Correctness ("Hoare") Triples

Part 2: Sequencing, Assignment, Strengthening, and Weakening

CS 536: Science of Programming, Spring 2023

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 (both partial and total correctness work here). 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. $\{ \neg p \rightarrow r \} S \{ \neg q \rightarrow t \}$
   e. $\{ p \rightarrow r \} S \{ q \rightarrow t \}$
   f. $\{ p \wedge r \} S \{ q \}$
   g. $\{ p \} S \{ q \vee t \}$
   h. $\{ p \vee r \} S \{ q \}$
   i. $\{ p \} S \{ q \wedge t \}$

2. Arrange the following predicates in decreasing order of strength.

   a. $x_1 = c \wedge x_2 < d$
   b. $x_1 \leq m \vee x_2 \leq m \wedge m = max(c, d)$
   c. $x_1 = c$
   d. $\exists k \in \mathbb{N} . x\ k \leq m$
   e. $x_1 \leq c \vee x_2 \leq d$
   f. F
   g. $x_1 \leq c$
   h. T

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 $\{x \geq 0\}\ y := x*x*x\ \{y > 4*x\}$
   a. Show that this triple is invalid for partial correctness by giving a counterexample state σ that doesn't satisfy it.
   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*** $y \geq 0$ ***then*** $x := 3*y$ ***else*** $y := y*y$ ***fi***. Assume that all we know just before the ***if*** is T. (So basically, we know nothing.) For each of the positions below, 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 $y := y*y$?
   d. Just after $y := y*y$?
   e. Just after the ***fi*** (the "end if") ?
   (Hint: Combine your answers to parts (b) and (d).)

5. Find code to fill out $\{x \geq 0\}$ ***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 $y > 2*x$?)

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 $\{ q \}\ y := 2*z;\ x := (y+1)*y\ \{x \geq y*y\}$.
   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.

---

* Remember, we say "the" strongest predicate, but anything logically equivalent works too. Same for "the" weakest predicate.

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

8. The questions below have the form "If X, then Y _____ occur". To answer them, fill in the blank with "must", "can't", or "may or may not".
   - ***Must occur*** means X implies Y. (E.g., if $x>1$, then $x>0$ must occur.)
   - ***Can't occur*** means X implies $\neg Y$. (E.g., if $x>1$, then $x<-3$ can't occur.)
   - ***Can occur*** means that either $X \wedge Y$ or $X \wedge \neg Y$ can happen. (E.g., if $x>1$, then $y=0$ may or may not occur.)

   You're not required to justify your answer, though you can if you want to (and you should be able to if asked in to in an exam). Unless specified, assume that $\sigma \neq \bot$ and S may or may not be deterministic. (Note a number of these questions probably go more with Class 8 then Class 9.)

   a. If $\sigma \models \{p\}S\{q\}$ and $\sigma \not\models p$, then $\bot \in M(S,\sigma)$ _____ occur.
   b. If $\sigma \models \{p\}S\{q\}$ and $\sigma \not\models p$, then $M(S,\sigma)-\{\bot\} \models q$ _____ occur.
   c. If $\sigma \models \{p\}S\{q\}$ and $\sigma \models p$, then $\bot \in M(S,\sigma)$ _____ occur.
   d. If $\sigma \models \{p\}S\{q\}$ and $\sigma \models p$, then $M(S,\sigma)-\{\bot\} \models q$ _____ occur.
   e. If $\models_{\text{tot}} \{p\}S\{q\}$ then $\models_{\text{tot}} \{p\}S\{T\}$ _____ occur.
   f. If $\models_{\text{tot}} \{p\}S\{T\}$ then $\models_{\text{tot}} \{p\}S\{q\}$ _____ occur.
   g. If $\sigma \not\models \{p\}S\{q\}$ and S is deterministic, then $\sigma \models p$, $\bot \notin M(S,\sigma)$, and $M(S,\sigma) \models \neg q$ _____ all occur simultaneously.
   h. If $\bot \notin M(S,\sigma)$, $M(S,\sigma) \not\models q$, and S is deterministic, then $M(S,\sigma) \models \neg q$ _____ occur.
   i. If $\bot \notin M(S,\sigma)$, $M(S,\sigma) \not\models q$, and S is nondeterministic, then $M(S,\sigma) \models \neg q$ _____ occur.
   j. If $M(S,\sigma) \not\models q$, $\tau \in M(S,\sigma)$, and S is nondeterministic, then $\tau \models q$ _____ occur.
   k. If S is deterministic and $\sigma \models \{p\}S\{q\}$, then $\sigma \models \{p\}S\{\neg q\}$ _____ occur.
   l. If $\sigma \not\models_{\text{tot}} \{p\}S\{q\}$ and S is deterministic, then $\sigma \models \{p\}S\{\neg q\}$ _____ occur.
   m. If $\sigma \not\models_{\text{tot}} \{p\}S\{q\}$ and S is nondeterministic, then $\sigma \models \{p\}S\{\neg q\}$ _____ occur.
   n. If $\sigma \not\models \{p\}S\{q\}$ and S is deterministic, then $\sigma \models_{\text{tot}} \{p\}S\{\neg q\}$ _____ occur.
   o. If $\sigma \not\models \{p\}S\{q\}$ and S is non-deterministic, then $\sigma \models_{\text{tot}} \{p\}S\{\neg q\}$ _____ occur.

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

1. (a) – (g) are all valid, (h) and (i) are not. The explanations for (d) and (e) are a little subtle.
   For (d), $\{ \neg p \to r \}\ S\ \{ \neg q \to t \}$ is equivalent to $\{ \neg\neg p \vee r \}\ S\ \{ \neg\neg q \vee t \}$, which is the same as (b).
   For (e), we already know $\{ p \}\ S\ \{ q \}$, so if we also know $\{ p \to r \}\ S\ \{ q \to t \}$, then with the help of modus ponens, we know $\{ p \wedge r \}\ S\ \{ q \wedge t \}$, which is (a).

2. (f) F, (a) $x_1 = c \wedge x_2 < d$, (c) $x_1 = c$, (g) $x_1 \le c$, (e) $x_1 \le c \vee x_2 \le d$, (b) $x_1 \le m \vee x_2 \le m \wedge m = max(c, d)$, (d) $\exists\ k \in \mathbb{N}.\, x_k \le m)$, (h) T

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*** $y \le 0$ ***then*** $x := 3*y$ ***else*** $y := y*y$ ***fi***)
   a. $y \le 0$ just before $x := 3*y$
   b. $y \le 0 \wedge x = 3*y$ just after $x := 3*y$
   c. $y > 0$ just before $y := y*y$
   d. $sqrt(y) > 0 \wedge y = sqrt(y)^2$ just after $y := y*y$ *
   e. $(b) \vee (d)$ just after the ***fi***

   * There are other ways to phrase (d) such as $\exists\ y_0.\ y_0 > 0 \wedge y = y_0^2$, but note we can't replace $y = y_0^2$ with $y_0 = sqrt(y)$ because $sqrt$ truncates, so saying $y_0 = sqrt(y)$ makes us forget
   that y is a perfect square after $y := y*y$.

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

6. (Set up joining of two statements using backward assignment)
   a. With $Q(x) \equiv x > 15$, we can use $Q(x*x) \equiv x*x > 15$ for p in $\{p\}\ x := x*x\ \{Q(x)\}$.
   b. With $S(x) \equiv p$ (as in part a), we can use $S(x-1)$ for q in $\{q\}\ x := x-1\ \{S(x)\}$.
   Expanding, $S(x) \equiv p \equiv x*x > 15$, which makes $S(x-1) \equiv (x-1)*(x-1) > 15$.

7. (Repeat #6)

a. With $Q(x, y) \equiv x \geq y*y$, we can use $Q((y+1)*y, y)$ for p in $\{p\}\ x := (y+1)*y\ \{Q(x,y)\}$. Expanding, $p \equiv Q((y+1)*y, y) \equiv (y+1)*y \geq y*y$. (Note $(y+1)*y \geq y*y \Leftrightarrow T$, but the question asked for a syntactic calculation, not a syntactic calculation followed by logical reduction.)

b. With $S(y) \equiv p \equiv (y + 1) * y \geq y * y$, we can use $q \equiv S(2*z)$ in $\{q\}\ y := 2*z\ \{p\}$. Expanding, $q \equiv S(2*z) \equiv (2*z + 1) * 2*z \geq (2*z) * (2*z)$. (Note just saying $2*z*2*z$ is ok because we're now allowing associativity of * in our notion of $\equiv$.)

8. (Hoare triple properties and relationships)

   a-c. can

   d,e must

   f. can

   g,h must

   i,j can

   k. can't

   l. must

   m. can

   n. must

   o. can

