# 10 The Proof Method of Owicki & Gries

## 10.1 Soundness of the Owicki & Gries Proof Method

In order to prove the soundness of the Owicki & Gries proof method we first prove the soundness of the initialisation and the auxiliary variables rules.

**Lemma 10.1 (Initialisation rule)** Let $h$ be a total function such that the set of write variables of $h$ consists of auxiliary variables of $P$ which do not occur in $\psi$, then $\models \{\varphi\}P\{\psi\}$ implies $\models \{\varphi \circ h\}P\{\psi\}$.

**Proof**
First note that $\varphi \circ h$ is a total boolean function because both $\varphi$ and $h$ are total and $\varphi$ is boolean. Next, let $\bar{z} = \mathit{write}(h)$ and $c \to f$ be a transition of $P$. Then $f = f_1 \circ f_2$, for some $f_1$ and $f_2$ such that $\bar{z} \cap \mathit{var}(f_1) = \emptyset$ and the write variables of $f_2$ are only among $\bar{z}$. Since $\bar{z}$ is a collection of auxiliary variables of $P$, for every pair of states $\sigma$ and $\sigma'$ such that $\sigma(x) = \sigma'(x)$, for all $x \in \mathit{VAR} \setminus \bar{z}$, we have that $\sigma \models c$ if and only if $\sigma' \models c$, because $c$ does not involve the variables of $\bar{z}$. Moreover, for all $x \in \mathit{VAR} \setminus \bar{z}$, we have that $f(\sigma)(x) = f_1(\sigma)(x) = f_1(\sigma')(x) = f(\sigma')(x)$, because the write variables of $f_2$ are only among $\bar{z}$ and $f_1$ does not involve the variables of $\bar{z}$. Now let $\sigma \models \varphi \circ h$ and $\sigma'$ be a final state of a terminating computation of $P$ starting from $\sigma$. By a straightforward induction on the length of the computation, using the above observation, we derive that there exists an execution of $P$ starting from $h(\sigma)$ and resulting in a state $\sigma''$ such that $\sigma'(x) = \sigma''(x)$, for all $x \in \mathit{VAR} \setminus \bar{z}$. So, since $h(\sigma) \models \varphi$, we infer by $\models \{\varphi\}P\{\psi\}$ that $\sigma'' \models \psi$. But the variables of $\bar{z}$ do not occur in $\psi$ so we also conclude that $\sigma' \models \psi$.

■

**Lemma 10.2 (Auxiliary variables rule)** Let $\bar{z}$ be a set of auxiliary variables of $P'$, and $P$ be obtained from $P'$ by restricting all state transformations of $P'$ to all variables excluding $\bar{z}$. Furthermore let $\psi$ be a predicate in which no variable of $\bar{z}$ occurs. Then $\models \{\varphi\}P'\{\psi\}$ implies $\models \{\varphi\}P\{\psi\}$.

**Proof**
Let $c \to f$ be a transition of $P$ and $c \to f \circ g$ be the corresponding transition of $P'$. Since $c$ and $g$ are total functions, and $g$ only changes the values of variables belonging to $\bar{z}$, the effect of executing $c \to f$ in some state $\sigma$ such that $c(\sigma) = tt$ is well-defined iff executing $c \to f \circ g$ in $\sigma$ is well-defined, since $f$ does not involve $\bar{z}$. We have that $f$ does not involve the auxiliary variables $\bar{z}$ and that the write variables of $g$ are among $\bar{z}$. For every pair of states $\sigma$ and $\sigma'$ such that $\sigma(x) = \sigma'(x)$, for every $x \in \mathit{VAR} \setminus \bar{z}$, it follows that $\sigma \models c$ if and only if $\sigma' \models c$ and that $f(\sigma)(x) = f \circ g(\sigma)(x)$ is well-defined whenever $f(\sigma)(x)$ is well-defined,

for all $x \in VAR \setminus \bar{z}$. Now let $\sigma \models \varphi$ and $\sigma'$ be the final state of a terminating computation of $P$ starting from $\sigma$. By a straightforward induction on the length of the computation we derive, using the above observations, that there exists a final state $\sigma''$ of an execution of $P'$ starting from $\sigma$ such that $\sigma'(x) = \sigma''(x)$, for every $x \in VAR \setminus \bar{z}$. So by $\models \{\varphi\}P'\{\psi\}$ we infer that $\sigma'' \models \psi$ and, thus, since $\sigma'$ and $\sigma''$ only differ with respect to the values of the variables $\bar{z}$, and the variables of $\bar{z}$ do not occur in $\psi$, we conclude that $\sigma' \models \psi$.

■

Observe that had we allowed undefined, or partially defined, operations upon auxiliary variables, then the auxiliary variables rule would have been unsound, as the valid triple

$$\models \{true\}\ (x, y := 1/0, 0)\ \{y = 2\}$$

demonstrates. Certainly $x$ is an auxiliary variable of $(x, y) := (1/0, 0)$. However, removing the auxiliary variable component from that assignment does not result in a valid triple, since $\not\models \{true\}\ y := 0\ \{y = 2\}$. This observation is made in [McC89].

Assume that a proof using Owicki & Gries' proof method, that is satisfying points 1 through 5 of Definition 9.5, has been given for $\{\varphi\}\ P\ \{\psi\}$. Then we want to be convinced that this is a valid procedure, i.e., that this proof method is *sound*, and that $\models \{\varphi\}\ P\ \{\psi\}$ holds.

**Theorem 10.3 (Soundness)**
The proof method of Owicki & Gries as formulated in Definition 9.5 is sound.

**Proof**
We will prove that $\models \{\varphi\}P\{\psi\}$ holds. Let $P'$ be obtained from $P \equiv P_1 \| \ldots \| P_n$ as described in point 1 of Definition 95, with $\bar{z}$ a list of the newly introduced auxiliary variables. Furthermore let $\mathcal{Q}_l$ be associated with $l \in L_i$ for $i = 1, \ldots, n$ such that points 2, 3, 4 and 5 of Definition 9.5 are satisfied.

We need to prove that $\models \{\varphi\}P_1 \| \ldots \| P_n\{\psi\}$ holds, where $\varphi$ and $\psi$ in particular satisfy the following clause of Definition 3.17:

5 There exists a function $h$ whose write variables belong to $\bar{z}$ such that $\models \varphi \rightarrow \bigwedge_{i=1}^{n} \mathcal{Q}_{s_i} \circ h$ and $\models \bigwedge_{i=1}^{n} \mathcal{Q}_{t_i} \rightarrow \psi$ hold.

It suffices to prove $\models \{\bigwedge_{i=1}^{n} \mathcal{Q}_{s_i}\}\ P_1' \| \ldots \| P_n'\{\psi\}$ using the soundness of Floyd's inductive assertion method. The soundness of the initialisation rule then gives us

$$\models \{\bigwedge_{i=1}^{n} \mathcal{Q}_{s_i} \circ h\}P_1' \| \ldots \| P_n'\{\psi\},$$

and so $\models \{\varphi\}P_1' \| \ldots \| P_n'\{\psi\}$ follows using 5. Using the soundness of the auxiliary variables rule we conclude that $\models \{\varphi\}P_1 \| \ldots \| P_n\{\psi\}$.

We still have to prove $\models \{\bigwedge_{i=1}^{n} \mathcal{Q}_{s_i}\}P_1' \| \ldots \| P_n'\{\psi\}$. By associating $\bigwedge_{i=1}^{n} \mathcal{Q}_{l_i}$ with global label $\langle l_1, \ldots, l_n \rangle \in L_1 \times \ldots \times L_n$ it follows from the discussion in Sesion 8, that

(i) local correctness of $\{\mathcal{Q}_l | l \in L_i\}$ w.r.t. $P_i'$, i.e., $\{\mathcal{Q}_l | l \in L_i\}$ is an inductive assertion network for $P_i', i = 1, \ldots, n$, and

(ii) the interference freedom test, i.e., $\mathcal{Q}_l$ for $l \in L_i$ is invariant under transitions of $P'_j$, $j \neq i$,

both imply that $\mathcal{Q}_1 \times \ldots \times \mathcal{Q}_n$ is an inductive assertion network for $P'_1 \| \ldots \| P'_n$. Moreover point 5 above holds. Hence one can apply Floyd's inductive assertion method, and by the soundness of that method (Theorem 4.1)

$$\models \{\bigwedge_{i=1}^{n} \mathcal{Q}_{s_i}\} P'_1 \| \ldots \| P'_n \{\psi\}$$

follows.

■

# References


[McC89] E.R. McCurly. Auxiliary variables in partial correctness programming logics. *Information Processing Letters*, 33:131–133, 1989.