Exercises for which solution notes are available

Exercise 1
Write a specification which is true if and only if the following program terminates.

\[\text{WHILE } X > 1 \text{ DO IF ODD}(X) \text{ THEN } X := (3 \times X) + 1 \text{ ELSE } X := X \text{ DIV } 2\]

Exercise 2
Let \(C\) be the following command
\[
R := X; \\
Q := 0; \\
\text{WHILE } Y \leq R \text{ DO } (R := R - Y; Q := Q + 1)
\]
Find a condition \(P\) such that \([P] \quad C \quad [R < Y \land X = R + (Y \times Q)]\) is true.

Exercise 3
When is \([T] \quad C \quad [T]\) true?

Exercise 4
Write a partial correctness specification which is true if and only if the command \(C\) has the effect of multiplying the values of \(X\) and \(Y\) and storing the result in \(X\).

Exercise 5
Write a specification which is true if the execution of \(C\) always halts when execution is started in a state satisfying \(P\).

Exercise 6
Find the flaw in the ‘proof’ of \(1 = -1\) below:
1. \(\sqrt{-1 \times -1} = \sqrt{-1} \times \sqrt{-1}\) Reflexivity of =.
2. \(\sqrt{-1 \times -1} = (\sqrt{-1}) \times (\sqrt{-1})\) Distributive law of \(\sqrt{}\) over \(\times\).
3. \(\sqrt{-1 \times -1} = (\sqrt{-1})^2\) Definition of \((\cdot)^2\).
4. \(\sqrt{-1 \times -1} = -1\) definition of \(\sqrt{}\).
5. \(\sqrt{1} = -1\) As \(-1 \times -1 = 1\).
6. \(1 = -1\) As \(\sqrt{1} = 1\).

Exercise 7
Is the following specification true?
\[\vdash \{X=x \land Y=y\} \quad X := X + Y; \quad Y := X - Y; \quad X := X - Y \quad \{Y=x \land X=y\}\]
If so, prove it. If not, give the circumstances in which it fails.
Exercise 8
Show in detail that \( \vdash \{ X = R + (Y \times Q) \} \quad R := R - Y; \quad Q := Q + 1 \quad \{ X = R + (Y \times Q) \} \)

Exercise 9
Give a detailed formal proof that
\[
\vdash \{ T \} \quad \text{IF} \quad X \geq Y \quad \text{THEN} \quad \text{MAX} := X \quad \text{ELSE} \quad \text{MAX} := Y \quad \{ \text{MAX} = \max(X, Y) \}
\]
follows from \( \vdash X \geq Y \Rightarrow \max(X, Y) = X \) and \( \vdash Y \geq X \Rightarrow \max(X, Y) = Y \).

Exercise 10
Suppose we add to our little programming language commands of the form:

```
CASE E OF BEGIN C_1; \ldots; C_n END
```

These are evaluated as follows:
(i) First \( E \) is evaluated to get a value \( x \).
(ii) If \( x \) is not a number between 1 and \( n \), then the CASE-command has no effect.
(iii) If \( x = i \) where \( 1 \leq i \leq n \), then command \( C_i \) is executed.

Why is the following rule for CASE-commands wrong?
\[
\vdash \{ P \land E = 1 \} \quad C_1 \{ Q \}, \ldots, \vdash \{ P \land E = n \} \quad C_n \{ Q \}
\]
\[
\vdash \{ P \} \quad \text{CASE} \quad E \quad \text{OF} \quad \text{BEGIN} \quad C_1; \ldots; C_n \quad \text{END} \quad \{ Q \}
\]

*Hint:* Consider the case when \( P \) is ‘\( X = 0 \)’, \( E \) is ‘\( X \)’, \( C_1 \) is ‘\( Y := 0 \)’ and \( Q \) is ‘\( Y = 0 \)’.

Exercise 11
Devise a proof rule for the CASE-commands in the previous exercise and use it to show:
\[
\vdash \{ 1 \leq X \land X \leq 3 \} \quad \text{CASE} \quad X \quad \text{OF} \quad \text{BEGIN} \quad Y := X - 1; \quad Y := X - 2; \quad Y := X - 3 \quad \text{END} \quad \{ Y = 0 \}
\]

Exercise 12
Devise a proof rule for a command

```
REPEAT command UNTIL statement
```

The meaning of \( \text{REPEAT} \quad C \quad \text{UNTIL} \quad S \) is that \( C \) is executed and then \( S \) is tested; if the result is true, then nothing more is done, otherwise the whole \( \text{REPEAT} \) command is repeated. Thus \( \text{REPEAT} \ C \ UNTIL \ S \) is equivalent to \( C; \quad \text{WHILE} \quad \lnot S \quad \text{DO} \quad C. \)
Additional exercises without solution notes

Exercise 13
Use your REPEAT rule to deduce:

\[ \{ S = C + R \land R < Y \} \]
\[ \text{REPEAT (S:=S+1; R:=R+1) UNTIL R=Y} \]
\[ \{ S = C + Y \} \]

Exercise 14
Use your REPEAT rule to deduce:

\[ \{ X=x \land Y=y \} \]
\[ S:=0; \]
\[ \text{REPEAT} \]
\[ R:=0; \]
\[ \text{REPEAT (S:=S+1; R:=R+1) UNTIL R=Y}; \]
\[ X:=X-1 \]
\[ \text{UNTIL X=0} \]
\[ \{ S = x \times y \} \]

Exercise 15
The exponentiation function \( exp \) satisfies:

\[ \begin{align*}
exp(m, 0) &= 1 \\
exp(m, n+1) &= m \times exp(m, n)
\end{align*} \]

Devise a command \( C \) that uses repeated multiplication to achieve the following partial correctness specification:

\[ \{ X=x \land Y=y \land Y \geq 0 \} \]
\[ C \{ Z=exp(x,y) \land X=x \land Y=y \} \]

Prove that your command \( C \) meets this specification.

Exercise 16
Assume \( \text{gcd}(X,Y) \) satisfies:

\[ \begin{align*}
\text{gcd}(X,Y) &= \text{gcd}(X,Y) \\
\text{gcd}(X,Y) &= \text{gcd}(Y,X) \\
\text{gcd}(X,X) &= X
\end{align*} \]

Prove:

\[ \begin{align*}
\{ (A>0) \land (B>0) \land (\text{gcd}(A,B)=\text{gcd}(X,Y)) \} \\
\text{WHILE A>B DO A:=A-B;} \\
\text{WHILE B>A DO B:=B-A} \\
\{ (0<B) \land (B \leq A) \land (\text{gcd}(A,B)=\text{gcd}(X,Y)) \}
\end{align*} \]
Hence, or otherwise, use your rule for `REPEAT` commands to prove:

\[
\vdash \{A=a \land B=b\}
\]

REPEAT
WHILE \(A>B\) DO \(A:=A-B\);
WHILE \(B>A\) DO \(B:=B-A\)
UNTIL \(A=B\)
\(\{A=B \land A=gcd(a,b)\}\)

Exercise 17
Deduce:

\[
\vdash \{S = (x\times y)-(X\times Y)\}
\]

WHILE \(\neg ODD(X)\) DO \((Y:=2\times Y; \ X:=X \text{ DIV } 2)\)
\(\{S = (x\times y)-(X\times Y) \land ODD(X)\}\)

Exercise 18
Deduce:

\[
\vdash \{S = (x\times y)-(X\times Y)\}
\]

WHILE \(\neg(X=0)\) DO
WHILE \(\neg ODD(X)\) DO \((Y:=2\times Y; \ X:=X \text{ DIV } 2);\)
\(S:=S+Y;\)
\(X:=X-1\)
\(\{S = x\times y\}\)

Exercise 19
Deduce:

\[
\vdash \{X=x \land Y=y\}
\]

\(S:=0;\)
WHILE \(\neg(X=0)\) DO
(WHILE \(\neg ODD(X)\) DO \((Y:=2\times Y; \ X:=X \text{ DIV } 2);\)
\(S:=S+Y;\)
\(X:=X-1)\)
\(\{S = x\times y\}\)

Exercise 20
Using \(P\times X^n=x^n\) as an invariant, deduce:

\[
\vdash \{X=x \land N=n\}
\]

\(P:=1;\)
WHILE \(\neg(N=0)\) DO
(IF \(ODD(N)\) THEN \(P:=P\times X\) else \(P:=P;\)
\(N:=N \text{ DIV } 2;\)
\(X:=X\times X)\)
\(\{P = x^n\}\)
Exercise 21
Prove that the command
\[
Z := 0; \\
\text{WHILE } \neg (X = 0) \text{ DO} \\
\quad (\text{IF } \text{ODD}(X) \text{ THEN } Z := Z + Y \text{ ELSE } Z := Z; \\
\quad Y := Y \times 2; \\
\quad X := X \text{ DIV } 2)
\]
computes the product of the initial values of \(X\) and \(Y\) and leaves the result in \(Z\).

Exercise 22
Prove that the command
\[
Z := 1; \\
\text{WHILE } N > 0 \text{ DO} \\
\quad (\text{IF } \text{ODD}(N) \text{ THEN } Z := Z \times X \text{ else } Z := Z; \\
\quad N := N \text{ DIV } 2; \\
\quad X := X \times X)
\]
assigns \(x^n\) to \(Z\), where \(x\) and \(n\) are the initial values of \(X\) and \(N\) respectively and we assume \(n \geq 0\).

Exercise 23
What are the verification conditions for the following specification?
\[
\{ \text{T} \} \text{ IF } X \geq Y \text{ THEN MAX} := X \text{ ELSE MAX} := Y \{ \text{MAX} = \text{max}(X, Y) \}
\]
Are they true?

Exercise 24
What are the verification conditions for the following specification?
\[
\{ X = R + (Y \times Q) \} R := R - Y; \ Q := Q + 1 \{ X = R + (Y \times Q) \}
\]
Are they true?

Exercise 25
What are the verification conditions generated by the following annotated specification. Are they true?
\{X=n\}
BEGIN
    Y:=1; \{Y = 1 \land X = n\}
    WHILE X\neq 0 DO \{Y\times X! = n!\}
    (Y:=Y\times X; X:=X-1)
END
\{X=0 \land Y=n!\}

Exercise 26
Why are the verification conditions for the annotated specification
\{T\} WHILE F DO \{F\} X:=0 \{T\}
not provable, even though \vdash \{T\} WHILE F DO X:=0 \{T\}.

Exercise 27
Prove by induction on the structure of \(C\) that if no variable occurring in \(P\)
is assigned to in \(C\), then \vdash \{P\} C\{P\}.

Exercise 28
Devise verification conditions for commands of the form REPEAT \(C\) UNTIL \(S\)
(see Exercise 12).

Exercise 29
Consider the following alternative scheme for generating VCs from annotated
WHILE-commands (due to Silas Brown).

### WHILE-commands

Alternative verification conditions generated from
\{P\} WHILE \(S\) DO \{R\} \(C\) \{Q\}
are

1. (i) \(P \land S \Rightarrow R\)
2. (ii) \(P \land \neg S \Rightarrow Q\)
3. (iii) the verification conditions generated by
\{R\} \(C\{(Q \land \neg S) \lor (R \land S)\}\)

Either justify these VCs, or find a counterexample.