The weakest precondition, the speciafication of a problem

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*

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

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. $wp(S,Q) \vee wp(S,R) \implies wp(S, Q \wedge R)$

Example 3: *Let $A = (x{:}\mathbb{N})$ be a statespace. $R\colon A \to \mathbb{L}$ 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:

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

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".

4 Theorem of specification

Definition: *We say that set B is a parameter space of problem $F \subseteq A \times A$, if there exist a relation $F_1 \subseteq A \times B$ and relation $F_2 \subseteq B \times A$, such that $F = F_2 \circ F_1$ holds.*

Remark: *Any problem $F \subseteq A \times A$ has a parameter space. Since, we can choose B as$A$, and let $F_1 \subseteq A \times B$ and $F_2 \subseteq B \times A$ be relations such that $F_1 = id$ (in other words id is a relation that assign the element a to every $a \in A$) and $F_2 = F$. Then, obviously, $F \circ id = F$.*

Definition: *Let A and B not empty arbitrary sets and $R \subseteq A \times B$ be any relation. The inverse relation of R is:*

$$R^{(-1)} ::= \{(b,a) \in B \times A | (a,b) \in R\}$$

in other words, the inverse of R maps from set B to set A, that only contains the pair $(b,a) \in B \times A$, if $(a,b) \in R$.

Theorem: *Let $F \subseteq A \times A$ be any problem, B is a parameter space of F (so there exist $F_1 \subseteq A \times B$ and $F_2 \subseteq B \times A$ relations such that $F = F_2 \circ F_1$). Let us define the logical functions $Q_b \colon A \to \mathbb{L}$ and $R_b \colon A \to \mathbb{L}$ for every $b \in B$ by providing their truth set:*

$$\lceil Q_b \rceil ::= F_1^{(-1)}(b)$$

$$\lceil R_b \rceil ::= F_2(b)$$

If $\forall b \in B : Q_b \implies wp(S, R_b)$ then program S solves problem F.

$\lceil Q_b \rceil = \{a \in A \mid (a,b) \in F_1\}$, so the truth set of Q_b contains all the states of A, to which relation F_1 assigns the parameter $b \in B$.
$\lceil R_b \rceil = \{a \in A \mid (b,a) \in F_2\}$, so the truth set of R_b contains all the states of A, that are assigned to $b \in B$ by the relation F_2.

5 The specification of a problem

Let as consider the problem, where a positive divisor of a given positive integer number is sought. The statespace of the problem is $A = (n{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$. This problem can be given formally as a set of $(u,v) \in A \times A$ pairs, where the values that belong to variable n are equal in states u and v, and the value of variable d in goalstate v is a divisor of the value of variable n in the initial state u:

$$\{(u, v) \in A \times A \mid n(u) = n(v) \wedge d(v)|n(u)\}$$

Let us provide a different form of the formal description of the problem, by using the notations of the theorem of specification.
We can notice that to every state $a \in A$ where variable n returns the same value, the problem assigns the same states; the problem does not depend on the value of d of the initial state. Let us write down the problem F as a composition of relations F_1 and F_2, such that, to states whose image by F is the same, F_1 assigns the same parameter. Since the value of n is the same in these states, it is advised to assign the same (labelled) parameter to them by the relation F_1. In other words, let a parameter space of the problem is the set of (labelled) positive integers, where the value can by referred by variable n' (as we have only one componenent, the using of a variable would be not necessary, but in a general case it is needed):
$B = (n' {:} \mathbb{N}^+)$.
The fact, that F_1 only assigns $b \in B$ to state $a \in A$ if their n and n' components are equal, can be expressed by providing thelogical function Q_b introduced in the theorem of specification. Let $b \in B$ any arbitrary parameter, then
$\forall a \in A : Q_b(a) = (n(a) = n'(b))$.
Of course, we get the problem F as a composition of relations F_1 and F_2, if F_2 assigns such a state a to parameter $b \in B$, where $d(a)$ is a divisor of the value of n in the initial state. Therefor, for any $b \in B$ let R_b such a logical function, where
$\forall a \in A : R_b(a) = (n(a) = n'(b) \wedge d(a)|n(a))$.
Notice that we need the condition $n(a) = n'(b)$, leaving that out we would only say that in the goalstates the value of d
is a divisor of the current value of n, no stronger relationship between the initial end endstate would be expressed. Thus, the specification of the problem is

$A = (n {:} \mathbb{N}^+, d {:} \mathbb{N}^+)$
$B = (n' {:} \mathbb{N}^+)$
$\forall b \in B : Q_b(a) = (n(a) = n'(b))$ (where $a \in A$ is any state)
$\forall b \in B : R_b(a) = (n(a) = n'(b) \wedge d(a)|n(a))$ (where $a \in A$ is any state)

In the followings, this formal description of the problem (so that in contains the statepace of the problem, a parameter space of the problem; it also contains the definitions of logical functions Q_b and R_b for every $b \in B$) is called the specification of the problem.

Since d is function over statespace A that maps to $\mathbb{N}$ (that means it can take only an element $a \in A$), similarly Q_b is a logical function defined to a parameter $b \in B$ that assigns a logical value to an element $a \in A$; by leaving out the notations that can be figured out, we get the following short form:
$A = (n {:} \mathbb{N}^+, d {:} \mathbb{N}^+)$
$B = (n' {:} \mathbb{N}^+)$
$Q = (n = n')$
$R = (Q \wedge d|n)$