Rely-guarantee and Owicki-Gries

(1) Owicki & Gries. An Axiomatic Proof Technique for Parallel Programs I. Acta Informatica 6, 319-340 (1976)

* Take the standard rules from Hoare logic:

$$\frac{}{\{P\}\ \text{skip}\ \{P\}} \qquad \frac{}{\{P[E/x]\}\ x := E\ \{P\}}$$

$$\frac{\{P\}\ C_1\ \{Q\} \quad \{Q\}\ C_2\ \{R\}}{\{P\}\ C_1 ; C_2\ \{R\}} \qquad \frac{\{P\}\ C_1\ \{Q\} \quad \{P\}\ C_2\ \{Q\}}{\{P\}\ C_1 \oplus C_2\ \{Q\}} \qquad \frac{\{P\}\ C\ \{P\}}{\{P\}\ C^*\ \{P\}}$$

$$\frac{}{\{P\}\ \text{assume}(B)\ \{P \wedge B\}} \qquad \frac{P \Rightarrow P' \quad \{P'\}\ C\ \{Q'\} \quad Q' \Rightarrow Q}{\{P\}\ C\ \{Q\}}$$

* Add the following rules for concurrency:

$$\frac{\{P\}\ C\ \{Q\}}{\{P\}\ \text{atomic}\ C\ \{Q\}} \qquad \frac{\{P_1\}\ C_1\ \{Q_1\} \quad \{P_2\}\ C_2\ \{Q_2\}}{\{P_1 \wedge P_2\}\ C_1 \,||\, C_2\ \{Q_1 \wedge Q_2\}}$$

"the proofs are interference-free"

* A statement T with precondition $pre(T)$ does not interfere with a proof $\{P\}\ C\ \{Q\}$ iff:
  - $\{pre(T) \wedge Q\}\ T\ \{Q\}$, and
  - for every subcommand C' of C, with precondition $pre(C')$, except those appearing inside atomic blocks:

$$\{pre(T) \wedge pre(C')\}\ T\ \{pre(C')\}$$

* Two proofs do not interfere iff the first proof does not interfere with any statements from the other and vice versa. (except those inside "atomic")

* Add a rule for eliminating/introducing auxiliary variables:

$$\frac{\{P\}\ C\ \{Q\} \qquad X \cap fv(remove(C,X)) = \emptyset \quad X \cap (fv(P) \cup fv(Q)) = \emptyset}{\{P\}\ remove(C,X)\ \{Q\}}$$

where $remove(C,X)$ replaces all assignments $x := \cdots$ for $x \in X$ with skip.

② Examples:

(a)

$\{x=0\}$

$\{x=0\}$ ‖ $\{\text{true}\}$

$x := x+1$ ‖ $a := x$;

$\{x=1\}$ ‖ $\{a \le x\}$

‖ $b := x$

‖ $\{a \le b\}$

$\{x=1 \wedge a \le b\}$

Interference-freedom checks:

- $\{\text{true} \wedge x=0\}\ x := x+1\ \{\text{true}\}$
- $\{a \le x \wedge x=0\}\ x := x+1\ \{a \le x\}$
- $\{a \le b \wedge x=0\}\ x := x+1\ \{a \le b\}$

(b)

$\{x=0 \wedge a=0 \wedge b=0\}$

C ‖

$\{x = a+b\} \wedge a=0\}$ ‖ $\{x = a+b\} \wedge b=0\}$

atomic (‖ atomic (

$\{x = a+b\} \wedge a=0\}$ ‖

$x := x+1$; ‖ $x := x+1$;

$a := a+1$; ‖ $b := b+1$

$\{x = a+b \wedge a=1\}$ ‖ $\{x = a+b \wedge b=1\}$

) ‖)

$\{x = a+b \wedge a=1\}$ ‖ $\{x = a+b \wedge b=1\}$

$\{x = a+b \wedge a=1 \wedge b=1\}$

$\{x=2\}$ ~~$\{a=1 \wedge b=1\}$~~

Therefore:

$\{x=0\}\ a:=0;\ b:=0;\ C\ \{x=2\}$

By the aux. variable rule:

$\{x=0\}$

atomic $(x := x+1)$ ‖ atomic $(x := x+1)$

$\{x=2\}$