More on Relations and Hoare Logic

Viktor Kunčak

November 8, 2019

Syntactic vs Semantic Hoare Triples

We defined Hoare triple for sets and relations: $\{P\}r\{Q\}$ where $P \subseteq S$, $r \subseteq S \times S$, $Q \subseteq S$:

$$\forall \bar{x}, \bar{x}'.(\bar{x} \in P \wedge (\bar{x}, \bar{x}') \in r \longrightarrow \bar{x}' \in Q)$$

We also extend this notation when A, B are formulas and c is a program fragment (command). In such case, let

- $P = A_s$
- $r = \rho(c)$ (relation associated with the command)
- $Q = B_s$

here, if F is a formula (e.g. A or B) over x, then F_s denotes $\{\bar{x} \mid F\}$ i.e. the set of states where formula holds.
Then we define $\{A\}c\{B\}$ to mean

$$\{A_s\}\ \rho(c)\ \{B_s\}$$

which reduces it to the case of sets and relations.

Exercise: Which Hoare triples are valid?

Assume all variables to be over integers.

1. $\{j = a\}$ j =j+1 $\{a = j + 1\}$
2. $\{i = j\}$ i=j+i $\{i > j\}$
3. $\{j = a + b\}$ i=b; j=a $\{j = 2 * a\}$
4. $\{i > j\}$ j=i+1; i=j+1 $\{i > j\}$
5. $\{i \mathrel{!}= j\}$ **if** i>j **then** m=i–j **else** m=j–i $\{m > 0\}$
6. $\{i = 3 * j\}$ **if** i>j **then** m=i–j **else** m=j–i $\{m - 2 * j = 0\}$

Review: Three Forms of Hoare Triple

Lemma: the following three conditions are equivalent:

- $\{P\}r\{Q\}$
- $P \subseteq wp(r, Q)$
- $sp(P, r) \subseteq Q$

Proof. The three conditions expand into the following three formulas

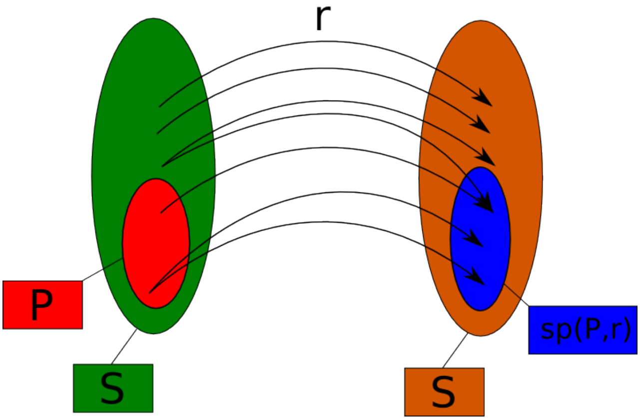
- $\forall s, s'. \; [(s \in P \wedge (s, s') \in r) \rightarrow s' \in Q]$
- $\forall s. \; [s \in P \rightarrow (\forall s'.(s, s') \in r \rightarrow s' \in Q)]$
- $\forall s'. \; [(\exists s. \; s \in P \wedge (s, s') \in r) \rightarrow s' \in Q]$

which are easy to show equivalent using basic first-order logic properties, such as $(P \wedge Q \longrightarrow R) \longleftrightarrow (P \longrightarrow (Q \longrightarrow R))$, $(\forall u.(A \longrightarrow B)) \longleftrightarrow (A \longrightarrow \forall u.B)$ when $u \notin FV(A)$, and $(\forall u.(A \longrightarrow B)) \longleftrightarrow ((\exists u.A) \longrightarrow B)$ when $u \notin FV(B)$.

Lemma: Characterization of sp

$sp(P, r)$ is the the smallest set Q such that $\{P\}r\{Q\}$, that is:

- $\{P\}r\{sp(P, r)\}$
- $\forall Q \subseteq S.\ \{P\}r\{Q\} \rightarrow sp(P, r) \subseteq Q$



$$\{P\}\ r\ \{Q\} \Leftrightarrow \forall s, s' \in S. (s \in P \land (s, s') \in r \rightarrow s' \in Q)$$

Proof of Lemma: Characterization of sp

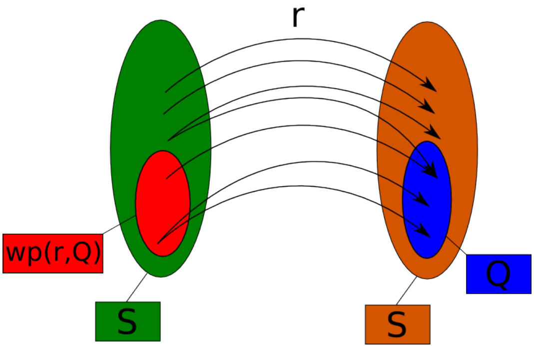
Apply Three Forms of Hoare triple. The two conditions then reduce to:

- $sp(P, r) \subseteq sp(P, r)$
- $\forall P \subseteq S.\ sp(P, r) \subseteq Q \rightarrow sp(P, r) \subseteq Q$

Lemma: Characterization of wp

$wp(r, Q)$ is the largest set P such that $\{P\}r\{Q\}$, that is:

- $\{wp(r, Q)\}r\{Q\}$
- $\forall P \subseteq S.\ \{P\}r\{Q\} \rightarrow P \subseteq wp(r, Q)$



$$\{P\}\ r\ \{Q\} \Leftrightarrow \forall s, s' \in S. (s \in P \wedge (s, s') \in r \rightarrow s' \in Q)$$

$$wp(r, Q) = \{s \mid \forall s'. (s, s') \in r \rightarrow s' \in Q\}$$

Proof of Lemma: Characterization of wp

Apply Three Forms of Hoare triple. The two conditions then reduce to:

- $wp(r, Q) \subseteq wp(r, Q)$
- $\forall P \subseteq S.\ P \subseteq wp(r, Q) \rightarrow P \subseteq wp(r, Q)$

Exercise: Postcondition of inverse versus wp

Lemma:

$$S \setminus wp(r, Q) = sp(S \setminus Q, r^{-1})$$

In other words, when instead of good states we look at the completement set of "error states", then *wp* corresponds to doing *sp* backwards.

Note that $r^{-1} = \{(y,x) \mid (x,y) \in r\}$ and is always defined.

Exercise: Postcondition of inverse versus wp

Lemma:

$$S \setminus wp(r, Q) = sp(S \setminus Q, r^{-1})$$

In other words, when instead of good states we look at the completement set of "error states", then *wp* corresponds to doing *sp* backwards.

Note that $r^{-1} = \{(y, x) \mid (x, y) \in r\}$ and is always defined.

Proof of the lemma: Expand both sides and apply basic first-order logic properties.

Left side:
$x \in S \setminus wp(r, Q)$
$x \notin wp(r, Q)$
$\neg(\forall x'.(x, x') \in r \longrightarrow x' \in Q)$
$\exists x'.(x, x') \in r \land x' \notin Q$

Right side:
$x \in sp(S \setminus Q, r^{-1})$
$\exists x'.x' \notin Q \land (x', x) \in r^{-1}$
$\exists x'.x' \notin Q \land (x, x') \in r$

More Laws on Preconditions and Postconditions

Disjunctivity of sp

$$sp(P_1 \cup P_2, r) = sp(P_1, r) \cup sp(P_2, r)$$

$$sp(P, r_1 \cup r_2) = sp(P, r_1) \cup sp(P, r_2)$$

Conjunctivity of wp

$$wp(r, Q_1 \cap Q_2) = wp(r, Q_1) \cap wp(r, Q_2)$$

$$wp(r_1 \cup r_2, Q) = wp(r_1, Q) \cap wp(r_2, Q)$$

Pointwise wp

$$wp(r, Q) = \{s \mid s \in S \wedge sp(\{s\}, r) \subseteq Q\}$$

Pointwise sp

$$sp(P, r) = \bigcup_{s \in P} sp(\{s\}, r)$$

Proof of wp with respect to relation union

$$wp(r_1 \cup r_2, Q) = wp(r_1, Q) \cap wp(r_2, Q)$$

Left side:

$x \in wp(r_1 \cup r_2, Q)$
$\forall x'.((x,x') \in r_1 \cup r_2 \longrightarrow x' \in Q)$
$\forall x'.(((x,x') \in r_1) \vee ((x,x') \in r_2)) \longrightarrow x' \in Q)$
$\forall x'.\big(((x,x') \in r_1 \longrightarrow x' \in Q) \ \wedge$
$\quad ((x,x') \in r_2 \longrightarrow x' \in Q)\big)$

Right side:

$x \in wp(r_1, Q) \cap wp(r_2, Q)$
$x \in wp(r_1, Q)$ and $x \in wp(r_2, Q)$
$(\forall x'.(x,x') \in r_1 \longrightarrow x' \in Q) \ \wedge$
$(\forall x'.(x,x') \in r_2 \longrightarrow x' \in Q)$

where we used the fact that $(A \vee B) \longrightarrow C$ is equivalent to $(A \longrightarrow C) \wedge (B \longrightarrow C)$

Hoare Logic for Loop-free Code

Expanding Paths

The condition

$$\{P\} \left(\bigcup_{i \in J} r_i \right) \{Q\}$$

is equivalent to

$$\forall i. i \in J \rightarrow \{P\} r_i \{Q\}$$

Proof: By definition, or use that the first condition is equivalent to $sp(P, \bigcup_{i \in J} r_i) \subseteq Q$ and $\{P\} r_i \{Q\}$ to $sp(P, r_i) \subseteq Q$

Transitivity

If $\{P\} s_1 \{Q\}$ and $\{Q\} s_2 \{R\}$ then also $\{P\} s_1 \circ s_2 \{R\}$.
We write this as the following inference rule:

$$\frac{\{P\} s_1 \{Q\}, \quad \{Q\} s_2 \{R\}}{\{P\} s_1 \circ s_2 \{R\}}$$

Hoare Logic for Loops

The following inference rule holds:

$$\frac{\{P\}s\{P\}, \quad n \geq 0}{\{P\}s^n\{P\}}$$

Proof is by transitivity.
By Expanding Paths condition, we then have:

$$\frac{\{P\}s\{P\}}{\{P\}\bigcup_{n\geq 0} s^n\{P\}}$$

In fact, $\bigcup_{n\geq 0} s^n = s^*$, so we have

$$\frac{\{P\}s\{P\}}{\{P\}s^*\{P\}}$$

This is the rule for non-deterministic loops.

Loops with Conditions

Note that $\{P\}$ *assume*(b) $\{P \cap b_s\}$
Define $\rho(\mathit{while}(b)c) = (\Delta_{b_s} \circ r)^* \circ \Delta_{(\neg b)_s}$ where $r = \rho(c)$.
From the rule for non-deterministic loops we have:

$$\frac{\{P\}\Delta_{b_s} \circ r\{P\}}{\{P\}(\Delta_{b_s} \circ r)*\{P\}}$$

We can thus show:

$$\cfrac{\cfrac{\{P \cap b_s\}\ r\ \{P\}}{\{P\}\ \Delta_{b_s}\ \{P \cap b_s\}\ r\ \{P\}}}{\{P\}\ (\Delta_{b_s} \circ r)^*\ \{P\}\ \Delta_{(\neg b)_s}\ \{P \cap (\neg b)_s\}}$$

i.e.

$$\frac{\{P \cap b_s\}\ r\ \{P\}}{\{P\}\ \underbrace{(\Delta_{b_s} \circ r)^* \circ \Delta_{(\neg b)_s}}_{\rho(\mathit{while}(b)c)}\ \{P \cap (\neg b)_s\}}$$

if we use formulas and commands instead of sets and relations:

$$\frac{\{P \wedge b\}c\{P\}}{\{P\}\mathit{while}(b)c\{P \wedge \neg b\}}$$

Exercise

We call a relation $r \subseteq S \times S$ functional if $\forall x, y, z \in S.(x, y) \in r \wedge (x, z) \in r \rightarrow y = z$. For each of the following statements either give a counterexample or prove it. In the following, $Q \subseteq S$.

(i) for any r, $wp(r, S \setminus Q) = S \setminus wp(r, Q)$

(ii) if r is functional, $wp(r, S \setminus Q) = S \setminus wp(r, Q)$

(iii) for any r, $wp(r, Q) = sp(Q, r^{-1})$

(iv) if r is functional, $wp(r, Q) = sp(Q, r^{-1})$

(v) for any r, $wp(r, Q_1 \cup Q_2) = wp(r, Q_1) \cup wp(r, Q_2)$

(vi) if r is functional, $wp(r, Q_1 \cup Q_2) = wp(r, Q_1) \cup wp(r, Q_2)$

(vii) for any r, $wp(r_1 \cup r_2, Q) = wp(r_1, Q) \cup wp(r_2, Q)$

(viii) Alice has a conjecture: For all sets S and relations $r \subseteq S \times S$ it holds:

$$\Big(S \neq \emptyset \wedge dom(r) = S \wedge \Delta_S \cap r = \emptyset\Big) \rightarrow \Big(r \circ r \cap ((S \times S) \setminus r) \neq \emptyset\Big)$$

where $\Delta_S = \{(x, x) \mid x \in S\}$, $dom(r) = \{x \mid \exists y.(x, y) \in r\}$. She tried many sets and relations and did not find any counterexample. Is her conjecture true? If so, prove it; if false, provide a counterexample for which S is as small as possible.

Properties of Program Contexts

Some Properties of Relations

$$(p_1 \subseteq p_2) \rightarrow (p_1 \circ p) \subseteq (p_2 \circ p)$$

$$(p_1 \subseteq p_2) \rightarrow (p \circ p_1) \subseteq (p \circ p_2)$$

$$(p_1 \subseteq p_2) \wedge (q_1 \subseteq q_2) \quad \rightarrow \quad (p_1 \cup q_1) \subseteq (p_2 \cup q_2)$$

$$(p_1 \cup p_2) \circ q = (p_1 \circ q) \cup (p_2 \circ q)$$

Monotonicity of Expressions using $\cup$ and $\circ$

Consider relations that are subsets of $S \times S$ (i.e. S^2)
The set of all such relations is

$$C = \{r \mid r \subseteq S^2\}$$

Let $E(r)$ be given by any expression built from relation r and some additional relations $b_1, \ldots, b_n$, using $\cup$ and $\circ$.
Example: $E(r) = (b_1 \circ r) \cup (r \circ b_2)$
$E(r)$ is function $C \to C$, maps relations to relations
Claim: E is monotonic function on C:

$$r_1 \subseteq r_2 \to E(r_1) \subseteq E(r_2)$$

Prove of disprove.

Monotonicity of Expressions using $\cup$ and $\circ$

Consider relations that are subsets of $S \times S$ (i.e. S^2)
The set of all such relations is

$$C = \{r \mid r \subseteq S^2\}$$

Let $E(r)$ be given by any expression built from relation r and some additional relations $b_1, \ldots, b_n$, using $\cup$ and $\circ$.
Example: $E(r) = (b_1 \circ r) \cup (r \circ b_2)$
$E(r)$ is function $C \to C$, maps relations to relations
Claim: E is monotonic function on C:

$$r_1 \subseteq r_2 \to E(r_1) \subseteq E(r_2)$$

Prove of disprove.
Proof: induction on the expression tree defining E, using monotonicity properties of $\cup$ and $\circ$