{pGCL}$ itself is defined inductively as follows:

$$\begin{aligned}
 \text{trans}(\text{abort}) &\triangleq \text{abort} \\
 \text{trans}(\text{skip}) &\triangleq \text{counter} := \text{counter} + 1; \text{skip} \\
 \text{trans}(x := E) &\triangleq \text{counter} := \text{counter} + 1; x := E \\
 \text{trans}(\{c_1\} [p] \{c_2\}) &\triangleq \text{counter} := \text{counter} + 1; \{ \text{trans}(c_1) \} [p] \{ \text{trans}(c_2) \} \\
 \text{trans}(\text{ite}(G) \{c_1\} \{c_2\}) &\triangleq \text{counter} := \text{counter} + 1; \text{ite}(G) \{ \text{trans}(c_1) \} \{ \text{trans}(c_2) \} \\
 \text{trans}(\text{while}(G) \{c_1\}) &\triangleq \text{counter} := \text{counter} + 1; \text{while}(G) \{ \text{trans}(c_1) \}
 \end{aligned}$$

Then $c' \triangleq \text{counter} := 0; \text{trans}(c)$.