

Activity/Homework: Meanings of Programs; Satisfaction; Trivial Triples

A. Why?

To understand how programs work, we must understand what they mean. To know if a program meets its specification, we have to know when predicates are satisfied.

B. Outcomes

By the end of the activity you should

- Be able to calculate $\mathcal{M}\llbracket S \rrbracket(\sigma)$ for short programs S .
- Be able to check whether or not a predicate is satisfied in a state. (I.e., is $\sigma \models p$?)

C. Questions

We'll do some of these questions as an activity; do the rest as homework.

For the activity, let's do questions 1, 2.

Meanings of Programs

1. If $\sigma_0(x) = 5$ and $\sigma_0(y) = 9$, what is $\mathcal{M}\llbracket x := x+1 ; y := y * x \rrbracket(\sigma_0)$?

Group 6: $\mathcal{M}\llbracket x:=x+1; y:=y^*x \rrbracket(\sigma_0)$

$$= \sigma_0[x := \alpha+1; y := y^*\alpha] \quad \text{where } \alpha = \sigma_0(x)$$

$$= \sigma_0[x := \sigma_0(x)+1; y := y^*\sigma_0(x)]$$

$$= \sigma_0[x := 5+1; y := 9*6]$$

$$= \sigma_0[x := 6; y := 54]$$

$$\mathcal{M}\llbracket x:=6; y:=54 \rrbracket$$

So $\sigma_0[x := \alpha+1; y := y^*\alpha]$ means you're updating twice?

$$\sigma_0[x := \alpha+1][y := y^*\alpha]$$

An update needs to be like $\dots[y := \text{value}]$, not $\dots[y := \text{expr}]$

[I'd write this as;]

$$\mathcal{M}\llbracket x:=x+1; y:=y^*x \rrbracket(\sigma_0) = \{ \sigma_0[x:=6][y:=54] \}$$

$$\mathcal{M}\llbracket x:=x+1; y:=y^*x \rrbracket(\sigma_0)$$

$$= \mathcal{M}\llbracket y:=y^*x \rrbracket(\mathcal{M}\llbracket x:=x+1 \rrbracket(\sigma_0))$$

$$= \mathcal{M}\llbracket y:=y^*x \rrbracket(\{ \sigma_0[x := \sigma_0(x)+1] \})$$

$$= \mathcal{M}\llbracket y:=y^*x \rrbracket(\{ \sigma_0[x := 6] \})$$

$$= \{ \sigma_0[x := 6][y := \sigma_0[x := 6](y^*x)] \}$$

$$= \{ \sigma_0[x := 6][y := 54] \}$$

because

$$\begin{aligned}\sigma_0[x := 6](y * x) &= \sigma_0[x := 6](y) * \sigma_0[x := 6](x) \\ &= \sigma_0(y) * 6 = 9 * 6 = 54\end{aligned}$$

2. For the same σ_0 , what is $\mathcal{M}[y := y * x; x := x + 1](\sigma_0)$?

$$\begin{aligned}\text{Group 5: } \sigma_0[y := \sigma_0(y) * \sigma_0(x)][x := \sigma_0(x) + 1] \\ &= \sigma_0[y := 9 * 5][x := 5 + 1] \\ &= \sigma_0[y := 45][x := 6]\end{aligned}$$

Technically we need curly braces (for singleton set), but again, not a big deal.

3. Let σ_1 be a state and let $S \equiv \text{if } v > w \text{ then } w := w * 2 \text{ else } v := v * 3 \text{ fi}$. What is $\mathcal{M}[S](\sigma_1)$? Note: you'll have two cases, depending on the relationship between $\sigma_1(v)$ and $\sigma_1(w)$. The new values of v and w will involve $\sigma_1(v)$ and $\sigma_1(w)$.

If $\sigma_1(v) > \sigma_1(w)$, then $\mathcal{M}[S](\sigma_1) = \mathcal{M}[w := w * 2](\sigma_1) = \{\sigma_1[w := \sigma_1(w * 2)]\} = \{\sigma_1[w := \sigma_1(w) * 2]\}$. If $\sigma_1(v) \leq \sigma_1(w)$, then $\mathcal{M}[S](\sigma_1) = \mathcal{M}[v := v * 3](\sigma_1) = \{\sigma_1[v := \sigma_1(v) * 3]\}$

4. Let $\Omega \equiv \text{while true do skip od}$. For any σ , what is the sequence of test states (τ_0, τ_1, \dots) for $\mathcal{M}[\Omega](\sigma)$? What set is the value of $\mathcal{M}[\Omega](\sigma)$?

$\tau_0 = \{\sigma\}$ by definition. $\tau_1 = \mathcal{M}[\text{skip}](\tau_0) = \{\tau_0\} = \{\sigma\}$. Similarly, $\tau_2 = \tau_3 = \dots = \{\sigma\}$. So the entire sequence is $\{\sigma\}, \{\sigma\}, \dots$. The value of $\mathcal{M}[\Omega](\sigma) = \emptyset$.

5. Let $W \equiv \text{while } x \neq 0 \text{ do } x := x - 1 \text{ od}$. Let $\sigma'(x) = 3$. What is the sequence of test states for $\mathcal{M}[W](\sigma')$? What is the value of $\mathcal{M}[W](\sigma')$?

$\tau_0 = \{\sigma'\}$; $\tau_1 = \mathcal{M}[x := x - 1](\tau_0) = \{\tau_0[x := \tau_0(x) - 1]\} = \{\tau_0[x := \sigma'(x) - 1]\} = \{\sigma'[x := 2]\}$
 $\tau_2 = \mathcal{M}[x := x - 1](\tau_1) = \{\tau_1[x := \tau_1(x) - 1]\} = \{\tau_1[x := \sigma'[x := 2](x) - 1]\} = \{\sigma'[x := 1]\}$
 Similarly, $\tau_3 = \{\sigma'[x := 0]\}$. Since $\tau_3 \models x = 0$, we get $\mathcal{M}[W](\sigma') = \{\tau_3\}$

6. Let $\sigma''(x) = -4$. What is the sequence of test states for $\mathcal{M}[W](\sigma'')$? [Same W as in the previous question.] What is the value of $\mathcal{M}[W](\sigma'')$?

For all states σ , $\mathcal{M}[x := x - 1](\sigma) = \{\sigma[x := \sigma(x) - 1]\} = \{\sigma[x := \sigma(x) - 1]\}$

$\tau_0 = \{\sigma''\}$, $\tau_1 = \{\tau_0[x := \tau_0(x) - 1]\} = \{\sigma''[x := -5]\}$. Continuing, τ_2 maps x to -6 , τ_3 maps x to -7 , ..., and none of these satisfy $x = 0$, so $\mathcal{M}[W](\sigma'') = \emptyset$.

Predicate Satisfaction

7. Give an example of a state that $\models 0 < m < n$. Also, give an example of a state that $\not\models 0 < m < n$. (The state should be “proper” — define type-correct values for m and n — even though those values don't satisfy $0 < m < n$.)

- (a) a state that maps m to 2 and n to 3
- (b) a state that maps m to 2 and n to 1

8. For an existential, $\sigma \models \exists x \in T . p$ iff there's some value (of type T) for x that makes σ updated at x with α satisfy p . E.g., $\sigma \models \exists x . x^2 < 1$ (where x ranges over the integers); we can use 0 for the “witness” α and find $\sigma[x := 0] \models x^2 < 1$. In general, it's possible to have many witnesses. What are the possible witnesses α that can be used to show $\sigma \models \exists x . x^2 > 1$?

If x has the value 2 (so $\alpha = 2$), then $\sigma[x:=\alpha] = \sigma[x:=2] \models x^2 > 1$ because in $\sigma[x:=2]$, x^2 has the value 4.

9. If we have a set of states X , then “ X satisfies p ” (written $X \models p$) means that every state in X satisfies p . (And if $X = \emptyset$, then $X \models p$ automatically.) Now, in general, $\sigma \models p \rightarrow q$ iff $\sigma \models p$ implies that $\sigma \models q$. Question: Say $\sigma \models p \rightarrow q$ for all states σ . If $X \models p$, then does $X \models q$ also?

Definition: If we have a set of states X , then “ X satisfies p ” (written $X \models p$) means that every state in X satisfies p . (And if $X = \emptyset$, then $X \models p$ automatically.)

Definition: $\sigma \models p \rightarrow q$ iff $\sigma \models p$ implies that $\sigma \models q$.

Suppose we have an implication $p \rightarrow q$ that is satisfied in all states. If X is a set of states and $X \models p$, then is $X \models q$?

Yes: $X \models q$ means for all $\sigma \in X$, we have $\sigma \models q$. For each of those σ , since $\sigma \in X$, we know $\sigma \models p$. Since σ also $\models p \rightarrow q$, we have that $\sigma \models q$.

Trivial Partial Correctness Triples

10. Remember, $\sigma \models \{p\} S \{q\}$ iff $(\sigma \not\models p)$ or $(M[S](\sigma) = \emptyset)$ or $M[S](\sigma) \models q$. There are three cases in which $\sigma \models \{p\} S \{q\}$ kind of trivially:

- (a) When $\sigma \not\models p$ for every σ .
- (b) When $M[S](\sigma) = \emptyset$ for every σ .
- (c) When $\tau \models q$ for every state τ (because then the ones $\in M[S](\sigma)$ must $\models q$ too).

Give an example of a p that fits case (a). Give an example of an S that fits case (b).

Give an example of a q that fits case (c).

(a) false

(b) The program S is `while true do skip od` [always goes into an infinite loop]

(c) true

So all triples of the form $\{\text{false}\}$ any statement $\{\text{any postcondition}\}$ is always satisfied

Also triples of the form $\{p\}$ always infinite loop $\{q\}$

Also triples of the form $\{p\} S \{\text{true}\}$