Correctness ("Hoare") Triples, pt. 1

CS 536: Science of Programming, Fall 2021

For all the questions below, you can assume (unless otherwise said) that $\sigma \in \Sigma$, not $\Sigma_\perp$. (I.e., we're not trying to start run a program after an infinite loop or runtime failure.)

1. For a loop-free program without runtime errors, is there any difference between partial and total correctness?
2. Say we're given $\sigma \vDash \{x > 0\}\ S\ \{y > x\}$ for all σ and we're given a state τ where $\tau(x) = -3$. Do we know what S will do if we run in τ? Must it terminate? (With or without a runtime error?) Diverge? Must $y > x$ afterwards? How about $y \le x$?
3. For which σ does $\sigma \vDash \{x > 1\}\ y := x*x\ \{y > x\}$ hold? Is this triple valid?
4. For which σ does $\sigma \vDash \{x > 0\}\ y := x*x\ \{y > x\}$ hold? Is this triple valid?
5. Under partial correctness, does $\sigma \vDash \{F\}\ S\ \{q\}$ hold for all σ, q, and S? What about $\sigma \vDash \{p\}\ S\ \{T\}$? Do these triples say anything interesting about S?
6. Repeat the previous question under total correctness: Does $\sigma \vDash [F]\ S\ [q]$ always hold? Does $\sigma \vDash [p]\ S\ [T]$? Do these triples say anything interesting about S?

For Problems 7 – 14, say for each statement whether it's true or false and give a brief explanation. (Just a sentence or two is fine.) Assume $\sigma \in \Sigma$. (Remember, if $\sigma \vDash$ any predicate or triple, then $\sigma \ne \perp$.)

7. If $\sigma \vDash \{p\}\ S\ \{q\}$, then $\sigma \vDash p$.
8. If $\sigma \nvDash \{p\}\ S\ \{q\}$, then $\sigma \nvDash p$.
9. If $M(S, \sigma) \subseteq \{\perp_d, \perp_e\}$, then $\sigma \vDash \{p\}\ S\ \{q\}$.
10. If $\sigma \vDash p$ and $M(S, \sigma) \cap \{\perp_d, \perp_e\} \ne \emptyset$, then $\sigma \nvDash [p]\ S\ [q]$.
11. If $\sigma \vDash \{p\}\ S\ \{q\}$ and $\sigma \vDash p$, then every state in $M(S, \sigma)$ either $\in \{\perp_d, \perp_e\}$ or satisfies q.
12. If $\sigma \vDash \{p\}\ S\ \{q\}$ and $\sigma \nvDash p$, then every state in $M(S, \sigma)$ is either $\in \{\perp_d, \perp_e\}$ or satisfies $\neg q$.

15. Let $S \equiv x := x * x;\ y := y * y$ and let $\sigma(x) = \alpha$ and $\sigma(\xi) = \beta$. Verify that $\sigma \vDash \{x > y > 0\}\ S\ \{x > y > 0\}$. I.e., assume σ satisfies the precondition, calculate $M(S, \sigma)$, and verify that $M(S, \sigma) - \perp$ satisfies the postcondition.

 © James Sasaki, 2021

Solution to Practice 8 (Hoare Triples, pt 1)

1. No: For a loop-free, failure-free program, there's no difference between partial and total correctness.
2. No to all the questions: The triple only tells us what will happen if the precondition is satisfied. Since $\tau \not\vDash x > 0$, the triple doesn't say anything about what will happen when you run S; it might cause an error or terminate in a state, and that state might satisfy $y > x$, but it might not.
3. All states satisfy the triple, so the triple is valid.
4. States in which x = 1 do not satisfy the triple; states in which x > 1 set y appropriately and do satisfy the triple. States in which x < 1 satisfy the triple trivially.
5. Under partial correctness, for all S, $\{F\}\ S\ \{q\}$ and $\{p\}\ S\ \{T\}$ are valid (satisfied in all states), but neither triple says anything useful about the program S.
6. Under total correctness, $\{F\}\ S\ \{q\}$ is again valid and doesn't say anything useful about S. Under total correctness, however, $\sigma_{tot} \vDash \{p\}\ S\ \{T\}$ if and only if S always terminates when run it in σ. (I.e., it never goes into an infinite loop or fails at runtime.)

7. False; $\sigma \vDash \{p\}\ S\ \{q\}$ does not imply $\sigma \vDash p$. (It doesn't imply $\sigma \not\vDash p$ either.)
8. False; if $\sigma \in \Sigma$ and $\sigma \not\vDash \{p\}\ S\ \{q\}$, then $\sigma \vDash p$ (and $M(S, \sigma) \cap \Sigma \vDash \neg q$).
9. True; under partial correctness, if S always causes an error when run in a σ that satisfies p, then $\sigma \vDash \{p\}\ S\ \{q\}$.
10. True: If $\sigma \vDash p$, then for $\sigma \vDash [p]\ S\ [q]$ to hold, we need $M(S, \sigma) \vDash q$. If $M(S, \sigma) \cap \{\bot_d, \bot_e\} \neq \emptyset$, then $M(S, \sigma) \not\vDash q$, so $\sigma \not\vDash [p]\ S\ [q]$.
11. True; if $\{p\}\ S\ \{q\}$ is partially correct and we run S in a state satisfying p, then either S causes an error or terminates in a state satisfying q.
12. False; if a triple is satisfied in σ but σ doesn't satisfy the precondition, then all possibilities can happen: S might diverge, it might cause a runtime error, and even if it terminates, the final state might satisfy q but it doesn't have to.

15. We're given $S \equiv x := x * x;\ y := y * y$ and $\sigma(x) = \alpha$ and $\sigma(y) = \beta$. For arbitrary σ,

$$\begin{aligned} M(S, \sigma) &= M(x := x * x;\ y := y * y, \sigma) \\ &= M(y := y * y, M(x := x * x, \sigma)) \\ &= M(y := y * y, \sigma[x \mapsto \alpha^2])) \\ &= \{\ \sigma[x \mapsto \alpha^2][y \mapsto \beta^2]\ \}. \end{aligned}$$

Since $\sigma(x) = \alpha$ and $\sigma(y) = \beta$., so $\sigma \vDash x > y > 0$ implies $\alpha > \beta > 0$, which implies $\alpha^2 > \beta^2 > 0$, which implies $\sigma[x \mapsto \alpha^2][y \mapsto \beta^2] \vDash x > y > 0$. Thus $\sigma \vDash \{x > y > 0\}\ S\ \{x > y > 0\}$; i.e., if $\sigma \vDash x > y > 0$ then $M(S, \sigma) - \bot \vDash x > y > 0$.

 © James Sasaki, 2021

So if $\sigma \vDash x > y > 0$, then $M(S, \sigma) - \bot \neq \emptyset$ and $\vDash x > y > 0$. Therefore, $\sigma \vDash \{x > y > 0\}\ S\ \{x > y > 0\}$.

 © James Sasaki, 2021