The theorem of specification

1 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.

2 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:

$A = (n{:}\mathbb{N}^+, d{:}\mathbb{N}^+)$

$B = (n'{:}\mathbb{N}^+)$

$Q = (n = n')$

$R = (Q \wedge d|n)$