软件分析与验证	**截止时间: Apr 10, 2022**

作业 2

授课老师: 贺飞　　　　周雨豪 (2018013399)

助教: 徐荣琛、谢兴宇、韩志磊、刘江宜

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:

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

- 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: 一阶理论

1-1 请基于皮亚诺算术理论 $\mathcal{T}_{PA}$ 表示如下的公式:

$$\forall x, y.\ \exists z.\ 2x + 1 < 3y + z$$

Solution $\forall x, y.\exists z, w.2x + 1 + w = 3y + z$ ■

1-2 证明 $\mathcal{T}_{\mathbb{Z}}$ 可以归约到 $\mathcal{T}_{\mathbb{N}}$。

Solution 签名 $\Sigma_{\mathbb{Z}}$ 中的整数部分归约为 $\exists z.z = x + 1 + ... + 1$ 或 $\exists z.z + 1 + ... + 1 = x$，$x$ 为签名 $\Sigma_{\mathbb{N}}$ 中的整数。数乘 $x \cdot y$ 规约为 x 个 y 相加。算数减号 $-x$ 归约为 $+(-x)$。大于号 $x > y$ 规约为 $\exists z.x = y + z$。■

Problem 2: 程序语义

2-1 计算下列表达式在给定状态 $\{x \mapsto 3, y \mapsto 1, z \mapsto 0\}$ 下的值：

1. $x \leq y \rightarrow z \neq x$；
2. $(x - z) * (y + 1)$。

Solution

1. $3 \leq 1 \rightarrow 0 \neq 3 \Leftrightarrow true$；
2. $(3 - 0) * (1 + 1) = 3 * 2 = 6$。

■

2-2 证明 IMP 程序语句 **while**$(x < 0)$ $\{x := y * y;\}$ 和 **if**$(x < 0)$ $\{x := y * y;\}$ **else skip** 是语义等价的。

Solution $[\![\textbf{while}(x < 0)\ \{x := y * y;\}]\!] = \{(s, s') \mid$ 存在一个整数 n 和一组状态序列 $s, t_1, t_2, \ldots, t_n = s'$，使得对任意的 $0 \leq i < n : [\![x < 0]\!]_{t_i} = true, (t_i, t_{i+1}) = [\![x := y * y]\!], [\![x < 0]\!] = false\}$。
因为 $y * y$ 必不小于 0，所以 $[\![\textbf{while}(x < 0)\ \{x := y * y;\}]\!] = \{(s, s') \mid x < 0 \Leftrightarrow true$ 且 $(s, s') \in [\![x := y * y]\!]_s$ 或 $x \geq 0 \Leftrightarrow true$ 且 $(s, s') \in [\![skip]\!]_s = [\![\textbf{if}(x < 0)\ \{x := y * y;\}\ \textbf{else skip}]\!]$
由此两者语义等价 ■

Problem 3: Hoare 逻辑

3-1 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 $\{\varphi \land p\}\ \ st_1\ \ \{\psi\}$ 和 $\{\varphi \land \neg p\}\ \ st_2\ \ \{\psi\}$ 都是有效式。

Solution

$$\text{(分支)}\ \frac{\{\varphi \land p\}\ \ st_1\ \ \{\psi\}\quad \{\varphi \land \neg p\}\ \ st_2\ \ \{\psi\}}{\{\varphi\}\ \ \textbf{if}(p)\ \ \{st_1\}\ \ \textbf{else}\ \ \{st_2\}\ \ \{\psi\}}$$

$\models \{\varphi \land p\}\ \ st_1\ \ \{\psi\}\ \ \{\varphi \land \neg p\}\ \ st_2\ \ \{\psi\}$，则 $\{\varphi \land p\}\ \ st_1\ \ \{\psi\}$ 和 $\{\varphi \land \neg p\}\ \ st_2\ \ \{\psi\}$ 都是有效式。
■

3-2 试证明下面的霍尔三元组成立：

$$\{\text{even}(x)\}\ \ \textbf{while}(x > 0)\,\{x := x - 1\}\ \ \{\text{even}(x) \land x \le 0\}$$

其中，$\text{even}(x) \leftrightarrow \exists t.\ x = 2t$。

Solution ■

$$\text{(赋值)}\frac{}{\{x - 1 > 0\}\ \ x := x - 1\ \ \{x > 0\}}$$

$$\text{(结论弱化)}\frac{}{\{x - 1 > 0\}\ \ x := x - 1\ \ \{\text{even}(x)\}}$$

$$\text{(前提加强)}\frac{}{\{\text{even}(x) \land x > 0\}\ \ x := x - 1\ \ \{\text{even}(x)\}}$$

$$\text{(循环)}\frac{}{\{\text{even}(x)\}\ \ \textbf{while}(x > 0)\,\{x := x - 1\}\ \ \{\text{even}(x) \land x \le 0\}}$$