《软件分析与验证》第五次书面作业讲解

朱俸民

清华大学

2020 年 5 月

Contents

Contents

1
参考解答

Question

Are the following Hoare triples valid? And why?

(1-1) $\{X = 0 \wedge Y = 1\}\ X := X + 1; Y := Y + 1\ \{X = 1 \wedge Y = 2\}$

(1-2) $\{\top\}$ while $X \leq 0$ do $X := X + 1$ end $\{X \geq 0\}$

(1-3) $[\top]$ while $X > 0$ do $X := X - 1$ end $[X \leq 0]$

(1-4) $\{\top\}$ while $X > 0$ do $X := X - 1$ end $\{X = 0\}$

1
参考解答

Question

Are the following Hoare triples valid? And why?
(1-1) $\{X = 0 \wedge Y = 1\}\ X := X + 1; Y := Y + 1\ \{X = 1 \wedge Y = 2\}$
(1-2) $\{\top\}$ while $X \leq 0$ do $X := X + 1$ end $\{X \geq 0\}$
(1-3) $[\top]$ while $X > 0$ do $X := X - 1$ end $[X \leq 0]$
(1-4) $\{\top\}$ while $X > 0$ do $X := X - 1$ end $\{X = 0\}$

(1-1) Valid. Trivially by (Asgn).
(1-2) Valid. The loop does not terminate once entering.
(1-3) Valid. The loop terminates when $X > 0$.
(1-4) Invalid. The post condition does not hold when $X < 0$.

Solution This hoare triple is not valid. Because for $Q : \{X \geq 0\}$, consider $\sigma[X \mapsto 0]$, execute command we'll get $\sigma[X \mapsto 1]$. That means this command doesn't terminate at environment $\sigma[X \mapsto 0]$, and $X = 0 \notin Q$. ■

Solution This hoare triple is not valid. Because for $Q : \{X \geq 0\}$, consider $\sigma[X \mapsto 0]$, execute command we'll get $\sigma[X \mapsto 1]$. That means this command doesn't terminate at environment $\sigma[X \mapsto 0]$, and $X = 0 \notin Q$. ■

当循环条件不成立时，循环总是可终止的

1 错误解答

1-1 $\{X = 0 \wedge Y = 1\}\ X := X + 1; Y := Y + 1\ \{X = 1 \wedge Y = 2\}$

Solution valid ■

1-2 $\{\top\}$ while $X \leq 0$ do $X := X + 1$ end $\{X \geq 0\}$

Solution valid ■

1-3 $[\top]$ while $X > 0$ do $X := X - 1$ end $[X \leq 0]$

Solution valid ■

1-4 $\{\top\}$ while $X > 0$ do $X := X - 1$ end $\{X = 0\}$

Solution not valid ■

1 错误解答

1-1 $\{X = 0 \wedge Y = 1\}\ X := X + 1; Y := Y + 1\ \{X = 1 \wedge Y = 2\}$

Solution valid ■

1-2 $\{\top\}$ while $X \leq 0$ do $X := X + 1$ end $\{X \geq 0\}$

Solution valid ■

1-3 $[\top]$ while $X > 0$ do $X := X - 1$ end $[X \leq 0]$

Solution valid ■

1-4 $\{\top\}$ while $X > 0$ do $X := X - 1$ end $\{X = 0\}$

Solution not valid ■

没有审题：题目要求说明原因

Solution

Valid. Brfore ececution, $X = 0$ and $Y = 1$.

It is Hoare triples valid.

Solution

Valid. Brfore ececution, $X = 0$ and $Y = 1$.

It is Hoare triples valid.

注意单词拼写、句法等

Contents

2-1
参考解答

Question

Compute wlp(if $X > 0$ then $Y := X$ else $Y := -X, Y > 5$).

Question

Compute wlp(if $X > 0$ then $Y := X$ else $Y := -X, Y > 5$).

$$
\begin{aligned}
&\mathsf{wlp}(\text{if } X > 0 \text{ then } Y := X \text{ else } Y := -X, Y > 5) \\
=&(X > 0 \to \mathsf{wlp}(Y := X, Y > 5)) \wedge (X \leq 0 \to \mathsf{wlp}(Y := -X, Y > 5)) \\
=&(X > 0 \to X > 5) \wedge (X \leq 0 \to X < -5) \\
=&(X \leq 0 \vee X > 5) \wedge (X > 0 \vee X < -5) \\
=&X < -5 \vee X > 5
\end{aligned}
$$

Solution

$$\mathsf{wlp}(\text{if } X > 0 \text{ then } Y := X \text{ else } Y := -X, Y > 5)$$

$$\Rightarrow (X > 0 \rightarrow \mathsf{wlp}(Y := X, Y > 5)) \wedge (X \leq 0 \rightarrow \mathsf{wlp}(Y := -X, Y > 5))$$

$$\Rightarrow (X > 0 \rightarrow X > 5) \wedge (X \leq 0 \rightarrow -X > 5)$$

$$\Rightarrow (X \leq 0 \vee X > 5) \wedge (X > 0 \vee X \leq -5)$$

Solution

$$\mathsf{wlp}(\text{if } X > 0 \text{ then } Y := X \text{ else } Y := -X, Y > 5)$$

$$\Rightarrow (X > 0 \rightarrow \mathsf{wlp}(Y := X, Y > 5)) \wedge (X \leq 0 \rightarrow \mathsf{wlp}(Y := -X, Y > 5))$$

$$\Rightarrow (X > 0 \rightarrow X > 5) \wedge (X \leq 0 \rightarrow -X > 5)$$

$$\Rightarrow (X \leq 0 \vee X > 5) \wedge (X > 0 \vee X \leq -5)$$

这里是等价变换，要用“等号”！

Question

Compute $\mathsf{wlp}(\textsf{while } X > 0 \textsf{ do } X := X + 1 \textsf{ end}, X \leq 0)$.

Solution

Suppose $\mathsf{wlp}(\textsf{while } X > 0 \textsf{ do } \{X > 0\}\ X := X + 1 \textsf{ end}, X \leq 0) = X > 0$.

Then

$$\mathsf{vc}(\textsf{while } X > 0 \textsf{ do } \{X > 0\}\ X := X + 1 \textsf{ end}, X \leq 0) = \left\{ \begin{array}{l} (X > 0) \wedge (X \leq 0) \Rightarrow (X \leq 0) \\ (X > 0) \wedge (X > 0) \Rightarrow (X > -1) \end{array} \right\}$$

Every formula in $\mathsf{vc}(\textsf{while } X > 0 \textsf{ do } \{X > 0\}\ X := X + 1 \textsf{ end}, X \leq 0)$ is valid, so

$$\mathsf{wlp}(\textsf{while } X > 0 \textsf{ do } X := X + 1 \textsf{ end}, X \leq 0) = X > 0$$

Question

Compute wlp(while $X > 0$ do $X := X + 1$ end, $X \leq 0$).

Solution

Suppose wlp(while $X > 0$ do $\{X > 0\}$ $X := X + 1$ end, $X \leq 0) = X > 0$.

Then

$$\text{vc}(\text{while } X > 0 \text{ do } \{X > 0\}\ X := X + 1 \text{ end}, X \leq 0) = \left\{ \begin{array}{l} (X > 0) \wedge (X \leq 0) \Rightarrow (X \leq 0) \\ (X > 0) \wedge (X > 0) \Rightarrow (X > -1) \end{array} \right\}$$

Every formula in vc(while $X > 0$ do $\{X > 0\}$ $X := X + 1$ end, $X \leq 0$) is valid, so

$$\text{wlp}(\text{while } X > 0 \text{ do } X := X + 1 \text{ end}, X \leq 0) = X > 0$$

这个前置条件是最弱的吗？

2-2
参考解答

Solution $\mathsf{wlp}(\textsf{while } X > 0 \textsf{ do } X := X + 1 \textsf{ end}, X \leq 0) = \top$, let's prove by the definition of wlp.

1. $\{\top\}$ while $X > 0$ do $X := X + 1$ end $\{X \leq 0\}$ is valid:
   (a) Starting from an enviroment satisfying $X \leq 0$, the while loop will terminate immediately, leaving X unchanged, thus satisfying $X \leq 0$.
   (b) Starting from an enviroment satisfying $X > 0$, the while loop will not terminate because the loop body will increment X by 1, thus always satisfying condition $X > 0$.

   In conclusion, $\{P\}$ while $X > 0$ do $X := X + 1$ end $\{X \leq 0\}$ is valid for every P, so is for $\top$.
2. $\top$ is the weakest condition, because $P \to \top$ for every P.

2-2
不完整解答

Solution $\mathsf{wlp}(\text{while } X > 0 \text{ do } X := X + 1 \text{ end},\ X \leq 0)$

$\mathsf{wlp}(\text{if } X > 0 \text{ then } X := X + 1; \text{while } X > 0 \text{ do } X := X + 1 \text{ else skip},\ X \leq 0)$

$(X > 0 \rightarrow \mathsf{wlp}(X := X + 1;\ \text{while } X > 0 \text{ do } X := X + 1,\ X > 0)) \wedge (X \leq 0 \rightarrow X \leq 0)$

2-2
不完整解答

Solution $\mathsf{wlp}(\text{while } X > 0 \text{ do } X := X + 1 \text{ end},\ X \leq 0)$

$\mathsf{wlp}(\text{if } X > 0 \text{ then } X := X + 1; \text{while } X > 0 \text{ do } X := X + 1 \text{ else skip},\ X \leq 0)$

$(X > 0 \rightarrow \mathsf{wlp}(X := X + 1;\ \text{while } X > 0 \text{ do } X := X + 1,\ X > 0)) \wedge (X \leq 0 \rightarrow X \leq 0)$

没有把不动点的结果计算（猜）出来

综上，因此式子的wlp为T。

综上，因此式子的wlp为T。

注意符号要规范！

Contents

3
参考解答

$$\{X = m\} \twoheadrightarrow \{X = m \wedge 0 = 0\}$$
$$Y := 0;$$
$$\{X = m \wedge Y = 0\} \twoheadrightarrow \{X = m \wedge Y = 0 \wedge 0 = 0\}$$
$$Z := 0;$$
$$\{X = m \wedge Y = 0 \wedge Z = 0\} \twoheadrightarrow \{Z = Y \times X \wedge X = m\}$$
while $\neg(Y = X)$ do
$$\{Z = Y \times X \wedge X = m \wedge Y \neq X\} \twoheadrightarrow \{Z + X = (Y + 1) \times X \wedge X = m\}$$
$$Z := Z + X;$$
$$\{Z = (Y + 1) \times X \wedge X = m\}$$
$$Y := Y + 1$$
$$\{Z = Y \times X \wedge X = m\}$$
end
$$\{Z = Y \times X \wedge X = m \wedge Y = X\} \twoheadrightarrow \{Z = m \times m\}$$

3
错误解答 1

$\{\top\} \twoheadrightarrow \{0 = 0\}$
$Y := 0;$
$\{Y = 0\} \twoheadrightarrow \{Y = 0 \wedge 0 = 0\}$
$Z := 0;$
$\{Y = 0 \wedge Z = 0\} \twoheadrightarrow \{Z = X \times Y\}$
while $\neg(Y = X)$ **do**
$\{Z = X \times Y \wedge Y \neq X\} \twoheadrightarrow \{Z + X = X \times Y + X = X \times (Y + 1)\}$
  $Z := Z + X$
  $\{Z = X \times (Y + 1)\}$
  $Y := Y + 1$
  $\{Z = X \times Y\}$
end
$\{Z = X \times Y \wedge \neg Y \neq X\} \twoheadrightarrow \{Z = X \times X = m \times m\}$

3
错误解答 1

$\{\top\} \twoheadrightarrow \{0 = 0\}$
$Y := 0;$
$\{Y = 0\} \twoheadrightarrow \{Y = 0 \wedge 0 = 0\}$
$Z := 0;$
$\{Y = 0 \wedge Z = 0\} \twoheadrightarrow \{Z = X \times Y\}$
while $\neg(Y = X)$ **do**
$\{Z = X \times Y \wedge Y \neq X\} \twoheadrightarrow \{Z + X = X \times Y + X = X \times (Y + 1)\}$
  $Z := Z + X$
  $\{Z = X \times (Y + 1)\}$
  $Y := Y + 1$
  $\{Z = X \times Y\}$
end
$\{Z = X \times Y \wedge \neg Y \neq X\} \twoheadrightarrow \{Z = X \times X = m \times m\}$

前置条件不对（默认前置条件是“全局”成立的）!

错误解答 2

$\{X = m\}$
$Y := 0;$
$Z := 0;$
$\{Z = Y \times X\}$

$\{X = m \wedge Y = 0 \wedge Z = 0\}$ ⇒ ???
while $\neg(Y = X)$ do
$\{Z = Y \times X \wedge X = m \wedge \neg\neg Y = X\} \twoheadrightarrow \{Z + X = (Y + 1) \times X \wedge X = m\}$
  $Z := Z + X;$
$\{Z = (Y + 1) \times X \wedge X = m\}$
  $Y := Y + 1$
$\{Z = Y \times X \wedge X = m\}$
end

错误解答 2

$\{X = m\}$
$Y := 0;$
$Z := 0;$
$\{Z = Y \times X\}$

$\{X = m \wedge Y = 0 \wedge Z = 0\}$ ⇒ ???
while $\neg(Y = X)$ do
$\{Z = Y \times X \wedge X = m \wedge \neg\neg Y = X\} \twoheadrightarrow \{Z + X = (Y + 1) \times X \wedge X = m\}$
  $Z := Z + X;$
$\{Z = (Y + 1) \times X \wedge X = m\}$
  $Y := Y + 1$
$\{Z = Y \times X \wedge X = m\}$
end

忽略必要的步骤!

3
错误解答 3

$$\{X = m \wedge Y = 0 \wedge Z = 0\} \twoheadrightarrow \{Z = Y \times X \wedge X = m\}$$
while $\neg(Y = X)$ do
$$\{Z = Y \times X \wedge \neg(Y = X)\} \twoheadrightarrow \{Z + X = (Y + 1) \times X\}$$
$$Z := Z + X;$$
$$\{Z = (Y + 1) \times X\}$$
$$Y := Y + 1$$
$$\{Z = Y \times X\}$$
end
$$\{Z = Y \times X \wedge Y = X \wedge X = m\} \twoheadrightarrow \{Z = m \times m\}$$

3
错误解答 3

$$\{X = m \wedge Y = 0 \wedge Z = 0\} \twoheadrightarrow \{Z = Y \times X \wedge X = m\}$$
while $\neg(Y = X)$ do
$$\{Z = Y \times X \wedge \neg(Y = X)\} \twoheadrightarrow \{Z + X = (Y + 1) \times X\}$$
$$Z := Z + X;$$
$$\{Z = (Y + 1) \times X\}$$
$$Y := Y + 1$$
$$\{Z = Y \times X\}$$
end
$$\{Z = Y \times X \wedge Y = X \wedge X = m\} \twoheadrightarrow \{Z = m \times m\}$$

省去了必要的条件!

3 不规范解答

while $\neg(Y = X)$ do

$\{X = m \wedge Y \leq X \wedge Z = Y * m \wedge Y \neq X\} \twoheadrightarrow \{X = m \wedge Z + X = (Y + 1) * m \wedge Y + 1 \leq X\}$

$Z := Z + X;$

$\{X = m \wedge Z = (Y + 1) * m \wedge Y + 1 \leq X\}$

$Y := Y + 1$

$\{X = m \wedge Z = Y * m \wedge Y \leq X\}$

end

$\{X = m \wedge Z = Y * m \wedge \neg(Y = X)\} \twoheadrightarrow Z = Y * m$

$\{X = m \wedge Y = 0 \wedge Y <= X \wedge 0 = 0\}$

while $\neg(Y = X)$ do

$\{X = m \wedge Y \leq X \wedge Z = Y * m \wedge Y \neq X\} \twoheadrightarrow \{X = m \wedge Z + X = (Y + 1) * m \wedge Y + 1 \leq X\}$

$Z := Z + X;$

$\{X = m \wedge Z = (Y + 1) * m \wedge Y + 1 \leq X\}$

$Y := Y + 1$

$\{X = m \wedge Z = Y * m \wedge Y \leq X\}$

end

$\{X = m \wedge Z = Y * m \wedge \neg(Y = X)\} \twoheadrightarrow Z = Y * m$

$\{X = m \wedge Y = 0 \wedge Y <= X \wedge 0 = 0\}$

注意符号要规范!

Contents

4-1
错误解答 1

$$(\text{Havoc})\ \frac{}{\{P\}\ \textsf{havoc}\ x\ \{P[n/x]\}} \qquad \{a \in \mathbb{N}\}\ \textsf{havoc}\ X\{\ X = a\}$$

4-1
错误解答 1

$$(\text{Havoc})\ \frac{}{\{P\}\ \textsf{havoc}\ x\ \{P[n/x]\}} \qquad \{a \in \mathbb{N}\}\ \textsf{havoc}\ X \{\ X = a\}$$

反例: $\{\top\}$ havoc X $\{X = 1\}$ invalid

4-1
错误解答 2

$$(\text{Havoc})\frac{\exists\, c \vdash \{P\}X := c\{Q\}}{\{P\}\textsf{havoc } X\{Q\}} \quad (\text{Havoc})\frac{}{\{Q[n/x]\}\textsf{havoc } x\{Q\}}$$

4-1
错误解答 2

$$(\text{Havoc})\frac{\exists\, c \vdash \{P\}X := c\{Q\}}{\{P\}\text{havoc } X\{Q\}} \quad (\text{Havoc})\frac{}{\{Q[n/x]\}\text{havoc } x\{Q\}}$$

反例: $\{1 = 1\}$ havoc X $\{X = 1\}$ invalid

4-1
参考解答

$$\{\forall x.Q\}\text{havoc } x\ \{Q\} \quad \text{Asgn}\ \frac{}{\{\forall a.Q[a/x]\}\ \text{havoc } x\ \{Q\}}$$

4-2
错误解答 1

$$\text{Repeat}\ \frac{\{P \wedge \neg b\}\ c\ \{P\}}{\{P\}\ \textsf{repeat}\ c\ \textsf{until}\ b\ \textsf{end}\ \{P \wedge b\}}$$

$$\text{Repeat}\ \frac{\{P \wedge \neg b\}\ c\ \{P\}}{\{P\}\ \text{repeat}\ c\ \text{until}\ b\ \text{end}\ \{P \wedge b\}}$$

反例:

$$\frac{\{X = 0 \wedge \neg \top\}\ X := 1\ \{X = 0\}}{\{X = 0\}\ \text{repeat}\ X := 1\ \text{until true end}\ \{X = 0 \wedge \top\}}$$

is actually invalid

错误解答 2

$$(\text{RepeatTrue})\ \frac{\{P\}c\{Q\} \qquad \{Q\}b\{\top\}}{\{P\}\textsf{repeat } c \textsf{ until } b \textsf{ end}\{Q\}}$$

$$(\text{RepeatFalse})\ \frac{\{P\}c\{P'\} \qquad \{P'\}b\{\bot\} \qquad \{P'\}\textsf{repeat } c \textsf{ until } b \textsf{ end}\{Q\}}{\{P'\}\textsf{repeat } c \textsf{ until } b \textsf{ end}\{Q\}}$$

$$(\text{RepeatTrue})\ \frac{\{P\}c\{Q\} \qquad \{Q\}b\{\top\}}{\{P\}\textsf{repeat } c \textsf{ until } b \textsf{ end}\{Q\}}$$

$$(\text{RepeatFalse})\ \frac{\{P\}c\{P'\} \qquad \{P'\}b\{\bot\} \qquad \{P'\}\textsf{repeat } c \textsf{ until } b \textsf{ end}\{Q\}}{\{P'\}\textsf{repeat } c \textsf{ until } b \textsf{ end}\{Q\}}$$

$\{P\}\ b\ \{Q\}$ 不符合 Hoare triple 的语法（中间只能是语句/命令）

4-2
错误解答 3

$$(\text{Repeat})\frac{\{P\}c\{Q\} \qquad \{Q \wedge b\}c\{Q\}}{\{P\}\textsf{repeat } c \textsf{ until } b \textsf{ end}\{Q \wedge \neg b\}}$$

$$(\text{Repeat})\frac{\{P\}c\{Q\} \qquad \{Q \wedge b\}c\{Q\}}{\{P\}\textsf{repeat } c \textsf{ until } b \textsf{ end}\{Q \wedge \neg b\}}$$

注意 repeat 循环退出时，b 为真

Solution Repeat-loop can be transformed to while-loop:

$$\texttt{repeat } c \texttt{ until } b \texttt{ end}, \;\Rightarrow\; c; \texttt{ while } \neg b \texttt{ do } c \texttt{ end},$$

From the Hoare rules for seq and while-loop:

$$(\text{Seq})\frac{\{P\}\ c_1\ \{P'\} \quad \{P'\}\ c_2\ \{Q\}}{\{P\}\ c_1; c_2\ \{Q\}}$$

$$(\text{While})\frac{\{P \wedge b\}\ c\ \{P\}}{\{P\}\ \texttt{while } b \texttt{ do } c \texttt{ end}\ \{P \wedge \neg b\}}$$

We can get the Hoare rule for repeat-loop:

$$(\text{Repeat})\frac{\{P\}\ c\ \{Q\} \quad \{Q \wedge \neg b\}\ c\ \{Q\}}{\{P\}\ \texttt{repeat } c \texttt{ until } b \texttt{ end}\ \{Q \wedge b\}}$$

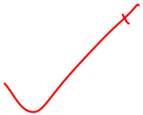
And Q is a loop invariant. ■

$$\text{Repeat}\ \frac{\{P\}\ c\ \{P\}}{\{P\}\ \textsf{repeat}\ c\ \textsf{until}\ b\ \textsf{end}\ \{P \wedge b\}}$$

or

Give Hoare rule for repeat-loop:

$$\frac{\{P \wedge \neg b\}c\{P\}}{\{P \wedge \neg b\}\textsf{repeat}\ c\ \textsf{until}\ b\ \textsf{end}\{P \wedge b\}}$$



证明.

1 $\dfrac{\{P \wedge \neg b\}c\{P\}}{\{P\}\textsf{while}\ \neg b\ \textsf{do}\ c\ \textsf{end}\{P \wedge b\}}$ (while-loop rule)

2 $\dfrac{\{P \wedge \neg b\}c\{P\}\quad \{P\}\textsf{while}\ \neg b\ \textsf{do}\ c\ \textsf{end}\{P \wedge b\}}{\{P \wedge \neg b\}c;\textsf{while}\ \neg b\ \textsf{do}\ c\ \textsf{end}\{P \wedge b\}}$ (sequence rule)

3 $\dfrac{\{P \wedge \neg b\}c\{P\}\quad \{P\}\textsf{while}\ \neg b\ \textsf{do}\ c\ \textsf{end}\{P \wedge b\}}{\{P \wedge \neg b\}\textsf{repeat}\ c\ \textsf{until}\ b\ \textsf{end}\{P \wedge b\}}$ (Equivalence with repeat-loop)

Therefore with condition $\{P \wedge \neg b\}c\{P\}$ we'll get $\{P \wedge \neg b\}\textsf{repeat}\ c\ \textsf{until}\ b\ \textsf{end}\{P \wedge b\}$. □