# Solutions to exercises for the *Hoare logic*

(based on material written by Mark Staples)

**Exercise 1**

We are interested in termination, so that means we need to use the terminology of *total correctness*, i.e. we need to use the square brackets. Assuming that the question means that the program should terminate on every input, then we to have a precondition which is true of every input. The condition $T$ will do for that. We can make the postcondition any true thing, so we could just use $T$ again. However, note that to escape the loop the guard must be false, so we can equally well say

$$[T]\ \mathtt{C}\ [\mathtt{X} \leq 1]$$

**Exercise 2**

The only possibility of non-termination is the while loop. The guard involves variables `R` and `Y`, and the body of the loop only affects the value of `R`. First note that if $\mathtt{Y} = 0$, then if we get into the body of the loop, the value of `R` never changes, so we need initially, at least

$$(\mathtt{Y} \leq \mathtt{X}) \Rightarrow (\mathtt{Y} \neq 0)$$

If `Y` is negative, then in the body of the loop, `R` will always increase. If we enter the loop, we will never leave it. So, we need that initially

$$\mathtt{Y} < 0 \Rightarrow \mathtt{X} < \mathtt{Y}$$

There are no problems with the last case — If `Y` is positive, then `R` will always decrease, until it is less than `Y`. Certainly the loop will terminate, and the postcondition will even be satisfied if `X` is negative.

So, a condition $P$ which would work is $\mathtt{Y} > 0$. This is stronger than we need, but nonetheless satisfies the two conditions noted above.

**Exercise 3**

$[T]$ `C` $[T]$ is true when `C` terminates for every possible value of its state variables. This specification says nothing about the behaviour of `C` — it could have done anything to its program variables after some finite time.

**Exercise 4**

The intention of the question here is perhaps unclear. The specifier may mean:

$$\{\texttt{X = x}\}\ \texttt{C}\ \{\texttt{X = x}\times\texttt{Y}\}$$

or, may have intended that `Y` doesn't change. That would be represented by the stronger specification:

$$\{\texttt{X = x} \wedge \texttt{Y = y}\}\ \texttt{C}\ \{\texttt{X = x}\times\texttt{Y} \wedge \texttt{Y = y}\}$$

**Exercise 5**

$[P]$ `C` $[T]$ is true when `C` is guaranteed to halt when starting in a state satisfying $P$.

**Exercise 6**

The flaw is in the step from line 5 to 6. $\sqrt{}$ is a relation rather than a function: $\sqrt{1}$ is equal to two values:, 1 and $-1$, so the last line could correctly read $-1 = 1 \vee 1 = 1$.

**Exercise 7**

It is true. Working backwards through the command sequence, using the Sequential Composition rule and Assignment Axiom, we get a proof tree:

$$\dfrac{\begin{array}{c}\{\texttt{X} = x \wedge \texttt{Y} = y\}\ \texttt{X:=X+Y}\ \{(\texttt{X} - \texttt{Y}) = x \wedge (\texttt{X} - (\texttt{X} - \texttt{Y})) = y\},\\ \{(\texttt{X} - \texttt{Y}) = x \wedge (\texttt{X} - (\texttt{X} - \texttt{Y})) = y\}\ \texttt{Y:=X-Y}\ \{\texttt{Y} = x \wedge (\texttt{X} - \texttt{Y}) = y\},\\ \{\texttt{Y} = x \wedge (\texttt{X} - \texttt{Y}) = y\}\ \texttt{X:=X-Y}\ \{\texttt{Y} = x \wedge \texttt{X} = y\}\end{array}}{\{\texttt{X} = x \wedge \texttt{Y} = y\}\ \texttt{X:=X+Y; Y:=X-Y; X:=X-Y}\ \{\texttt{Y} = x \wedge \texttt{X} = y\}}\ \text{Derived Seq Comp}$$

The second two antecedents are instances of the assignment axiom. (In fact, to get them, you can start from the postcondition, and work backwards through the assignment statements, deriving the mid conditions.) The first antecedent provable from the assignment axiom and the Precondition Strengthening rule:

$$\dfrac{\begin{array}{c}(\texttt{X} = x \wedge \texttt{Y} = y) \Rightarrow (((\texttt{X} + \texttt{Y}) - \texttt{Y}) = x \wedge ((\texttt{X} + \texttt{Y}) - ((\texttt{X} + \texttt{Y}) - \texttt{Y})) = y),\\ \{\texttt{X} = x \wedge \texttt{Y} = y\}\ \texttt{X:=X+Y}\ \{(\texttt{X} - \texttt{Y}) = x \wedge (\texttt{X} - (\texttt{X} - \texttt{Y})) = y\}\end{array}}{\{\texttt{X} = x \wedge \texttt{Y} = y\}\ \texttt{X:=X+Y}\ \{(\texttt{X} - \texttt{Y}) = x \wedge (\texttt{X} - (\texttt{X} - \texttt{Y})) = y\}}\ \text{Precondition Str.}$$

The logical condition follows from arithmetic.

Note that here the derived precondition is *equal* to the given precondition. The Precondition Strengthening rule certainly applies, as equivalent propositions imply each other. However, here we could have instead just replace 'equals-for-equals' directly and avoided the use of the Precondition Strengthening rule.

## Exercise 8

We start with the following portion of the derivation (working backwards from the last line, ending up with the top two conditions):

$$\frac{\{\texttt{X} = \texttt{R} + \texttt{Y} * \texttt{Q}\}\ \texttt{R := R-Y}\ \{Mid\} \qquad \{Mid\}\ \texttt{Q := Q+1}\ \{\texttt{X} = \texttt{R} + \texttt{Y} * \texttt{Q}\}}{\{\texttt{X} = \texttt{R} + \texttt{Y} * \texttt{Q}\}\ \texttt{R := R-Y; Q := Q+1}\ \{\texttt{X} = \texttt{R} + \texttt{Y} * \texttt{Q}\}}\ \text{Seq Comp}$$

Now we have to find a condition $Mid$ which satisfies both of the assignment Hoare-triples. Find $Mid$ using the Assignment Rule on the second assignment, as $\{Post[E/V]\}$ `V:=E` $\{Post\}$, here

$$Post = \texttt{X} = \texttt{R} + \texttt{Y} * \texttt{Q}$$

so here

$$Mid = Post[Q + 1/Q]$$

i.e.

$$Mid = \texttt{X} = \texttt{R} + \texttt{Y} * (\texttt{Q} + \texttt{1})$$

We use this condition as the postcondition to the first assignment, so we need to prove

$$\{\texttt{X} = \texttt{R} + \texttt{Y} * \texttt{Q}\}\ \texttt{R := R-Y}\ \{\texttt{X} = \texttt{R} + \texttt{Y} * (\texttt{Q} + \texttt{1})\}$$

We can do this by appealing to the Assignment Rule, and the Precondition Strengthening Rule. The Assignment Axiom shows us that we need a precondition

$$(\texttt{X} = \texttt{R} + \texttt{Y} * (\texttt{Q} + \texttt{1}))[R - Y/R]$$

i.e.

$$\texttt{X} = \texttt{R} - \texttt{Y} + \texttt{Y} * (\texttt{Q} + \texttt{1})$$

In fact, this is by arithmetic *equal* to our given precondition, so we don't need to use the Precondition Strengthening rule — we can just substitute equals for equals to finish the proof.

## Exercise 9

The Conditional rule gives use two proof obligations:

$$\frac{\{X \geq \texttt{Y}\}\ \texttt{MAX := X}\ \{\texttt{MAX} = max(\texttt{X}, \texttt{Y})\} \quad \{\texttt{X} < \texttt{Y}\}\ \texttt{MAX := Y}\ \{\texttt{MAX} = max(\texttt{X}, \texttt{Y})\}}{\{T\}\ \texttt{IF X} \geq \texttt{Y THEN MAX := X ELSE MAX := Y}\ \{\texttt{MAX} = max(\texttt{X}, \texttt{Y})\}}\ \text{Conditional}$$

They are each proven in the same way. Let's start with the first:

$$\frac{X \geq \texttt{Y} \Rightarrow (\texttt{X} = max(\texttt{X}, \texttt{Y})) \quad \dfrac{}{\{\texttt{X} = max(\texttt{X}, \texttt{Y})\}\ \texttt{MAX := X}\ \{\texttt{MAX} = max(\texttt{X}, \texttt{Y})\}}\ \text{Assignment Axiom}}{\{X \geq \texttt{Y}\}\ \texttt{MAX := X}\ \{\texttt{MAX} = max(\texttt{X}, \texttt{Y})\}}\ \text{Precondition Str.}$$

The condition above is just our given fact `(i)` about *max*. Note that I didn't just randomly guess the right-hand side of the implication — it is the same as the precondition of the assignment condition, and that can be derived by performing the assignment substitution on the postcondition.

The other branch of the conditional is similar, but instead eventually depending upon our given fact `(ii)` about *max*:

$$\dfrac{X < \mathtt{Y} \Rightarrow (\mathtt{Y} = max(\mathtt{X},\mathtt{Y})) \quad \dfrac{}{\{\mathtt{Y} = max(\mathtt{X},\mathtt{Y})\}\ \mathtt{MAX\ :=\ X}\ \{\mathtt{MAX} = max(\mathtt{X},\mathtt{Y})\}}\ \text{Assignment Axiom}}{\{X \geq \mathtt{Y}\}\ \mathtt{MAX\ :=\ X}\ \{\mathtt{MAX} = max(\mathtt{X},\mathtt{Y})\}}\ \text{Precondition Str.}$$

**Exercise 10**

The given rule covers case (iii) of the informal evaluation description, but not case (ii). This can be seen by looking at the hint case, which is (wrongly) accepted by the given rule. In the hint case, we get the condition

$$\{\mathtt{X} = 0 \wedge \mathtt{X} = 1\}\ \mathtt{Y\ :=\ 0}\ \{\mathtt{Y} = 0\}$$

The precondition is $F$, which can be transformed, using the Precondition Strengthening rule, into anything. (As $F \Rightarrow Q$ for any $Q$.) In particular, it can be transformed into $0 = 0$, which make the condition an instance of the Assignment Axiom.

**Exercise 11**

We need to strengthen the Case Rule. We can do this by adding an extra antecedent:

$$\dfrac{..,\vdash P \Rightarrow ((0 < E \leq n) \vee Q)}{\{P\}\ \mathtt{CASE\ \ldots\ \ END}\ \{Q\}}\ \text{Case Rule}$$

This is logically equivalent to

$$\vdash (P \wedge (0 \geq E \vee E > n)) \Rightarrow Q)$$

Using this corrected rule, we can show, where

$$\begin{aligned} PRE &\ \widehat{=}\ 1 \leq \mathtt{X} \leq 3 \\ POST &\ \widehat{=}\ \mathtt{Y} = 0 \\ C &\ \widehat{=}\ \mathtt{CASE\ X\ OF\ BEGIN\ Y:=\ X-1;\ Y\ :=\ X-2;\ Y\ :=\ X-3\ END} \end{aligned}$$

that:

$$\dfrac{\begin{array}{c}\{PRE \wedge \mathtt{X} = 1\}\ \mathtt{Y\ :=\ X-1}\ \{POST\} \\ \{PRE \wedge \mathtt{X} = 2\}\ \mathtt{Y\ :=\ X-2}\ \{POST\} \\ \{PRE \wedge \mathtt{X} = 3\}\ \mathtt{Y\ :=\ X-3}\ \{POST\} \\ (0 \leq \mathtt{X} \leq 3) \Rightarrow ((0 \leq \mathtt{X} \leq 3) \vee POST)\end{array}}{\{PRE\}\ C\ \{POST\}}\ \text{Case Rule}$$

The first condition follows as below:

$$\dfrac{\dfrac{\mathtt{X}=1 \Rightarrow \mathtt{X}-1=0}{(\mathit{PRE} \wedge \mathtt{X}=1) \Rightarrow (\mathit{POST}[\mathtt{X}-1/\mathtt{Y}])} \quad \dfrac{}{\{\mathit{POST}[\mathtt{X}-1/Y\}\ \mathtt{Y\ :=\ X-1}\ \{\mathit{POST}\}}\ \text{Assign Axiom}}{\{\mathit{PRE} \wedge X=1\}\ \mathtt{Y\ :=\ X-1}\ \{\mathit{POST}\}}\ \text{Precondition Str.}$$

The other assignment conditions follow similarly. The last condition follows trivially by logic.

**Exercise 12**

We are given that

$$\mathtt{REPEAT\ C\ UNTIL\ S} \equiv \mathtt{C;\ WHILE\ \neg S\ DO\ C}$$

So, we can derive a rule for the Repeat command:

$$\dfrac{\{P\}\ \mathtt{C}\ \{Q\} \quad \dfrac{\{Q \wedge \neg S\}\ \mathtt{C}\ \{Q\}}{\{Q\}\ \mathtt{WHILE\ \neg S\ DO\ C}\ \{Q \wedge S\}}\ \text{While Rule}}{\{P\}\ \mathtt{C;\ WHILE\ \neg S\ DO\ C}\ \{Q \wedge S\}}\ \text{Sequential Comp. Rule}$$

So, we have derived:

$$\dfrac{\{P\}\ \mathtt{C}\ \{Q\} \quad \{Q \wedge \neg S\}\ \mathtt{C}\ \{Q\}}{\{P\}\ \mathtt{REPEAT\ C\ UNTIL\ S}\ \{Q \wedge S\}}\ \text{Repeat Rule}$$