Correctness ("Hoare") Triples

Part 2: Sequencing, Assignment, Strengthening, and Weakening

CS 536: Science of Programming, Fall 2022

A. Why

- To specify a program's correctness, we need to know its precondition and postcondition (what should be true before and after executing it).
- The semantics of a verified program combines its program semantics rule with the state-oriented semantics of its specification predicates.
- To connect correctness triples in sequence, we need to weaken and strengthen conditions.

B. Objectives

At the end of today you should be able to:

- Differentiate between different annotations for the same program.
- Determine whether two correctness triples can be joined and to give the result of joining.
- Reason "backwards" about assignment statements.
- Connect correctness triples in sequence by weakening and strengthening intermediate conditions

C. Problems

1. Suppose $\{p\}\ S\ \{q\}$ and $\{r\}\ S\ \{t\}$ are both valid under some form of correctness (partial or total). Which of the following must also be valid?

   a. $\{p \wedge r\}\ S\ \{q \wedge t\}$ b. $\{p \vee r\}\ S\ \{q \vee t\}$ c. $\{p \wedge r\}\ S\ \{q \vee t\}$
   d. $\{p \rightarrow r\}\ S\ \{q \rightarrow t\}$ e. $\{\neg p \rightarrow r\}\ S\ \{\neg q \rightarrow t\}$ f. $\{p \wedge r\}\ S\ \{q\}$
   g. $\{p\}\ S\ \{q \wedge t\}$ h. $\{p \vee r\}\ S\ \{q\}$ i. $\{p\}\ S\ \{q \vee t\}$

2. Arrange the following predicates in decreasing order of strength: [2022-09-20]
   $x_1 = c \wedge x_2 < d$; $x_1 \le m \vee x_2 \le m \wedge m = max(c, d)$; $x_1 = c$; $(\exists\, k \in \mathbb{N} . x_k \le m)$; $x_1 \le c \vee x_2 \le d$; F; $x_1 \le c$

For the following problems, assume we're working over $\mathbb{Z}$. If there is more than one correct answer then any right answer is sufficient.

3. Consider the triple $\{x \ge 0\}\ y := x*x*x\ \{y > 4*x\}$ [2022-09-20]

   a. Show that this triple is invalid for partial correctness by giving a counterexample state σ that doesn't satisfy it.

 © James Sasaki, 2022

b. Let $P(a, b) \equiv b > 4*a$. Using the backward assignment rule, what is the (weakest) precondition such that $\{...\}\ y := x*x*x\ \{y > 4*x\}$ is valid? State the condition in terms of $P(...)$ and also applying the definition of P. (E.g., $P(5, 1) \equiv 5 > 4*1$.)

c. What are the values of x that don't meet the requirement in (b)?

4. Consider the statement ***if*** $y \ge 0$ ***then*** $x := 3*y$ ***else*** $x := y*y$ ***fi***. Assume that all we know just before the ***if*** is T. (So basically, we know nothing.) What is the strongest (most precise) predicate that is correct

   a. Just before $x := 3*y$?
   b. Just after $x := 3*y$?
   c. Just before $x := 5*y$?
   d. Just after $x := 5*y$?
   e. Just after the ***fi*** (the "end if") ?
   (Hint: Combine your answers to parts (b) and (d).)

5. Find code to fill out $\{x \ge 0\}$ ***if*** *???* ***then*** $y := x*x$ ***else*** $y :=$ *???* ***fi*** $\{y > 2*x\}$ to get a valid triple. There is more than one right answer. (Hint: If $y = x*x$, then when is $y > 2*x$?) [2022-09-20]

Recall that backward assignment tells us that $\{ R(e) \}\ x := e\ \{ R(x) \}$ is valid; here $R(x)$ is a predicate function over x and $R(e)$ is the predicate R gives when $x \equiv e$. E.g., $\{ R(2*k) \}\ x := 2*k\ \{ R(x) \}$ is valid, and if, say, $R(x) \equiv x \% 2 = 0$ (x is even), then the precondition is $R(2*k) \equiv 2*k \% 2 = 0$,

6. Our goal is to use backward assignment to find p and q such that $\models \{p\}\ x := x*x\ \{x > 15\}$ and $\models \{q\}\ x := x+1\ \{p\}$ so that we can join them to get $\{q\}\ y := 2*z;\ x := (y+1)*y\ \{x \ge y*y\}$.

   a. Take $\{p\}\ x := x*x\ \{Q(x)\}$ where $Q(x) \equiv$ the postcondition $x > 15$. Fill in the missing parts in $p \equiv Q(???) \equiv$???, using backward assignment.
   b. Now take $\{q\}\ x := x+1\ \{S(x)\}$ where $S(x) \equiv p$ (from part a). Fill in $q \equiv S(???) \equiv$???, again using backward assignment.

7. Repeat the previous problem using $\{p\}\ x := (y+1)*y\ \{x \ge y*y\}$ and $\models \{q\}\ y := 2*z\ \{p\}$

 © James Sasaki, 2022

Solution to Practice 9 (Hoare Triples, pt. 2)

1. a, b, c, e, f, i

2. $F \mid x_1 = c \wedge x_2 < d \mid x_1 = c \mid x_1 \le c \mid x_1 \le c \vee x_2 \le d \mid x_1 \le m \vee x_2 \le m \wedge m = max(c, d) \mid (\exists\, k \in \mathbb{N} . x_k \le m)$

3. a. One example is $\sigma = \{ x = 0 \}$, another is $\{ x = 1 \}$.
   b. $P(4*x, x*x*x) \equiv 4*x > x*x*x$.
   c. This does not hold if x is $0, 1, 2,$ or $x \le -2.$

4. (Strongest conditions and ***if*** $y \ge 0$ ***then*** $x := 3*y$ ***else*** $x := y*y$ ***fi***)
   a. $y \ge 0$
   b. $y \ge 0 \wedge x = 3*y$
   c. $y < 0$
   d. $y < 0 \wedge x = y*y$
   e. $(y \ge 0 \wedge x = 3*y) \vee (y < 0 \wedge x = y*y)$

5. If $y = x*x$, then $y > 2*x$ for all $x \ge 0$ except $x = 0, 1,$ and 2. So our test is $x > 2$. When $x = 0, 1,$ or 2, we need to set y so that $y > 2*x$. The first two that come to mind are $y := x*x + 1$ and $y := 5$, but there are any number of more ways. Anyway, one answer is

   $\{x \ge 0\}$ ***if*** $x > 2$ ***then*** $y := x*x$ ***else*** $y := 5$ ***fi*** $\{y > 2*x\}$

6. (Set up joining of two statements using backward assignment)
   a. $p \equiv Q(x*x) \equiv x*x > 15$ for $\{p\}\ x := x*x\ \{x > 15\}$ where $Q(x) \equiv x > 15$
   b. $q \equiv S(x+1) \equiv (x+1)*(x+1) > 15$ for $\{q\}\, x := x*x\, \{p\}$, where $S(x) \equiv p \equiv x*x > 15.$

7. (Repeat #6)
   a. $p \equiv Q((y+1)*y, y) \equiv (y+1)*y \ge y*y$ for $\{p\}\ x := (y+1)*y\ \{x \ge y*y\}$, where $Q(x, y) \equiv x \ge y*y$.
   b. $q \equiv S(2*z) \equiv (2*z +1)*(2*z) \ge (2*z)*(2*z)$ for $\{q\}\, y := 2*z\, \{p\}$, where $S(y) \equiv p \equiv (y+1)*y \ge y*y.$

 © James Sasaki, 2022