Hoare Logic. Weakest Preconditions, Strongest Postconditions

Viktor Kunčak

About Strength and Weakness

Putting Conditions on Sets Makes them Smaller

Let P_1 and P_2 be formulas ("conditions") whose free variables are among $\bar{x}$. Those variables may denote program state.

When we say "condition P_1 is stronger than condition P_2" it simply means

$$\forall \bar{x}.\ (P_1 \rightarrow P_2)$$

- if we know P_1, we immediately get (conclude) P_2
- if we know P_2 we need not be able to conclude P_1

Stronger condition = smaller set: if P_1 is stronger than P_2 then

$$\{\bar{x} \mid P_1\} \subseteq \{\bar{x} \mid P_2\}$$

- strongest possible condition: "false" $\rightsquigarrow$ smallest set: $\emptyset$
- weakest condition: "true" $\rightsquigarrow$ biggest set: set of all tuples

Hoare Triples

Hoare Logic Example

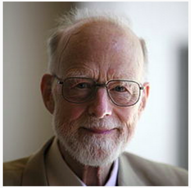
We have seen how to translate programs into relations. We can use these relations in a proof system called Hoare logic. Hoare logic is a way of inserting annotations into code to make proofs about (imperative) program behavior simpler.

Example proof:

```
//{0 <= y}
i = y;
//{0 <= y & i = y}
r = 0;
//{0 <= y & i = y & r = 0}
while //{r = (y−i)*x & 0 <= i}
 (i > 0) (
  //{r = (y−i)*x & 0 < i}
  r = r + x;
  //{r = (y−i+1)*x & 0 < i}
  i = i − 1
  //{r = (y−i)*x & 0 <= i}
)
//{r = x * y}
```

Hoare Triple Definitions

Sir Charles Antony Richard Hoare



Sir Charles Antony Richard Hoare giving a conference at the EPFL on 20 June 2011

Born 11 January 1934

from Wikipedia page *Tony Hoare*

`http://slideshot.epfl.ch/play/suri_hoare`

$P, Q \subseteq S \qquad r \subseteq S \times S$

Hoare Triple:

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

($\{P\}$ and $\{Q\}$ do not denote singleton sets, they are just notation for assertions)

Strongest postcondition:

$$sp(P, r) = \{s' \mid \exists s. s \in P \land (s, s') \in r\}$$

Weakest precondition:

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

Postconditions and Their Strength

What is the relationship between these postconditions?

$$\{x = 5\} \quad x := x + 2 \quad \{\mathbf{x > 0}\}$$

$$\{x = 5\} \quad x := x + 2 \quad \{\mathbf{x = 7}\}$$

Postconditions and Their Strength

What is the relationship between these postconditions?

$$\{x = 5\} \quad x := x + 2 \quad \{\mathbf{x > 0}\}$$

$$\{x = 5\} \quad x := x + 2 \quad \{\mathbf{x = 7}\}$$

- weakest conditions (predicates) correspond to largest sets
- strongest conditions (predicates) correspond to smallest sets

that satisfy a given property.

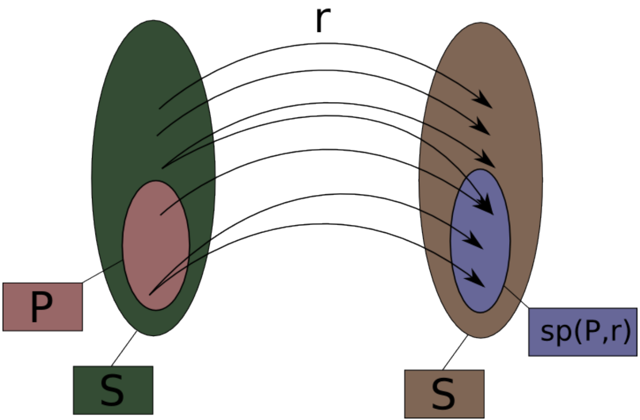
(Graphically, a stronger condition $x > 0 \wedge y > 0$ denotes one quadrant in plane, whereas a weaker condition $x > 0$ denotes the entire half-plane.)

Strongest Postcondition

Definition: For $P \subseteq S$, $r \subseteq S \times S$,

$$sp(P, r) = \{s' \mid \exists s. s \in P \land (s, s') \in r\}$$

This is simply the relation image of a set.

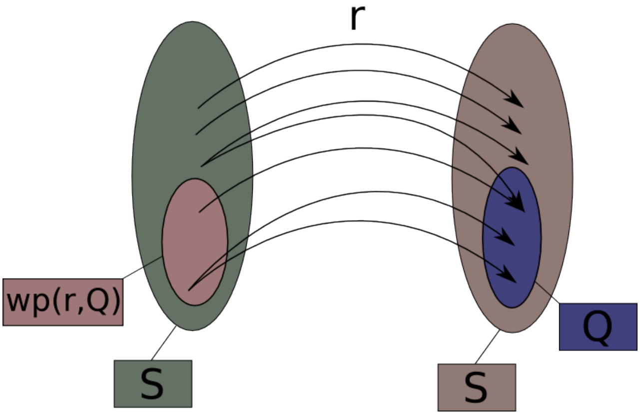


Weakest Precondition

Definition: for $Q \subseteq S$, $r \subseteq S \times S$,

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

Note that this is in general not the same as $sp(Q, r^{-1})$ when the relation is non-deterministic or partial.



Three Forms of Hoare Triple

Lemma: the following three conditions are equivalent:

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

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 $u \notin FV(B)$.