软件分析与验证 **截止时间: 2023 年 5 月 18 日**

作业 4

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: 谓词变换

1-1 计算下列最弱前置条件。

- $wlp(b[m] := b[n]; b[n] := t, b[m] < b[n])$
- $wlp(\textbf{if } y > 2 \textbf{ then } x := y - 5 \textbf{ else } x := -y, x \geq 0)$

Solution 两问的解答中，我们都会用到 $(p \to q) \wedge (\neg p \to r)$ 与 $(p \wedge q) \vee (\neg p \wedge r)$ 语义等价这一结论。

- $$\begin{aligned}
& wlp(b[m] := b[n]; b[n] := t, b[m] < b[n]) \\
= \ & wlp(b[m] := b[n], wlp(b[n] := t, b[m] < b[n])) \\
= \ & wlp(b[m] := b[n], (b[m] < b[n])[b \mapsto b\langle n \triangleleft t \rangle]) \\
= \ & wlp(b[m] := b[n], b\langle n \triangleleft t \rangle[m] < t) \\
= \ & wlp(b[m] := b[n], (m = n \to t < t) \wedge (m \neq n \to b[m] < t)) \\
= \ & wlp(b[m] := b[n], (m = n \wedge t < t) \vee (m \neq n \wedge b[m] < t)) \\
= \ & wlp(b[m] := b[n], m \neq n \wedge b[m] < t) \\
= \ & (m \neq n \wedge b[m] < t)[b \mapsto b\langle m \triangleleft b[n] \rangle] \\
= \ & m \neq n \wedge b[n] < t
\end{aligned}$$

- $$\begin{aligned} & wlp(\textbf{if } y>2 \textbf{ then } x:=y-5 \textbf{ else } x:=-y, x\geq 0) \\ = \ & (y>2 \to wlp(x:=y-5, x\geq 0)) \wedge (y\leq 2 \to wlp(x:=-y, x\geq 0)) \\ = \ & (y>2 \to (x\geq 0)[x\mapsto y-5]) \wedge (y\leq 2 \to (x\geq 0)[x\mapsto -y]) \\ = \ & (y>2 \to y-5\geq 0) \wedge (y\leq 2 \to -y\geq 0) \\ = \ & (y>2 \wedge y\geq 5) \vee (y\leq 2 \wedge y\leq 0) \\ = \ & (y\geq 5) \vee (y\leq 0) \end{aligned}$$

■

1-2 利用最弱前置条件推导，证明下列程序属性的正确性。

```
// {true}
n := 0;
x := 0;
while (r ≠ 0) {
  n := n + 1;
  x := x + 2 × n - 1;
  r := r - 1;
}
// {x = n × n}
```

提示：考虑使用循环不变式：$x=n\times n$。

Solution 前置条件 $\varphi\equiv\textbf{true}$，后置条件 $\psi\equiv(x=n\times n)$，循环不变式 $I\equiv(x=n\times n)$. 验证条件如下：

- 循环不变式的可达性：$\varphi\to wp(n:=0;x:=0,I)$
- 循环不变式的归纳性：$(I\wedge r\neq 0)\to wp(n:=n+1;x:=x+2\times n-1;r:=r-1,I)$
- 循环不变式的可证性：$(I\wedge r=0)\to\psi$

$$\begin{aligned} & wp(n:=0;x:=0,I) \\ = \ & wp(n:=0;x:=0,x=n\times n) \\ = \ & wp(n:=0,0=n\times n) \\ = \ & (0=0\times 0) \\ = \ & \textbf{true} \end{aligned}$$

$$
\begin{aligned}
& wp(n := n+1; x := x+2\times n-1; r := r-1, I) \\
= \ & wp(n := n+1; x := x+2\times n-1; r := r-1, x = n\times n) \\
= \ & wp(n := n+1; x := x+2\times n-1, x = n\times n) \\
= \ & wp(n := n+1, x+2\times n-1 = n\times n) \\
= \ & (x+2\times(n+1)-1 = (n+1)\times(n+1)) \\
= \ & (x = n\times n)
\end{aligned}
$$

因此，验证条件可化简为：

- **true** $\rightarrow$ **true**
- $(x = n\times n \wedge r \neq 0) \rightarrow x = n\times n$
- $(x = n\times n \wedge r = 0) \rightarrow x = n\times n$

不难验证，上述验证条件均为有效式，因此原程序属性的正确性得证。
■

Problem 2: 基本路径

2-1 请写出过程 Proc_A 的所有基本路径。

```
/* requires x > 0;
   ensures rv = 0; */
procedure Proc_M(x);

/* requires y > 0;
   ensures rv ≥ 0; */
procedure Proc_A(y) {
    if (y > 10)
    {
        v := Proc_M(y);
        assert(v ≥ 0);
        return v;
    }
    while(y > 0)
    /* invariant: y ≥ 0 */
    {
        t := y;
        while(t > 0)
        /* invariant: t ≥ 0 ∧ y ≥ t */
        {
            t := t - 1;
        }
```

```
        y := y - 1;
    }
    return 0;
}
```

Solution

基本路径 1：

```
// {y > 0}
assume y > 10;
// {y > 0}
```

基本路径 2：

```
// {y > 0}
assume y > 10;
assume v1 = 0;
v := v1;
// {v ≥ 0}
```

基本路径 3：

```
// {y > 0}
assume y > 10;
assume v1 = 0;
v := v1;
(assume v ≥ 0) // 一般省略，因为v ≥ 0已被基本路径2蕴含
rv := v;
// {rv ≥ 0}
```

基本路径 4：

```
// {y > 0}
assume y ≤ 10;
// {y ≥ 0}
```

基本路径 5：

```
// {y ≥ 0}
assume y > 0;
t := y;
// {t ≥ 0 ∧ y ≥ t}
```

基本路径 6：

```
// {t ≥ 0 ∧ y ≥ t}
assume t > 0;
t := t - 1;
// {t ≥ 0 ∧ y ≥ t}
```

基本路径 7:

```
// {t ≥ 0 ∧ y ≥ t}
assume t ≤ 0;
y := y - 1;
// {y ≥ 0}
```

基本路径 8:

```
// {y ≥ 0}
assume y ≤ 0
rv := 0;
// {rv ≥ 0}
```

■