软件分析与验证 截止时间：2023 年 4 月 27 日

作业 3 答案

授课老师：贺飞 你的姓名 (你的学号)

助教：韩志磊、徐志杰、谢兴宇

在开始完成作业前，请仔细阅读以下说明：

- 我们提供作业的 LaTeX 源码，你可以在其中直接填充你的答案并编译 PDF（请使用 xelatex）。当然，你也可以使用别的方式完成作业（例如撰写纸质作业后扫描到 PDF 文件之中）。但是请注意，最终的提交一定只是 PDF 文件。提交时请务必再次核对，防止提交错误。
- 在你的作业中，请务必填写你的姓名和学号，并检查是否有题目遗漏。请重点注意每次作业的截止时间。截止时间之后你仍可以联系助教补交作业，但是我们会按照如下公式进行分数的折扣：

$$\text{作业分数} = \text{满分} \times (1 - 10\% \times \min(\lceil \text{迟交周数} \rceil, 10)) \times \text{正确率}.$$

- 本次作业为独立作业，禁止抄袭等一切不诚信行为。作业中，如果涉及参考资料，请引用注明。

Problem 1: Hoare 逻辑

1-1 试证明如果霍尔三元组 $\{\varphi\}\ \textbf{if}\,(p)\,\{st_1\}\,\textbf{else}\,\{st_2\}\ \{\psi\}$ 是有效式，则霍尔三元组 $\{\varphi \wedge p\}\ st_1\ \{\psi\}$ 和 $\{\varphi \wedge \neg p\}\ st_2\ \{\psi\}$ 都是有效式。

Solution 考虑分支语句的关系语义定义即可得。■

1-2 证明下面的霍尔三元组是有效式：

$$\{\exists t.\, x = 3t\}\ \textbf{while}(x > 0)\,\{x := x - 1\}\ \{(\exists t.\, x = 3t) \wedge x \leq 0\}$$

Solution

$$\text{前提加强、结论弱化}\ \dfrac{\text{循环}\ \dfrac{\text{前提加强、结论弱化}\ \dfrac{\text{赋值}\ \dfrac{}{\{x - 1 \geq 0\}\ x := x - 1\ \{x \geq 0\}}}{\{(x \geq 0 \vee \exists t.\, x = 3t) \wedge x > 0\}\ x := x - 1\ \{x \geq 0 \vee \exists t.\, x = 3t\}}}{\{x \geq 0 \vee \exists t.\, x = 3t\}\ \textbf{while}\ (x > 0)\ \{x := x - 1\}\ \{(x \geq 0 \vee \exists t.\, x = 3t) \wedge \neg(x > 0)\}}}{\{\exists t.\, x = 3t\}\ \textbf{while}\ (x > 0)\ \{x := x - 1\}\ \{(\exists t.\, x = 3t) \wedge x \leq 0\}}$$

■

Problem 2: 循环

2-1 在扩展 IMP 语言中，下面两个语句是否语义等价，如果等价请给出证明，否则给出反例。

- $?p$
- $\textbf{if}(p)\ \textbf{skip}\ \textbf{else}\ ?\textbf{false}$

Solution 等价。考虑 $(s,s') \in [\![?p]\!]$，分成 $s \vDash p$ 和 $s \nvDash p$ 两种情况证明 $(s,s') \in [\![\textbf{if}\ (p)\ \textbf{skip}\ \textbf{else}\ ?\textbf{false}]\!]$ 即可。■

2-2 **repeat-until** 是另一种常见的循环形式，它的定义如下：

$$\textbf{repeat}\ st\ \textbf{until}(p) \equiv st; (?\neg p; st)^*; ?p$$

证明下面的推理规则是可靠的：

$$\frac{\{\varphi\}\ st\ \{\varphi'\} \quad \{\varphi' \wedge \neg p\}\ st\ \{\varphi'\}}{\{\varphi\}\ \textbf{repeat}\ st\ \textbf{until}(p)\ \{\varphi' \wedge p\}}$$

Solution

$$\equiv\dfrac{;\dfrac{\{\varphi\}\ st\ \{\varphi'\} \qquad ;\dfrac{*\dfrac{;\dfrac{?\dfrac{}{\{\varphi'\}\ ?\neg p\ \{\varphi' \wedge \neg p\}} \qquad \{\varphi' \wedge \neg p\}\ st\ \{\varphi'\}}{\{\varphi'\}\ ?\neg p; st\ \{\varphi'\}}}{\{\varphi'\}\ (?\neg p; st)^*\ \{\varphi'\}} \qquad ?\dfrac{}{\{\varphi'\}\ ?p\ \{\varphi' \wedge p\}}}{\{\varphi\}\ (?\neg p; st)^*; ?p\ \{\varphi'\}}}{\{\varphi\}\ st; (?\neg p; st)^*; ?p\ \{\varphi' \wedge p\}}}{\{\varphi\}\ \textbf{repeat}\ st\ \textbf{until}(p)\ \{\varphi' \wedge p\}}$$

■

Problem 3: 数组

3-1 基于数组理论 $\mathcal{T}_A$（及其扩展）编码以下陈述：

1. 数组 a 可以被从某个位置分成非空的两半，前一半的元素均小于后一半的元素；
2. 若对数组 a 和 b 的同一位置进行相同更新操作之后，数组 a 和 b 的完全相同，那么 a 和 b 仅有可能在该位置上有不同元素。

Solution

1. $\exists m.\ 0 \leq m < |a| - 1 \wedge \forall i.\ 0 \leq i \leq m < j < |a| \rightarrow a[i] < a[j]$
2. $\forall i, v.\ 0 \leq i < |a| \wedge 0 \leq i < |b| \wedge a\langle i \triangleleft v\rangle = b\langle i \triangleleft v\rangle \rightarrow \forall j.\ 0 \leq j < |a| \wedge 0 \leq j < |b| \wedge j \neq i \rightarrow a[j] = b[j]$

■

3-2 在扩展 IMP 语言中，证明下面的霍尔三元组是有效式：

$$\begin{array}{l} \{m < a[0] \wedge i = 0\} \\ \textbf{while}\ (i < n)\ \{\ \textbf{if}\ (m < a[i])\ \{m := a[i]\}\ \textbf{else}\ \{\textbf{skip}\};\ i := i + 1\} \\ \{\forall k.\ (0 \leq k < n \rightarrow m \geq a[k])\} \end{array}$$

Solution 记

- $st = \textbf{while}\ (i < n)\ \{\ \textbf{if}\ (m < a[i])\ \{\ m := a[i]\ \}\ \textbf{else}\ \{\ \textbf{skip}\ \};\ i := i + 1\ \}$
- $st_1 = \textbf{if}\ (m < a[i])\ \{\ m := a[i]\ \}\ \textbf{else}\ \{\ \textbf{skip}\ \}$
- $st_2 = i := i + 1$
- $\varphi_1 = 0 \le i \le n \wedge \forall j.\ 0 \le j < i \to m \ge a[j]$
- $\varphi_2 = 0 \le i + 1 \le n \wedge \forall j.\ 0 \le j < i + 1 \to m \ge a[j]$
- $\varphi_3 = 0 \le i + 1 \le n \wedge \forall j.\ 0 \le j < i + 1 \to a[i] \ge a[j]$

证明树如下（为节省空间，前提加强和结论弱化规则未被标出，并且对前提加强和结论弱化规则的连续使用被合并表示）：

$$\dfrac{\text{循环}\ \dfrac{\text{顺序}\ \dfrac{\text{分支}\ \dfrac{\dfrac{\text{赋值}\ \dfrac{}{\{\varphi_3\}\ m := a[i]\ \{\varphi_2\}}}{\{\varphi_1 \wedge i < n \wedge m < a[i]\}\ m := a[i]\ \{\varphi_2\}} \qquad \dfrac{\text{空语句}\ \dfrac{}{\{\varphi_2\}\ \textbf{skip}\ \{\varphi_2\}}}{\{\varphi_1 \wedge i < n \wedge m \ge a[i]\}\ \textbf{skip}\ \{\varphi_2\}}}{\{\varphi_1 \wedge i < n\}\ st_1\ \{\varphi_2\}} \qquad \text{赋值}\ \dfrac{}{\{\varphi_2\}\ st_2\ \{\varphi_1\}}}{\{\varphi_1 \wedge i < n\}\ st_1; st_2\ \{\varphi_1\}}}{\{\varphi_1\}\ st\ \{\varphi_1 \wedge \neg(i < n)\}}}{\{m < a[0] \wedge i = 0\}\ st\ \{\forall k. 0 \le k < n \to m \ge a[k]\}}$$

■