

Programming Project

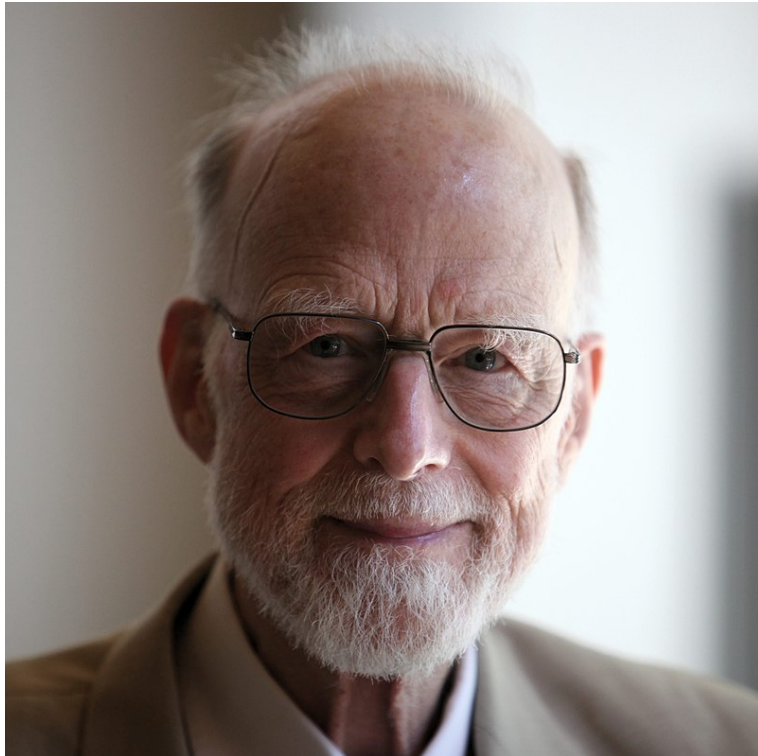
A Simple Hoare Logic Verifier

Kian Hunziker

Seminar Turing Award Winners and
their Contributions

17. December 2020

Hoare Triple



$$\{P\}C\{Q\}$$

- Precondition P
- Program C
- Postcondition Q

Hoare Triple



$$\{P\}C\{Q\}$$

$$\{X = 1\} \mathbf{x} := \mathbf{x} + 1 \{X = 2\}$$

General Approach

- Write Hoare triple
- Program may consist of arithmetic operations
- From postconditions derive preconditions
- Prove, that the given preconditions imply the derived preconditions
- Use linear programming for this proof

General Approach

$$\textit{givenPre} \Rightarrow \textit{derivedPre}$$

$$\equiv \neg(\textit{givenPre} \wedge \neg \textit{derivedPre})$$

Linear Program

- Use cplex by IBM to solve linear program

Example (Optimization Problem as Integer Program)

maximize $X_A + 5X_B$ subject to

$$2 + 2X_A \geq X_B$$

$$X_A + X_B \leq 12$$

$$X_A \leq 6$$

$$X_A \geq 0, \quad X_B \geq 0$$

Demo