

EECS3311 Software Design (Fall 2020)

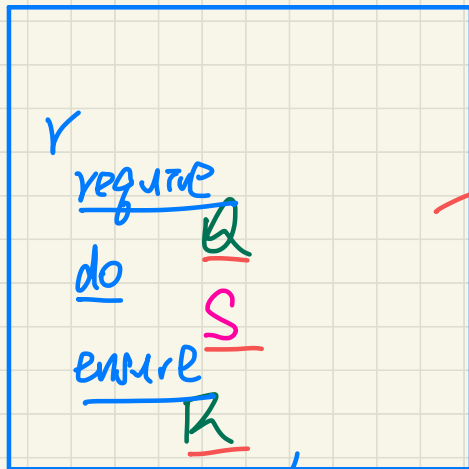
Q&A - Lecture Series W12

Monday, December 7

I think more important than proving Hoare Triple is finding the proper $\{Q\}$ and $\{R\}$ because the whole idea is to prove the correctness but who is going to prove the correctness of $\{Q\}$ and $\{R\}$

Rationale: Complement testing

source code



formulate

$\{ \underline{Q} \} \underline{S} \{ \underline{R} \}$

$\hookrightarrow \underline{Q \Rightarrow wp(S, R)}$

testing

Limitation: finite number of test inputs

$\{x > 0 \wedge y > 0\}$

if $x > y$ then

$bigger := x ; smaller := y$

else

$bigger := y ; smaller := x$

end

$\{bigger \geq smaller\}$

$S_1 \checkmark$

S_2

① wp(if $x > y$ then S_1 else S_2 end, $b \geq s$)
= { wp rule of conditionals }

$x > y \Rightarrow wp(S_1, b \geq s) \mid x > y$ (1.1.1)

$\neg(x > y) \Rightarrow wp(S_2, b \geq s) \mid \neg(x > y)$ (1.1.2)
Exercise.

Q: Is the above program correct?

(1.1.1) $wp(b := x ; s := y, b \geq s)$
= { wp rule of seq. comp. } $b \geq y$

② Formulate the src program into a Hoare Triple: $wp(b := x, wp(s := y, b \geq s))$
 $\{x > 0 \wedge y > 0\} \text{ if } x > y \text{ then } S_1 \text{ else } S_2 \text{ end } \{bigger \geq smaller\}$
Q \xrightarrow{S} R

① Prove that the above Hoare Triple is a tautology.

Q $\Rightarrow wp(S, R)$ (1.1) (1.2)

① $\frac{x}{L} + \frac{y}{L}$

\downarrow \downarrow
 free free

② $\forall z \mid 1 \leq z \leq 10 \cdot \frac{x+y}{L} + z \leq 100$

\downarrow \downarrow \downarrow
 free free free

banded.

Information Hiding

↳ Iterator Pattern

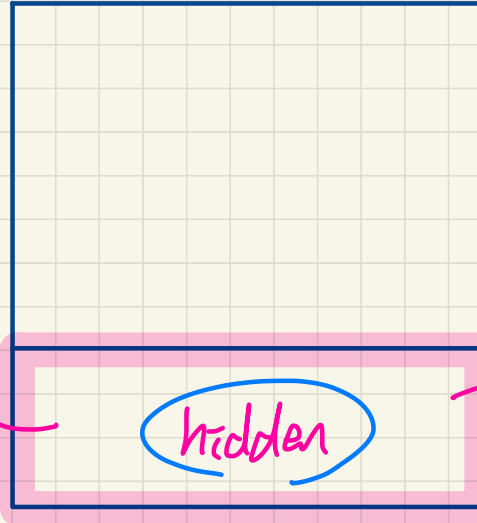
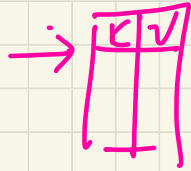
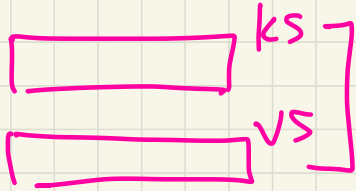
↳ Mathmodels

export status

feature {NONE}

↳ X.

design decision hidden system



- 1. data structures
two arrays
- 2. design decision

class X A D
B C

feature {Y}

[Y, imp in X.
end

part of system
subject to constant
changes
⇒ hide it.