The weakest precondition

1 Notable logical functions

Definition: *Let A be any set. $FALSE$ denotes the logical function, for which*

$$\forall a \in A\colon FALSE(a) = \{false\}$$

Definition: *Let A be any set. $TRUE$ denotes the logical function, for which*

$$\forall a \in A\colon TRUE(a) = \{true\}$$

So, to every element of a set A, the logical function $FALSE$ assigns the $false$ value, and $TRUE$ assigns the $true$ value, respectively.

2 The "implies" relation

Definition: *Let $Q, R \in A \to \mathbb{L}$ by any logical functions. In case $\lceil Q \rceil \subseteq \lceil R \rceil$ holds, then we say that Q implies R-t (in other words: R can be deduced from Q) and we use the following notation: $Q \implies R$.*

Notice that $Q \implies R$ means, that if for any $a \in A$ for which Q holds, then R also holds for a.

Example 1: *Let $A = \{1, 2, 3, 4\}$ be a set and $Q, R \in A \to \mathbb{L}$ be logical functions such that $\lceil Q \rceil = \{1, 3, 4\}$ and $\lceil R \rceil = \{1, 3\}$. In this case $Q \implies R$ does not hold (as to the element 4 the logical function Q assigns the $true$ value, whereas R assigns the $false$ value), but $R \implies Q$ holds.*

Example 2: *Let $A = (a{:}\mathbb{N}, h{:}\mathbb{N})$ be a statespace and $Q, R \in A \to \mathbb{L}$ be logical functions such that $Q = (a = 10)$ end $R = (h = a^3)$. Albeit there exists an element of A (currently the set A is a special set: a statespace, thus its elements are states) to which Q and R assign the $true$ logical value, namely the state $\{a{:}10, h{:}1000\}$, but it is not true that $Q \implies R$, as for example $\{a{:}10, h{:}82\} \in \lceil Q \rceil$ while R assigns the $false$ value to the element $\{a{:}10, h{:}82\}$.*

3 The weakest precondition

Definition: *Let $S \subseteq A \times (\bar{A} \cup \{\textbf{fail}\})^{**}$ be a program, $R \in A \to \mathbb{L}$ be a logical function. We say that the $wp(S, R)\colon A \to \mathbb{L}$ function is the weakest precondition of S with respect to the*

postcondition R, if

$$\lceil wp(S,R)\rceil = \{a \in A \mid a \in D_{p(S)} \wedge p(S)(a) \subseteq \lceil R\rceil\}$$

According to the definition, the weakest precondition holds for a state a, if it is guaranteed that the program S terminates without failure in case it start its execution from state a and every execution of S starting from a ends in states where R holds.

Theorem: *The properties of the weakest precondition wp*
Let $S \subseteq A \times (\bar{A} \cup \{\textbf{fail}\})^{**}$ be a program, $Q, R \in A \to \mathbb{L}$ be logical functions. Then

1. $wp(S, FALSE) = FALSE$
2. *if* $Q \implies R$ *then* $wp(S,Q) \implies wp(S,R)$
3. $wp(S,Q) \wedge wp(S,R) = wp(S, Q \wedge R)$
4. $wp(S,Q) \vee wp(S,R) \implies wp(S, Q \vee R)$

Exercise 1: *Let $A = (x{:}\mathbb{N})$ be a statespace. $R{:}\ A \to \mathbb{L}$ logical function is given, $R = (x < 10)$. Calculate the weakest precondition of the program $x := x - 5$ with respect to the postcondition R.*

First, let us analyse some possible executions of the program $x := x-5$ in order to see how it behaves starting its execution from various states of the satespace: to the state $\{x{:}8\}$ the sequence $< \{x{:}8\}, \{x{:}3\} >$ is assigned, whereas to the state $\{x{:}2\}$ the sequence $< \{x{:}2\}, fail >$ is associated. The programfunction of the program is applicable in states in the form of $\{x{:}a_1\}$, where $a_1 \geqslant 5$. Starting its execution from these states, it is guaranteed that the program will terminate faultlessly in states where the value that belongs to variable x is $a_1 - 5$. Starting from other states, the program will terminate in the state $fail$.

By using the definition of weakest precondition, and denoting the assignment $x := x - 5$ by S, we can say:

$$\begin{aligned}\lceil wp(S,R)\rceil = \{a \in A \mid a \in D_{p(S)} \wedge p(S)(a) \subseteq \lceil R\rceil\} = \\ \{a \in A \mid x(a) \geqslant 5 \wedge \{x(a) - 5\} \subseteq \lceil R\rceil\} = \\ \{a \in A \mid x(a) \geqslant 5 \wedge x(a) - 5 \in \lceil R\rceil\} = \\ \{a \in A \mid x(a) \geqslant 5 \wedge x(a) - 5 < 10\}\end{aligned}$$

In other words, we got that $wp(S,R) = (5 \leqslant x < 15)$ (remember that the name of the only variable of the statespace A is x, and we have just calculated the set of all elements where the weakest precondition holds).

The notion of weakest precondition is very important, on the other hand it is very easy to understand. Notice that in the previous example we calculated that the value of x has to be less than 15 in order for the program to terminate faultlessly in states where the value of x is less than 10.
Of course, it is also true that $(x \in [8..12]) \implies lf(x := x - 5, x < 10)$, that is, if the value that

belongs to variable x is from the set $[8..12]$, then the program $x := x-5$ terminates faultlessly for sure, moreover it terminates in states where $x < 10$ holds. The reason for this is, that the condition $x \in [8..12]$ is stricter than the weakest precondition we calculated. In general: if for any P logical function $P \implies wp(S, R)$ holds (that means that P is stricter than the condition $wp(S, R)$) then starting its execution from states where P holds, program S will terminate faultlessly and R holds for every endstate. This is why the weakest precondition is called "the weakest precondition".