Sequential Nondeterminism, Hoare Triples 1 & 2

CS 536: Science of Programming, Spring 2023

Due Thu Feb 16, 11:59 pm [not Sep 16]

A. Problems [60 points total]

Class 7: Sequential Nondeterminism

1. [$12 = 2 * 6$ points] Let DO be the nondeterministic loop [2023-02-13 do/od keywords]

   $\textbf{do}\ x \neq 0 \rightarrow x := x - 1;\ y := y + 1 \ \square\ x \neq 0 \rightarrow x := x - 1;\ y := y + 2\ \textbf{od}$

   a. First, let's work on what what a typical loop iteration does over an arbitrary state $\sigma = \{x = \beta, y = \delta\}$. Assume $\beta \geq 2$ and calculate the two states we can be in after a single iteration of the loop. I.e., what are the τ where $\langle DO, \sigma\rangle \rightarrow^3 \langle DO, \tau\rangle$?

   b. Extend part (a) to do κ iterations where $1 < \kappa \leq \beta$. What is the set of final states Σ' we can reach in 3κ iterations? I.e., what is $\Sigma' = \{\tau \in \Sigma \mid \langle DO, \sigma\rangle \rightarrow^{3\kappa} \langle DO, \tau\rangle\}$?

Classes 8 & 9: Hoare Triples, pt 1 & 2

2. [$16 = 4 * 4$ points]

   a. Using backward assignment, what can we use for precondition p_1 in the triple $\{p_1\}\ b := b + b\ \{b * c \leq d - b\}$? (Mild hint: Be careful with parenthesization)

   b. Using backward assignment, what can we use for p_2 in $\{p_2\}\ x := m\ \{1 \leq x * y \leq n * m\}$?

   c. Using backward assignment, what can we use for p_3 in $\{p_3\}\ y := n\ \{p_2\}$?

   d. Joining parts (b) and (c), what can we use for p_4 in $\{p_4\}\ y := n;\ x := m\ \{1 \leq x * y \leq n * m\}$?

3. [$6 = 2 * 3$ points] Let $p_0 \rightarrow p$, $p \rightarrow p_1$, $q_0 \rightarrow q$, and $q \rightarrow q_1$ all be valid. From $\{p\}\ S\ \{q\}$, there are four triples of the form $\{p_i\}\ S\ \{q_j\}$ that get by replacing p by p_0 or p_1 and q by q_0 or q_1.

   a. If $\sigma \vDash \{p\}\ S\ \{q\}$, which of the four triples $\sigma \vDash \{p_i\}\ S\ \{q_j\}$ is/are also satisfied by σ under $\vDash$? Briefly justify.

   b. Repeat part (a) but under total correctness.

4. [$8 = 2 * 4$ points] Say $\sigma \vDash \{p_1\}\ S\ \{q_1\}$ and $\sigma \vDash \{p_2\}\ S\ \{q_2\}$.

   a. Does $\sigma \vDash \{p_1 \wedge p_2\}\ S\ \{q_1 \vee q_2\}$? Justify briefly.

   b. Does $\sigma \vDash \{p_1 \vee p_2\}\ S\ \{q_1 \wedge q_2\}$? Justify briefly.

5. [*10* points] Answer the following questions below about the relationships between or variations of correctness triples. Assume $\sigma \neq \bot$ and S is deterministic.
   a. [*4* points] There are four statements of the form σ *(*$\models$ or $\not\models$*) {p} S {q* or $\neg q$*}*. Which (if any) of them are implied by $\sigma \models_{\text{tot}} \{ p \} S \{ q \}$?
   b. [*4* points] There are eight statements of the form σ *(*$\models$ or $\not\models$ *) {p} S {q* or $\neg q$*}*. Which (if any) of them are implied by $\sigma \models_{\text{tot}} \{ T \} S \{ q \}$?
   c. [*2* points] There are four statements of the form $\sigma \models \{ p \text{ or } \neg p \} \; S \; \{ q \text{ or } \neg q \}$. When can all four of them be satisfied at the same time, or is it impossible?

Definitions

"Σ_0 ***partly*** $\models p$" means there is a $\tau \in \Sigma_0$ with $\tau \models p$.

"Σ_0 ***partly*** $\not\models p$" means there is a $\tau \in \Sigma_0$ with $\tau \models \neg p$.

6. [*8* = *2* * *4* points] Now assume that $\sigma \neq \bot$ and S is nondeterministic and answer the following questions.
   a. There are four statements of the form σ partly ($\models$ or $\not\models$) $\{ p \} \; S \; \{ q$ or $\neg q \}$. If $\bot \notin M(S, \sigma)$, then which (if any) of them are implied by $\sigma \not\models \{ p \} S \{ q \}$?
   b. Continuing, which (if any) of the remaining statements can occur (but might not) when $\sigma \not\models \{ p \} S \{ q \}$?

Sequential Nondeterminism, Hoare Triples 1 & 2

Solutions

1. (Nondeterministic loop)
   a. $\{x = \beta - 1, y = \delta + 1\}$, $\{x = \beta - 1, y = \delta + 2\}$
   b. $\{x = \beta - \kappa, y = \delta''\}$ where $\kappa \le \delta'' \le 2\kappa$.
   κ times, we add 1 or 2 to δ, so we add a minimum of κ and a maximum of 2κ to δ.

2. (Sequence of backward assignments)
   a. $(b + b) * c \le d - (b + b)$
   b. $u \equiv 1 \le m * y \le n * m$
   c. $v \equiv 1 \le m * n \le n * m$
   d. $w \equiv v \equiv 1 \le m * n \le n * m$

3. (Weakening and strengthening conditions)
   a. $\{p_0\}\, S\, \{q_1\}$ by precondition strengthening and postcondition weakening.
   b. Same: $\{p_0\}\, S\, \{q_1\}$ by strengthening and postcondition weakening.

4. (Conjunctions and disjunctions of conditions)
   a. Yes. If $p_1 \wedge p_2$ holds then postcondition q_1 holds because of p_1 and q_2 holds because of p_2, so postcondition $q_1 \wedge q_2$ holds, and we can weaken that to $q_1 \vee q_2$.
   b. No. If $p_1 \vee p_2$ holds then postcondition $q_1 \vee q_2$ holds, using reasoning similar to part (a), but $q_1 \vee q_2$ doesn't imply $q_1 \wedge q_2$.
   holds. If p_1 holds then q_1 (and therefore $q_1 \vee q_2$) holds; alternatively if p_2 holds then q_2 (and therefore $q_1 \vee q_2$) holds, and $q_1 \vee q_2$ either way.

5. (Relationships among variations of triples)
   a. $\sigma \vDash_{\text{tot}} \{p\}\, S\, \{q\}$ implies $\sigma \vDash \{p\}\, S\, \{q\}$ and $\sigma \nvDash \{p\}\, S\, \{\neg q\}$.
   b. $\sigma \vDash_{\text{tot}} \{T\}\, S\, \{q\}$ implies $\sigma \vDash \{p\}\, S\, \{q\}$ and $\sigma \nvDash \{p\}\, S\, \{\neg q\}$.
   c. If $M(S, \sigma) = \{\bot\}$, then all four of $\sigma \vDash \{p\}\, S\, \{q\}$, $\sigma \vDash \{p\}\, S\, \{\neg q\}$, $\sigma \vDash \{\neg p\}\, S\, \{q\}$, $\sigma \vDash \{\neg p\}\, S\, \{\neg q\}$ are satisfied by σ.

6. (Partial $\vDash$ / $\nvDash$)
   a. $\sigma \nvDash \{p\}\, S\, \{q\}$ and $\bot \notin M(S, \sigma)$ then $M(S, \sigma)$ partly $\vDash \neg q$.
   b. $\sigma \nvDash \{p\}\, S\, \{q\}$ and $M(S, \sigma)$ partly $\vDash q$ can still occur.

