Correctness ("Hoare") Triples, pt. 1

For all the questions below, you can assume (unless otherwise said) that $\sigma \in \Sigma$, not $\Sigma \bot$. (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 $\sigma \models \{x > 0\} S \{y > x\}$ for all $\sigma$ and we’re given a state $\tau$ where $\tau(x) = -3$. Do we know what $S$ will do if we run in $\tau$? Must it terminate? (With or without a run-time error?) Diverge? Must $y > x$ afterwards? How about $y \leq x$?

3. For which $\sigma$ does $\sigma \models \{x > 1\} y := x \cdot x \{y > x\}$ hold? Is this triple valid?

4. For which $\sigma$ does $\sigma \models \{x > 0\} y := x \cdot x \{y > x\}$ hold? Is this triple valid?

5. Under partial correctness, does $\sigma \models \{F\} S \{q\}$ hold for all $\sigma$, $q$, and $S$? What about $\sigma \models \{p\} S \{T\}$? Do these triples say anything interesting about $S$?

6. Repeat the previous question under total correctness: Does $\sigma \models [F] S [q]$ always hold? Does $\sigma \models [p] S [T]$? Do these triples say anything interesting about $S$?

7. If $\sigma \models \{p\} S \{q\}$, then $\sigma \models p$.

8. If $\sigma \not\models \{p\} S \{q\}$, then $\sigma \not\models p$.

9. If $M(S, \sigma) = \bot$, then $\sigma \models \{p\} S \{q\}$.

10. If $\sigma \models p$ and $M(S, \sigma) \cap \{\bot\} \neq \emptyset$, then $\sigma \not\models [p] S [q]$.

11. If $\sigma \models \{p\} S \{q\}$ and $\sigma \not\models p$, then every state in $M(S, \sigma)$ either is $\bot$ or satisfies $q$.

12. If $\sigma \models \{p\} S \{q\}$ and $\sigma \not\models p$, then every state in $M(S, \sigma)$ is either $\bot$ or satisfies $\neg q$.

15. Let $S \equiv x := x \cdot x \; ; \; y := y \cdot y$ and let $\sigma(x) = \alpha$ and $\sigma(\xi) = \beta$. Verify that $\sigma \models \{x > y > 0\} S \{x > y > 0\}$. I.e., assume $\sigma$ satisfies the precondition, calculate $M(S, \sigma)$, and verify that $M(S, \sigma) - \bot$ satisfies the postcondition.
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 $\tau \not= x > 0$, 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, $\sigma \models [p] S [T]$ if and only if $S$ always terminates when run it in $\sigma$. (I.e., it never goes into an infinite loop or fails at runtime.)

7. False; $\sigma \models \{p\} S \{q\}$ does not imply $\sigma \models p$. (It doesn't imply $\sigma \not= p$ either.)

8. False; if $\sigma \in \Sigma$ and $\sigma \not= \{p\} S \{q\}$, then $\sigma \models p$ (and $M(S, \sigma) \cap \Sigma \models \neg q$).

9. True; under partial correctness, if $S$ always causes an error when run in a $\sigma$ that satisfies $p$, then $\sigma \models \{p\} S \{q\}$.

10. True: If $\sigma \models p$, then for $\sigma \models [p] S [q]$ to hold, we need $M(S, \sigma) \models q$. If $M(S, \sigma) \cap \{\bot_d, \bot_e\} \not= \emptyset$, then $M(S, \sigma) \not= q$, so $\sigma \not= [p] S [q]$.

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 $\sigma$ but $\sigma$ 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 $S \equiv x := x \times x; \ y := y \times y$ and $\sigma(x) = \alpha$ and $\sigma(y) = \beta$. For arbitrary $\sigma$,

$$M(S, \sigma) = M(x := x \times x; \ y := y \times y, \sigma) = M(y := y \times y, M(x := x \times x, \sigma)) = M(y := y \times y, \sigma[x \mapsto \alpha^2]) = \{ \sigma[x \mapsto \alpha^2][y \mapsto \beta^2] \}.$$  

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