

Rely-guarantee and Owicki-Gries

① Owicki & Gries. An Axiomatic Proof Technique for Parallel Programs I. Acta Informatica 6, 313-340 (1976)

* Take the standard rules from Hoare logic:

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

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

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

* Add the following rules for concurrency:

$$\frac{\{P\} C \{Q\}}{\{P\} \text{atomic } C \{Q\}} \quad \frac{\{P_1\} C_1 \{Q_1\} \quad \{P_2\} C_2 \{Q_2\} \quad \text{"the proofs are interference-free"}}{\{P_1 \wedge P_2\} C_1 \parallel C_2 \{Q_1 \wedge Q_2\}}$$

* A statement T with precondition $\text{pre}(T)$ does not interfere with a proof $\{P\} C \{Q\}$ iff:

- $\{\text{pre}(T) \wedge Q\} T \{Q\}$, and
- for every subcommand C' of C , with precondition $\text{pre}(C')$, except those appearing inside atomic blocks:

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

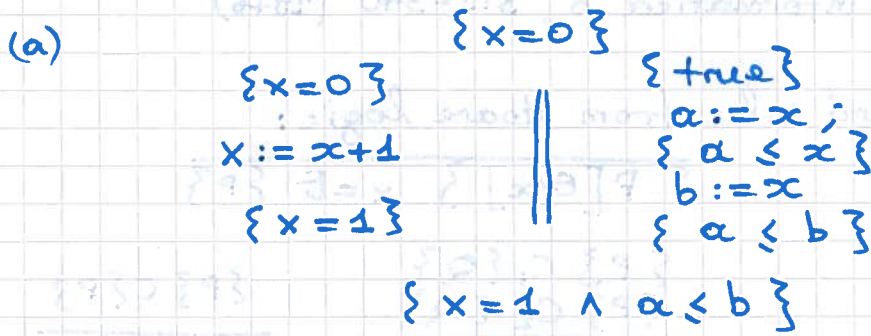
* Two proofs do not interfere iff the first proof does not interfere with any statements from the other and vice versa. (except those inside "atomic")

* Add a rule for eliminating/introducing auxiliary variables:

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

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

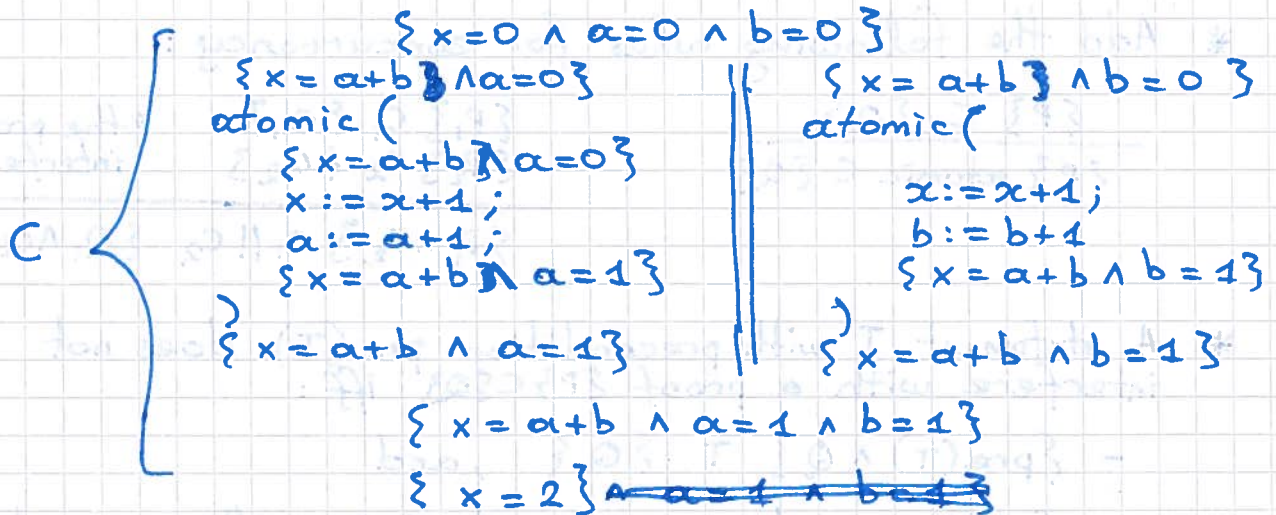
② Examples:



Interference-freeness checks:

- $\{true \wedge x=0\} \quad x := x+1 \quad \{true\}$
- $\{a \leq x \wedge x=0\} \quad x := x+1 \quad \{a \leq x\}$
- $\{a \leq b \wedge x=0\} \quad x := x+1 \quad \{a \leq b\}$

(b)



Therefore:

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

By the aux. variable rule:

$$\begin{array}{c}
 \{x=0\} \\
 \text{atomic} (x := x+1) \parallel \text{atomic} (x := x+1) \\
 \{x=2\}
 \end{array}$$