Hoare Triples; Weakest Preconditions; Substitution

CS 536: Science of Programming, Spring 2018

Due Wed Mar 7, 11:59 pm

3/4: p.1; 3/14: p.5

A. Instructions

- You can work together in groups of ≤ 4. Submit your work on Blackboard. Submit one copy, under the name of one person in the group (doesn't matter who). Include the names and A-IDs of everyone in the group (including the submitter) inside that copy.

B. Why?

- Correctness triples are how we write a program with its specification.
- Weakest preconditions give the most general precondition that a program needs.

C. Outcomes

After this homework, you should be able to

- Identify the properties that connect satisfaction of partial and total correctness triples with satisfaction of preconditions and postconditions and with the denotational semantics of programs.
- Be able to weaken or strengthen the conditions of a triple while maintaining validity.
- Be able to calculate the *wp* of a simple loop-free program.

D. Problems [100 points total]

Part 1: Hoare Triples [50 points]

For all these questions, write a short answer, at most a paragraph. As the default, assume $\sigma \in \Sigma$ and S might cause an error ($\bot \in M(S, \sigma)$ is possible). Remember that $\Sigma_\bot = \Sigma \cup \{\bot\}$ = the set of all states, with $\bot$ added; and if $\Sigma_0 \subseteq \Sigma_\bot$ (i.e, Σ_0 is a set of states possibly including $\bot$, then

- $\Sigma_0 \vDash q$ and $\Sigma_0 \vDash \neg q$ can't happen simultaneously.
- If $\bot \in \Sigma_0$ then $\Sigma_0 \nvDash q$ and $\Sigma_0 \nvDash \neg q$ simultaneously.
- If Σ_0 contains more than one member, then it's possible for $\Sigma_0 \nvDash q$ and $\Sigma_0 \nvDash \neg q$ to hold simultaneously.

1. [3 points] Why are $\vDash \{p\}\ S\ \{q\}$ and $\vDash_{tot} \{p\}\ S\ \{q\}$ equivalent if S cannot cause an error?
2. [3 points] If $\sigma \vDash_{tot} \{p\}\ S\ \{\mathtt{T}\}$ and $M(S, \sigma) \nsubseteq \Sigma$, can we conclude anything about σ?
3. [4 = 2 * 2 points] [3/4] Can $\sigma \nvDash_{tot} \{p\}\ S\ \{q\}$ and $\sigma \nvDash_{tot} \{p\}\ S\ \{\neg q\}$ occur simultaneously?[*]
   ~~Can $M(S, \sigma) \nvDash_{tot} \{p\}\ S\ \{q\}$ and $M(S, \sigma) \nvDash_{tot} \{p\}\ S\ \{\neg q\}$ to occur simultaneously~~
   a. When S is deterministic?
   b. When S is nondeterministic but always halts?

[*] (Note this question reduces to "Can $M(S, \sigma) \nvDash q$ and $M(S, \sigma) \nvDash \neg q$ occur simultaneously?")

Problems 4 - 10 are all written briefly as "Is X sufficient for Y or not-Y (or neither)?" There are three possibilities:

- X implies Y (i.e., X is sufficient for Y). Explain why Y must hold.
- X implies not-Y (i.e., X is sufficient for not-Y). Explain why not-Y must hold.
- X implies neither (i.e., X is sufficient for neither). Explain why both (X and Y) and (X and not-Y) are possible.

4. [3 points] Is $\sigma \models \{p\}\ S\ \{q\}$ sufficient for $\sigma \models p$ or $\sigma \models \neg p$?
5. [3 points] Is $\sigma \not\models \{p\}\ S\ \{q\}$ sufficient for $\sigma \models$ or $\not\models \{p\}\ S\ \{\neg q\}$?†
6. [8 = 4 * 2 points] Is $\sigma \not\models \{p\}\ S\ \{q\}$ sufficient for
   a. $\sigma \models p$ or $\sigma \models \neg p$?
   b. $M(S, \sigma) \subseteq \Sigma$ or $\nsubseteq \Sigma$?
   c. $M(S, \sigma) \models q$ or $\not\models q$?
   d. $M(S, \sigma) \models \neg q$ or $\not\models \neg q$?
7. [6 = 3 * 2 points] Are $\sigma \models p$ and $\sigma \models \{p\}\ S\ \{q\}$ together sufficient for
   a. $M(S, \sigma) \subseteq \Sigma$ or $\nsubseteq \Sigma$?
   b. $M(S, \sigma) \models q$ or $\not\models q$?
   c. $M(S, \sigma) \models \neg q \not\models \neg q$?
8. [6 = 3 * 2 points] Are $\sigma \models p$ and $\sigma \models_{tot} \{p\}\ S\ \{q\}$ together sufficient for
   a. $M(S, \sigma) \subseteq \Sigma$ or $\nsubseteq \Sigma$?
   b. $M(S, \sigma) \models q$ or $\not\models q$?
   c. $M(S, \sigma) \models \neg q$ or $\not\models \neg q$?
9. [8 = 4 * 2 points] Is $\sigma \not\models_{tot} \{p\}\ S\ \{q\}$ sufficient for
   a. $M(S, \sigma) \subseteq \Sigma$ or $\nsubseteq \Sigma$?
   b. $M(S, \sigma) \models q$ or $\not\models q$?
   c. $M(S, \sigma) \models \neg q$ or $\not\models \neg q$?
   d. $\sigma \models$ or $\not\models \{p\}\ S\ \{\neg q\}$?
10. [6 = 3 * 2 points] Are $\sigma \models \{p\}\ S\ \{q\}$ and $\sigma \not\models_{tot} \{p\}\ S\ \{q\}$ together sufficient for
    a. $M(S, \sigma) \subseteq \Sigma$ or $\nsubseteq \Sigma$?
    b. $M(S, \sigma) \models q$ or $\not\models q$?
    c. $M(S, \sigma) \models \neg q$ or $\not\models \neg q$?

Part 2: Weakest Preconditions; Substitutions [50 points]

1. [4 points] Assume $p_0 \rightarrow p_1, p_1 \rightarrow p_2, q_0 \rightarrow q_1$, and $q_1 \rightarrow q_2$ are valid. If $\{p_1\}\ S\ \{q_1\}$ is valid, then which of the following triples can we argue are valid using pre-/post-condition weakening/strengthening ? [Fun fact: The answer is the same for partial and total correctness!]
   a. $\{p_0\}\ S\ \{q_0\}$ b. $\{p_2\}\ S\ \{q_0\}$ c. $\{p_0\}\ S\ \{q_2\}$ d. $\{p_2\}\ S\ \{q_2\}$

For Problems 2 – 7, do syntactic calculations of *wp* or substitution but (unless you're asked to), don't do any arithmetic or logical simplifications. E.g., $(\texttt{x+x} \geq 2)[1/\texttt{x}] \equiv \texttt{1+1} \geq 2$ is completely correct. (Continuing with $\texttt{1+1} \geq 2 \Leftrightarrow 2 \geq 2 \Leftrightarrow$ T uses logical simplification; continuing with $\texttt{1+1} \geq 2 \equiv \texttt{T}$ is wrong because it's false.) See the solutions for the *wp* activity questions for the level of detail to give for your answers.

2. [6 points] Calculate $wp(\textbf{if } \texttt{b[M]} \leq \texttt{v} \textbf{ then } \texttt{L := M} \textbf{ else } \texttt{R := M} \textbf{ fi},\ \texttt{L} < \texttt{R} \wedge \texttt{b[L]} \leq \texttt{v} < \texttt{b[R]})$.
3. [6 points] Calculate $wp(\textbf{if } \texttt{even(x)} \textbf{ then } \texttt{x := x+y; y := y+z} \textbf{ fi},\ 0 \leq \texttt{x} < \texttt{n} \wedge \texttt{y} = \texttt{z*(n+x)})$.
4. [6 points] Calculate $wp(\texttt{i := i-j; s := s+i},\ 0 \leq \texttt{i} \leq \texttt{n} \wedge \texttt{s} = \texttt{g(i, n)})$.
5. [6 points] Consider the triple $\{p\}$ $\texttt{j := j-i; i := i+k}$ $\{\texttt{i} \leq \texttt{j} \wedge \texttt{j-i} < \texttt{n}\}$
   a. Calculate the *wp* of the statement and postcondition.
   b. Use logical simplification to get something equivalent but simpler to use for the precondition p.

† I.e., does it imply $\sigma \models \{p\}\ S\ \{\neg q\}$ or $\sigma \not\models \{p\}\ S\ \{\neg q\}$?

6. [6 points] Repeat the previous problem on $\{p\}$ `j := i*j; k := j+i*k` $\{0 < i < j < k\}$.

7. [14 points total] Let $p \equiv x*y < f(z) \vee \forall x\,.\,x \geq a \rightarrow \exists y\,.\,x \div y > y-a-z$. Calculate the following:
   a. [4 points] $p[y-z/x]$. b. [4 points] $p[y+z/y]$ c. [6 points] $p[x+y/a][y-z/x]$

Solution to Homework 3 — Hoare Triples; Strength; Weakest Preconditions

Spring 2018

Part 1 (Hoare Triples)

These four properties are used below (and remember, we've assumed $\sigma \in \Sigma$.):

(i) $\sigma \vDash \{p\}\ S\ \{q\}$ iff $\sigma \vDash \neg p$ or $M(S, \sigma) \nsubseteq \Sigma$ or $M(S, \sigma) \vDash q$.

(ii) $\sigma \vDash_{tot} \{p\}\ S\ \{q\}$ iff $\sigma \vDash \neg p$ or $((M(S, \sigma) \subseteq \Sigma$ and$)\ M(S, \sigma) \vDash q)$

(iii) $\sigma \nvDash \{p\}\ S\ \{q\}$ iff $\sigma \vDash p$ and $(M(S, \sigma) \subseteq \Sigma$ and$)\ M(S, \sigma) \nvDash q$

(iv) $\sigma \nvDash_{tot} \{p\}\ S\ \{q\}$ iff $\sigma \vDash p$ and $(M(S, \sigma) \nsubseteq \Sigma$ or $(M(S, \sigma) \subseteq \Sigma$ and $M(S, \sigma) \nvDash q))$

1. If S can't cause an error, then $M(S, \sigma) \subseteq \Sigma$, so (i) and (ii) are both $\Leftrightarrow (\sigma \vDash \neg p$ or $M(S, \sigma) \vDash q)$, so partial and total correctness of $\{p\}\ S\ \{q\}$ are identical.
2. If $M(S, \sigma) \nsubseteq \Sigma$, then $\bot \in M(S, \sigma)$, so $M(S, \sigma) \nvDash q$. By (ii), $\sigma \vDash_{tot} \{p\}\ S\ \{\mathrm{T}\}$ means $(\sigma \vDash \neg p$ or $M(S, \sigma) \vDash q)$. Since $M(S, \sigma) \nvDash q$, we must have $\sigma \vDash \neg p$.
3. (Can $M(S, \sigma) \nvDash_{tot} \{p\}\ S\ \{q\}$ and $\nvDash_{tot} \{p\}\ S\ \{\neg q\}$ simultaneously?)
   a. If S is deterministic then $M(S, \sigma) = \{\tau\} \subseteq \Sigma_\bot$. We need $\tau = \bot$: if $\tau \in \Sigma$ then either $\{\tau\} \vDash q$ or $\{\tau\} \vDash \neg q$, which implies that $M(S, \sigma)$ satisfies (under total correctness) either $\{p\}\ S\ \{q\}$ or $\{p\}\ S\ \{\neg q\}$.
   b. If S is nondeterministic but always halts then $M(S, \sigma) = \{\tau_1, \tau_2\} \subseteq \Sigma$. If τ_1 and τ_2 both $\vDash q$ then $M(S, \sigma) \vDash_{tot} \{p\}\ S\ \{q\}$. Similarly, if they both $\vDash \neg q$, then together $M(S, \sigma) \vDash_{tot} \{p\}\ S\ \{\neg q\}$. We need one of τ_1 and τ_2 to satisfy q and one to satisfy $\neg q$ so that the pair together satisfies neither q nor $\neg q$.
4. By (i), $\sigma \vDash \{p\}\ S\ \{q\}$ implies neither $\sigma \vDash p$ nor $\sigma \vDash \neg p$.
5. (Is $\sigma \nvDash \{p\}\ S\ \{q\}$ sufficient for $\sigma \vDash$ or $\nvDash \{p\}\ S\ \{\neg q\}$?) By (iii), $\sigma \nvDash \{p\}\ S\ \{q\}$ implies $\sigma \vDash p$ and $(M(S, \sigma) \subseteq \Sigma$ and$)\ M(S, \sigma) \nvDash q$. (Case 1) If $M(S, \sigma)$ has just one state, say τ, then $\tau \nvDash q$ implies $\tau \vDash \neg q$, so $\sigma \vDash \{p\}\ S\ \{\neg q\}$. (Case 2) If $M(S, \sigma)$ has multiple states, then for it to $\nvDash q$, it must have at least one member that $\vDash \neg q$. If every state in $M(S, \sigma) \vDash \neg q$, then $\sigma \vDash \{p\}\ S\ \{\neg q\}$; if some state in in $M(S, \sigma) \vDash q$, then $M(S, \sigma) \nvDash \neg q$, so $\sigma \nvDash \{p\}\ S\ \{\neg q\}$, so our condition is sufficient for neither.
6. By (iii), $\sigma \nvDash \{p\}\ S\ \{q\}$ implies (a) $\sigma \vDash p$, (b) $M(S, \sigma) \subseteq \Sigma$, and (c) $M(S, \sigma) \nvDash q$. (d) both $M(S, \sigma) \vDash$ and $M(S, \sigma) \nvDash \neg q$ are possible if $M(S, \sigma)$ has more than one state. If $M(S, \sigma) = \{\tau\}$ for some τ, then $M(S, \sigma) \nvDash q$ iff $M(S, \sigma) \vDash \neg q$ because $\tau \neq \bot$ by assumption.
7. By (i), if $\sigma \vDash p$ and $\sigma \vDash \{p\}\ S\ \{q\}$, then we have two possible situations:
   (a) $M(S, \sigma) \nsubseteq \Sigma$, which implies (b) $M(S, \sigma) \nvDash q$ and (d) $M(S, \sigma) \nvDash \neg q$
   or (a) $M(S, \sigma) \subseteq \Sigma$, so (b) $M(S, \sigma) \vDash q$, so (d) $M(S, \sigma) \nvDash \neg q$
8. By (ii), if $\sigma \vDash p$ and $\sigma \vDash_{tot} \{p\}\ S\ \{q\}$, then (a) $M(S, \sigma) \subseteq \Sigma$, (b) $M(S, \sigma) \vDash q$, and (c) $M(S, \sigma) \nvDash \neg q$.
9. By (iv), $\sigma \nvDash_{\mathrm{tot}} \{p\}\ S\ \{q\}$ implies $\sigma \vDash p$ and either
   (a) $M(S, \sigma) \nsubseteq \Sigma$, which implies (b) $M(S, \sigma) \nvDash q$ and (d) $M(S, \sigma) \nvDash \neg q$
   or (a) $M(S, \sigma) \subseteq \Sigma$ and (b) $M(S, \sigma) \nvDash q$. In this case, $M(S, \sigma) \vDash$ and $\nvDash \neg q$ are both possible, so our condition is (c) sufficient for neither $M(S, \sigma) \vDash \neg q$ nor $M(S, \sigma) \nvDash \neg q$.
10. (Assume $\sigma \vDash \{p\}\ S\ \{q\}$ and $\sigma \nvDash_{tot} \{p\}\ S\ \{q\}$ both hold)
    By (i), $\sigma \vDash \{p\}\ S\ \{q\}$ implies $\sigma \vDash \neg p$ or $M(S, \sigma) \nsubseteq \Sigma$ or $(M(S, \sigma) \subseteq \Sigma$ and$)\ M(S, \sigma) \vDash q$.

By (iv) $\sigma \not\vDash_{tot} \{p\}\ S\ \{q\}$ implies $\sigma \vDash p$ and $(M(S, \sigma) \not\subseteq \Sigma$ or $(M(S, \sigma) \subseteq \Sigma$ and $M(S, \sigma) \not\vDash q))$

We can't have $M(S, \sigma) \subseteq \Sigma$, because then $M(S, \sigma) \vDash$ and $\not\vDash q$ simultaneously. So we know (a) $M(S, \sigma) \not\subseteq \Sigma$ (i.e., S can cause an error) and therefore (b) $M(S, \sigma) \not\vDash q$ and $\sigma \vDash p$ and (c) $M(S, \sigma) \not\vDash \neg q$. (We also know $\sigma \vDash p$, but that wasn't asked about.)

Part 2 (Strength; Weakest Preconditions)

1. (Weakening and strengthening conditions) We can always strengthen preconditions and weaken postconditions, so we can replace p_1 by p_0 because $p_0 \to p_1$, and we can replace q_1 by q_2 because $q_1 \to q_2$. Only (c) below can be justified using strengthening and weakening.

   a. $\{p_0\}\ S\ \{q_0\}$: Precondition strengthening is ok; postcondition strengthening isn't ok.

   b. $\{p_2\}\ S\ \{q_0\}$: Precondition weakening isn't ok; neither is postcondition strengthening.

   c. $\{p_0\}\ S\ \{q_2\}$: Precondition strengthening and postcondition weakening are both ok.

   d. $\{p_2\}\ S\ \{q_2\}$: Precondition weakening isn't ok; postcondition weakening is ok.

   Note: Even though the triples (a), (b), and (d) aren't provable by weakening or strengthening, they might still be valid for other reasons.

2. Let $S \equiv$ **if** b[M] $\le$ v **then** L **:=** M **else** R **:=** M **fi**.

   Let $q \equiv$ L $<$ R $\wedge$ b[L] $\le$ v $<$ b[R]

   Let $w_1 \equiv wp($L **:=** M**,** $q) \equiv$ M $<$ R $\wedge$ b[M] $\le$ v $<$ b[R] $\wedge$ M $<$ R

   Let $w_2 \equiv wp($R **:=** M**,** $q) \equiv$ L $<$ M $\wedge$ b[L] $\le$ v $<$ b[M]

   Then $wp(S, q) \equiv ($b[M] $\le$ v $\to w_1) \wedge ($b[M] $>$ v $\to w_2)$

   $\equiv ($b[M] $\le$ v $\to$ M $<$ R $\wedge$ b[M] $\le$ v $<$ b[R]$) \wedge ($b[M] $>$ v $\to$ L $<$ M $\wedge$ b[L] $\le$ v $<$ b[M]$)$ ‡

[3/14 - $S_1 \equiv$ x+y, not x-y]

3. Let $S_1 \equiv$ x **:=** x+y, $S_2 \equiv$ y **:=** y+z, and $q \equiv 0 \le$ x $<$ n $\wedge$ y **=** z*(n+x).

   First, we can calculate $wp(S_2, q)$

   $\equiv$ $wp($y **:=** y+z, $0 \le$ x $<$ n $\wedge$ y **=** z*(n+x)$)$

   $\equiv 0 \le$ x $<$ n $\wedge$ y+z **=** z*(n*x)

   Then we can calculate $wp(S_1$ **;** $S_2, q)$

   $\equiv wp(S_1, wp(S_2, q))$

   $\equiv wp($x **:=** x+y, $0 \le$ x $<$ n $\wedge$ y+z **=** z*(n+x)$)$

   $\equiv 0 \le$ x+y $<$ n $\wedge$ y+z **=** z*(n+(x+y))

   Then $wp($**if** even(x) **then** S_1**;** S_2 **fi**, $q)$

   $\equiv wp($**if** even(x) **then** S_1**;** S_2 **else skip fi**, $q)$

   $\equiv ($even(x) $\to wp(S_1$**;** $S_2, q)) \wedge ($odd(x) $\to wp($**skip**, $q))$

   $\equiv ($even(x) $\to 0 \le$ x+y $<$ n $\wedge$ y+z **=** z*(n+(x+y))$) \wedge ($odd(x) $\to q)$

4. $wp($i **:=** i-j**;** s **:=** s+i, $0 \le$ i $\le$ n $\wedge$ s $=$ g(i**,** n)$)$

   $\equiv wp($i **:=** i-j, $wp($s **:=** s+i, $0 \le$ i $\le$ n $\wedge$ s $=$ g(i**,** n)$))$

‡ I think it's safe now to treat $\neg(e_1 < e_2) \equiv e_1 \ge e_2$, or $\neg$odd(x) $\equiv$ even(x) or $p \wedge$ T $\equiv p$.

$\equiv wp(\texttt{i := i-j}, 0 \le \texttt{i} \le \texttt{n} \wedge \texttt{s+i} = \texttt{g(i, n)})$

$\equiv 0 \le \texttt{i-j} \le \texttt{n} \wedge \texttt{s+i-j} = \texttt{g(i-j, n)}$

5. $wp(\texttt{j := j-i; i := i+k}, \texttt{i} \le \texttt{j} \wedge \texttt{j-i} < \texttt{n})$

$\equiv wp(\texttt{j := j-i}, wp(\texttt{i := i+k}, \texttt{i} \le \texttt{j} \wedge \texttt{j-i} < \texttt{n}))$

$\equiv wp(\texttt{j := j-i}, \texttt{i+k} \le \texttt{j} \wedge \texttt{j-(i+k)} < \texttt{n})$

$\equiv \texttt{i+k} \le \texttt{j-i} \wedge \texttt{j-i-(i+k)} < \texttt{n}$

$\Leftrightarrow \texttt{2*i+k} \le \texttt{j} \wedge \texttt{j} < \texttt{n+i+(i+k)}$

$\Leftrightarrow \texttt{2*i+k} \le \texttt{j} < \texttt{n+2*i+k}$

$\Leftrightarrow 0 \le \texttt{j} < \texttt{n}$

6. $wp(\texttt{j := i*j; k := j+i*k}, 0 < \texttt{i} < \texttt{j} < \texttt{k})$

$\equiv wp(\texttt{j := i*j}, wp(\texttt{k := j+i*k}, 0 < \texttt{i} < \texttt{j} < \texttt{k}))$

$\equiv wp(\texttt{j := i*j}, 0 < \texttt{i} < \texttt{j} < \texttt{j+i*k})$

$\equiv 0 < \texttt{i} < \texttt{i*j} < \texttt{i*j+i*k}$

$\Leftrightarrow 0 < \texttt{i} \wedge \texttt{i} < \texttt{i*j} < \texttt{i*j+i*k}$ (splitting apart the chained tests)

$\Leftrightarrow 0 < \texttt{i} \wedge 1 < \texttt{j} < \texttt{j+k}$ (dividing the right predicate by i)

$\Leftrightarrow \texttt{i} > 0 \wedge \texttt{j} > 1 \wedge \texttt{k} > 0$

$\Leftrightarrow 0 < \texttt{k}$ [and info about j]

7. (Substitutions involving $p \equiv \texttt{x*y} < \texttt{f(z)} \vee \forall \texttt{x} . \texttt{x} \ge \texttt{a} \to \exists \texttt{y} . \texttt{x} \div \texttt{y} > \texttt{y-a-z}$)

7a. $p[\texttt{y-z/x}] \equiv (\texttt{x*y} < \texttt{f(z)} \vee \forall \texttt{x} . \texttt{x} \ge \texttt{a} \to \exists \texttt{y} . \texttt{x} \div \texttt{y} > \texttt{y-a-z})[\texttt{y-z/x}]$

$\equiv (\texttt{x*y} < \texttt{f(z)})[\texttt{y-z/x}] \vee (\forall \texttt{x} . \texttt{x} \ge \texttt{a} \to \exists \texttt{y} . \texttt{x} \div \texttt{y} > \texttt{y-a-z})[\texttt{y-z/x}]$

$\equiv \texttt{(y-z)*y} < \texttt{f(z)} \vee \forall \texttt{x} . \texttt{x} \ge \texttt{a} \to \exists \texttt{y} . \texttt{x} \div \texttt{y} > \texttt{y-a-z}$ [the $\forall$x shields x]

7b. $p[\texttt{y+z/y}] \equiv (\texttt{x*y} < \texttt{f(z)} \vee \forall \texttt{x} . \texttt{x} \ge \texttt{a} \to \exists \texttt{y} . \texttt{x} \div \texttt{y} > \texttt{y-a-z})[\texttt{y+z/y}]$

$\equiv (\texttt{x*y} < \texttt{f(z)})[\texttt{y+z/y}] \vee (\forall \texttt{x} . \texttt{x} \ge \texttt{a} \to \exists \texttt{y} . \texttt{x} \div \texttt{y} > \texttt{y-a-z})[\texttt{y+z/y}]$

$\equiv \texttt{x*(y+z)} < \texttt{f(z)} \vee \forall \texttt{x} . \texttt{x} \ge \texttt{a} \to \exists \texttt{y} . \texttt{x} \div \texttt{y} > \texttt{y-a-z}$ [the $\exists$y shields y]

7c. To calculate $p[\texttt{x+y/a}][\texttt{y*z/x}]$, we'll first calculate $p_1 \equiv p[\texttt{x+y/a}]$, then we'll calculate $p_1[\texttt{y-z/x}]$

$p_1 \equiv p[\texttt{x+y/a}] \equiv (\texttt{x*y} < \texttt{f(z)} \vee \forall \texttt{x} . \texttt{x} \ge \texttt{a} \to \exists \texttt{y} . \texttt{x} \div \texttt{y} > \texttt{y-a-z})[\texttt{x+y/a}]$

$\equiv (\texttt{x*y} < \texttt{f(z)}[\texttt{x+y/a}] \vee \forall \texttt{x} . \texttt{x} \ge \texttt{a} \to \exists \texttt{y} . \texttt{x} \div \texttt{y} > \texttt{y-a-z})[\texttt{x+y/a}]$

$\equiv (\texttt{x*y} < \texttt{f(z)}) \vee (\forall \texttt{x} . \texttt{x} \ge \texttt{a} \to \exists \texttt{y} . \texttt{x} \div \texttt{y} > \texttt{y-a-z})[\texttt{x+y/a}]$

$\equiv \texttt{x*y} < \texttt{f(z)} \vee \forall \texttt{v} . (\texttt{x} \ge \texttt{a} \to \exists \texttt{y} . \texttt{x} \div \texttt{y} > \texttt{y-a-z})[\texttt{v/x}][\texttt{x+y/a}]$ (renaming x to v)

$\equiv \texttt{x*y} < \texttt{f(z)} \vee \forall \texttt{v} . (\texttt{v} \ge \texttt{a} \to \exists \texttt{y} . \texttt{v} \div \texttt{y} > \texttt{y-a-z})[\texttt{x+y/a}]$

$\equiv \texttt{x*y} < \texttt{f(z)} \vee \forall \texttt{v} . \texttt{v} \ge \texttt{x+y} \to (\exists \texttt{y} . \texttt{v} \div \texttt{y} > \texttt{y-a-z})[\texttt{x+y/a}]$

$\equiv \texttt{x*y} < \texttt{f(z)} \vee \forall \texttt{v} . \texttt{v} \ge \texttt{x+y} \to \exists \texttt{w} . (\texttt{v} \div \texttt{y} > \texttt{y-a-z})[\texttt{w/y}] [\texttt{x+y/a}]$ (renaming y to w)

$\equiv \texttt{x*y} < \texttt{f(z)} \vee \forall \texttt{v} . \texttt{v} \ge \texttt{x+y} \to \exists \texttt{w} . (\texttt{v} \div \texttt{w} > \texttt{w-a-z}) [\texttt{x+y/a}]$

$\equiv \texttt{x*y} < \texttt{f(z)} \vee \forall \texttt{v} . \texttt{v} \ge \texttt{x+y} \to \exists \texttt{w} . \texttt{v} \div \texttt{w} > \texttt{w-(x+y)-z}$

Then $p[\texttt{x+y/a}][\texttt{y-z/x}]$

$\equiv p_1[\texttt{y-z/x}]$

$\equiv$ (x*y < f(z) ∨ ∀v . v ≥ x+y → ∃w . v ÷ w > w−(x+y)−z) [y−z/x]

$\equiv$ (y−z)*y < f(z) ∨ ∀v . v ≥ (y−z)+y → ∃w . v ÷ w > w−((y−z)+y)−z

