Reasoning About Programs

Week 6 PMT - Method Calls
To discuss during PMT - do NOT hand in

Sophia Drossopoulou and Mark Wheelhouse

1st Question:

Consider the following Java methods:

```
1   int sqrt(int x){
2   // PRE: x ≥ 0                                   (P1)
3   // POST: r = ⌊√x⌋                               (Q1)
4       ...
5   }
6
7   void rootSome(int[] a){
8   // PRE: a ≠ null ∧ a.length ≥ 3 ∧ ∀i∈ℕ.[ 0 ≤ i < a.length ⟶ a[i] ≥ 0 ]   (P2)
9   // POST: ∀i∈ℕ.[ 0 ≤ i < 3 ⟶ a[i] = ⌊√a0[i]⌋ ]                            (Q2)
10      // MID: M1
11      a[0] = sqrt(a[0]);
12      // MID: M2
13      a[1] = sqrt(a[1]);
14      // MID: M3
15      a[2] = sqrt(a[2]);
16      // MID: M4
17  }
```

Note that whilst we know the specification of `sqrt`, we do not know its implementation.

a) Add mid-conditions M_1, M_2, M_3 and M_4 which are strong enough to prove that the `rootSome` method satisfies its specification.

b) Construct **all** of the proof obligations that would be required to prove that the method satisfies its specification.

c) Prove all of your obligations from part (b).

A possible answer:

a)

$$
\begin{aligned}
M_1 \;&\longleftrightarrow\; \texttt{a.length} \geq 3 \;\wedge\; \forall i{\in}\mathbb{N}.[\; 0 \leq i < \texttt{a.length} \longrightarrow \texttt{a}[i] \geq 0 \;] \;\wedge\; \texttt{a} \approx \texttt{a}_0 \\
M_2 \;&\longleftrightarrow\; \texttt{a.length} \geq 3 \;\wedge\; \forall i{\in}\mathbb{N}.[\; 0 \leq i < \texttt{a.length} \longrightarrow \texttt{a}[i] \geq 0 \;] \\
&\quad\wedge\; \forall i{\in}\mathbb{N}.[\; 0 \leq i < 1 \longrightarrow \texttt{a}[i] = \left\lfloor \sqrt{\texttt{a}_0[i]} \right\rfloor \;] \;\wedge\; \forall i{\in}\mathbb{N}.[\; 1 \leq i < \texttt{a.length} \longrightarrow \texttt{a}[i] = \texttt{a}_0[i] \;] \\
M_3 \;&\longleftrightarrow\; \texttt{a.length} \geq 3 \;\wedge\; \forall i{\in}\mathbb{N}.[\; 0 \leq i < \texttt{a.length} \longrightarrow \texttt{a}[i] \geq 0 \;] \\
&\quad\wedge\; \forall i{\in}\mathbb{N}.[\; 0 \leq i < 2 \longrightarrow \texttt{a}[i] = \left\lfloor \sqrt{\texttt{a}_0[i]} \right\rfloor \;] \;\wedge\; \forall i{\in}\mathbb{N}.[\; 2 \leq i < \texttt{a.length} \longrightarrow \texttt{a}[i] = \texttt{a}_0[i] \;] \\
M_4 \;&\longleftrightarrow\; \texttt{a.length} \geq 3 \;\wedge\; \forall i{\in}\mathbb{N}.[\; 0 \leq i < \texttt{a.length} \longrightarrow \texttt{a}[i] \geq 0 \;] \\
&\quad\wedge\; \forall i{\in}\mathbb{N}.[\; 0 \leq i < 3 \longrightarrow \texttt{a}[i] = \left\lfloor \sqrt{\texttt{a}_0[i]} \right\rfloor \;] \;\wedge\; \forall i{\in}\mathbb{N}.[\; 3 \leq i < \texttt{a.length} \longrightarrow \texttt{a}[i] = \texttt{a}_0[i] \;]
\end{aligned}
$$

b) In our substitution notation the proof obligations are:

line 10: Show that the precondition of `rootSome` establishes the midcondition M_1:
$P_2[\texttt{a} \mapsto \texttt{a}_0] \;\wedge\; \texttt{a} \approx \texttt{a}_0 \;\longrightarrow\; M_1$

line 11: Show that the midcondition M_1 establishes the precondition for `sqrt`:
$M_1 \;\longrightarrow P_1[\texttt{x} \mapsto \texttt{a}[0]]$

line 12: Show that the postcondition of `sqrt` establishes the midcondition M_2:
$Q_1[\texttt{x} \mapsto \texttt{a}[0]] \;\wedge\; M_1 \;\wedge\; \forall i{\in}\mathbb{N}.[\; 0 \leq i < \texttt{a.length} \wedge\, \texttt{i} \neq 0 \longrightarrow \texttt{a}'[i] = \texttt{a}[i] \;] \;\wedge\; \texttt{a}'[0] = \mathbf{r}$
$\longrightarrow\; M_2[\texttt{a} \mapsto \texttt{a}']$

line 13: Show that the midcondition M_2 establishes the precondition for `sqrt`:
$M_2 \;\longrightarrow P_1[\texttt{x} \mapsto \texttt{a}[1]]$

line 14: Show that the postcondition of `sqrt` establishes the midcondition M_3:
$Q_1[\texttt{x} \mapsto \texttt{a}[1]] \;\wedge\; M_2 \;\wedge\; \forall i{\in}\mathbb{N}.[\; 0 \leq i < \texttt{a.length} \wedge\, \texttt{i} \neq 1 \longrightarrow \texttt{a}'[i] = \texttt{a}[i] \;] \;\wedge\; \texttt{a}'[1] = \mathbf{r}$
$\longrightarrow\; M_3[\texttt{a} \mapsto \texttt{a}']$

line 15: Show that the midcondition M_3 establishes the precondition for `sqrt`:
$M_3 \;\longrightarrow P_1[\texttt{x} \mapsto \texttt{a}[2]]$

line 16: Show that the postcondition of `sqrt` establishes the midcondition M_4:
$Q_1[\texttt{x} \mapsto \texttt{a}[2]] \;\wedge\; M_3 \;\wedge\; \forall i{\in}\mathbb{N}.[\; 0 \leq i < \texttt{a.length} \wedge\, \texttt{i} \neq 2 \longrightarrow \texttt{a}'[i] = \texttt{a}[i] \;] \;\wedge\; \texttt{a}'[2] = \mathbf{r}$
$\longrightarrow\; M_4[\texttt{a} \mapsto \texttt{a}']$

line 17: Show that the midcondition M_4 establishes the postcondition of `rootSome`:
$M_4 \;\longrightarrow\; Q_2$

rootSome: Show that all array access are legal:

i) **line 11:** $M_1 \;\longrightarrow\; 0 \leq 0 < \texttt{a.length}$

ii) **line 13:** $M_2 \;\longrightarrow\; 0 \leq 1 < \texttt{a.length}$

iii) **line 15:** $M_3 \;\longrightarrow\; 0 \leq 2 < \texttt{a.length}$

Note that the proof obligations for lines 12, 14 and 16 explicitly state that the elements of `a` are unmodified except for those assigned to by the code at each step. Also, because arrays are passed by reference, we do not have to make any substitutions for `a` in the postcondition Q_2 on line 17.

These substitutions can be unfolded into the following full logical assertions:

line 10: Show that the precondition of `rootSome` establishes the midcondition M_1:

$$\begin{array}{c} \mathtt{a}_0 \neq \mathtt{null} \ \wedge \ \mathtt{a}_0\mathtt{.length} \geq 3 \ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < \mathtt{a}_0\mathtt{.length} \longrightarrow \mathtt{a}_0[i] \geq 0\ ] \ \wedge \ \mathtt{a} \approx \mathtt{a}_0 \\ \longrightarrow \\ \mathtt{a.length} \geq 3 \ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ] \ \wedge \ \mathtt{a} \approx \mathtt{a}_0 \end{array}$$

line 11: Show that the midcondition M_1 establishes the precondition for `sqrt`:

$$\begin{array}{c} \mathtt{a.length} \geq 3 \ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ] \ \wedge \ \mathtt{a} \approx \mathtt{a}_0 \\ \longrightarrow \\ \mathtt{a}[0] \geq 0 \end{array}$$

line 12: Show that the postcondition of `sqrt` establishes the midcondition M_2:

$$\begin{array}{c} \mathbf{r} = \left\lfloor \sqrt{\mathtt{a}[0]} \right\rfloor \\ \wedge \ \mathtt{a.length} \geq 3 \ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ] \ \wedge \ \mathtt{a} \approx \mathtt{a}_0 \\ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \wedge \mathtt{i} \neq 0 \longrightarrow \mathtt{a}'[i] = \mathtt{a}[i]\ ] \ \wedge \ \mathtt{a}'[0] = \mathbf{r} \\ \longrightarrow \\ \mathtt{a}'\mathtt{.length} \geq 3 \ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < \mathtt{a}'\mathtt{.length} \longrightarrow \mathtt{a}'[i] \geq 0\ ] \\ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < 1 \longrightarrow \mathtt{a}'[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ] \ \wedge \ \forall i{\in}\mathbb{N}.[\ 1 \leq i < \mathtt{a}'\mathtt{.length} \longrightarrow \mathtt{a}'[i] = \mathtt{a}_0[i]\ ] \end{array}$$

line 13: Show that the midcondition M_2 establishes the precondition for `sqrt`:

$$\begin{array}{c} \mathtt{a.length} \geq 3 \ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ] \\ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < 1 \longrightarrow \mathtt{a}[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ] \ \wedge \ \forall i{\in}\mathbb{N}.[\ 1 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] = \mathtt{a}_0[i]\ ] \\ \longrightarrow \\ \mathtt{a}[1] \geq 0 \end{array}$$

line 14: Show that the postcondition of `sqrt` establishes the midcondition M_3:

$$\begin{array}{c} \mathbf{r} = \left\lfloor \sqrt{\mathtt{a}[1]} \right\rfloor \\ \wedge \ \mathtt{a.length} \geq 3 \ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ] \\ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < 1 \longrightarrow \mathtt{a}[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ] \ \wedge \ \forall i{\in}\mathbb{N}.[\ 1 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] = \mathtt{a}_0[i]\ ] \\ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \wedge \mathtt{i} \neq 1 \longrightarrow \mathtt{a}'[i] = \mathtt{a}[i]\ ] \ \wedge \ \mathtt{a}'[1] = \mathbf{r} \\ \longrightarrow \\ \mathtt{a}'\mathtt{.length} \geq 3 \ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < \mathtt{a}'\mathtt{.length} \longrightarrow \mathtt{a}'[i] \geq 0\ ] \\ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < 2 \longrightarrow \mathtt{a}'[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ] \ \wedge \ \forall i{\in}\mathbb{N}.[\ 2 \leq i < \mathtt{a}'\mathtt{.length} \longrightarrow \mathtt{a}'[i] = \mathtt{a}_0[i]\ ] \end{array}$$

line 15: Show that the midcondition M_3 establishes the precondition for `sqrt`:

$$\begin{array}{c} \mathtt{a.length} \geq 3 \ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ] \\ \wedge \ \forall i{\in}\mathbb{N}.[\ 0 \leq i < 2 \longrightarrow \mathtt{a}[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ] \ \wedge \ \forall i{\in}\mathbb{N}.[\ 2 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] = \mathtt{a}_0[i]\ ] \\ \longrightarrow \\ \mathtt{a}[2] \geq 0 \end{array}$$

line 16: Show that the postcondition of `sqrt` establishes the midcondition M_4:

$$\begin{gathered}
\mathbf{r} = \left\lfloor \sqrt{\mathtt{a}[2]} \right\rfloor \\
\wedge\ \mathtt{a.length} \geq 3\ \wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ] \\
\wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < 2 \longrightarrow \mathtt{a}[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ]\ \wedge\ \forall i \in \mathbb{N}.[\ 2 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] = \mathtt{a}_0[i]\ ] \\
\wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \wedge \mathtt{i} \neq 2 \longrightarrow \mathtt{a}'[i] = \mathtt{a}[i]\ ]\ \wedge\ \mathtt{a}'[1] = \mathbf{r} \\
\longrightarrow \\
\mathtt{a}'\mathtt{.length} \geq 3\ \wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < \mathtt{a}'\mathtt{.length} \longrightarrow \mathtt{a}'[i] \geq 0\ ] \\
\wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < 3 \longrightarrow \mathtt{a}'[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ]\ \wedge\ \forall i \in \mathbb{N}.[\ 3 \leq i < \mathtt{a}'\mathtt{.length} \longrightarrow \mathtt{a}'[i] = \mathtt{a}_0[i]\ ]
\end{gathered}$$

line 17: Show that the midcondition M_4 establishes the postcondition of `rootSome`:

$$\begin{gathered}
\mathtt{a.length} \geq 3\ \wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ] \\
\wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < 3 \longrightarrow \mathtt{a}[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ]\ \wedge\ \forall i \in \mathbb{N}.[\ 3 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] = \mathtt{a}_0[i]\ ] \\
\longrightarrow \\
\forall i \in \mathbb{N}.[\ 0 \leq i < 3 \longrightarrow \mathtt{a}[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ]
\end{gathered}$$

rootSome: Show that all array access are legal:

i)

$$\begin{gathered}
\mathtt{a.length} \geq 3\ \wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ]\ \wedge\ \mathtt{a} \approx \mathtt{a}_0 \\
\longrightarrow \\
0 \leq 0 < \mathtt{a.length}
\end{gathered}$$

ii)

$$\begin{gathered}
\mathtt{a.length} \geq 3\ \wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ] \\
\wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < 1 \longrightarrow \mathtt{a}[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ]\ \wedge\ \forall i \in \mathbb{N}.[\ 1 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] = \mathtt{a}_0[i]\ ] \\
\longrightarrow \\
0 \leq 1 < \mathtt{a.length}
\end{gathered}$$

iii)

$$\begin{gathered}
\mathtt{a.length} \geq 3\ \wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ] \\
\wedge\ \forall i \in \mathbb{N}.[\ 0 \leq i < 2 \longrightarrow \mathtt{a}[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ]\ \wedge\ \forall i \in \mathbb{N}.[\ 2 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] = \mathtt{a}_0[i]\ ] \\
\longrightarrow \\
0 \leq 2 < \mathtt{a.length}
\end{gathered}$$

c) Proving the majority of the above assertions is relatively straight-forward. The cases where we have to reason about the effect of the method calls are the trickiest, so as an example we shall give the full proof for line 14 below. The remaining proofs are left as an exercise, but should follow the same format.

line 14: Show that the postcondition of `sqrt` establishes the midcondition M_3:

Given:

(1)	$\mathbf{r} = \left\lfloor \sqrt{\mathtt{a}[1]} \right\rfloor$	from Q_1
(2)	$\mathtt{a.length} \geq 3$	from M_2
(3)	$\forall i \in \mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] \geq 0\ ]$	from M_2
(4)	$\forall i \in \mathbb{N}.[\ 0 \leq i < 1 \longrightarrow \mathtt{a}[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ]$	from M_2
(5)	$\forall i \in \mathbb{N}.[\ 1 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}[i] = \mathtt{a}_0[i]\ ]$	from M_2
(6)	$\forall i \in \mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \wedge \mathtt{i} \neq 1 \longrightarrow \mathtt{a}'[i] = \mathtt{a}[i]\ ]$	implicit from code
(7)	$\mathtt{a}'[1] = \mathbf{r}$	from code line 13

To show:

(α)	$\mathtt{a}'\mathtt{.length} \geq 3$
(β)	$\forall i \in \mathbb{N}.[\ 0 \leq i < \mathtt{a}'\mathtt{.length} \longrightarrow \mathtt{a}'[i] \geq 0\ ]$
(γ)	$\forall i \in \mathbb{N}.[\ 0 \leq i < 2 \longrightarrow \mathtt{a}'[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ]$
(δ)	$\forall i \in \mathbb{N}.[\ 2 \leq i < \mathtt{a}'\mathtt{.length} \longrightarrow \mathtt{a}'[i] = \mathtt{a}_0[i]\ ]$

Proof:

(8)	$\mathtt{a}'\mathtt{.length} = \mathtt{a.length}$	from (6) and (7)
(α)	follows from (2) and (8)	
(9)	$1 < \mathtt{a.length}$	from (2)
(10)	$\mathtt{a}[1] = \mathtt{a}_0[1]$	from (5) and (9)
(11)	$\mathtt{a}'[1] = \left\lfloor \sqrt{\mathtt{a}[1]} \right\rfloor$	from (7) and (1)
(12)	$\mathtt{a}'[1] = \left\lfloor \sqrt{\mathtt{a}_0[1]} \right\rfloor$	from (11) and (10)
(13)	$\mathtt{a}[1] \geq 0$	from (3) and (9)
(14)	$\mathtt{a}'[1] \geq 0$	from (11) and (13)
(15)	$\forall i \in \mathbb{N}.[\ 0 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}'[i] \geq 0\ ]$	from (3), (6) and (14)
(α)	follows from (15) and (8)	
(16)	$\forall i \in \mathbb{N}.[\ 0 \leq i < 1 \longrightarrow \mathtt{a}'[i] = \left\lfloor \sqrt{\mathtt{a}_0[i]} \right\rfloor\ ]$	from (4) and (6)
(γ)	follows from (16) and (12)	
(17)	$\forall i \in \mathbb{N}.[\ 2 \leq i < \mathtt{a.length} \longrightarrow \mathtt{a}'[i] = \mathtt{a}_0[i]\ ]$	from (5) and (6)
(δ)	follows from (17) and (8)	