《软件工程理论基础》作业二

2025 年 5 月 15 日

作业提交说明

- 文件格式：PDF。
- 文件命名：命名格式为 “学号 _ 姓名 _v 版本”，例如 “123456_ 张三 _v1”（可简写为 “123456_ 张三”），我们将按照最新版本评分。
- 提交地址：`https://box.nju.edu.cn/u/d/db7ea58798b2451cb3a5/`。
- 截止时间：2025 年 5 月 30 日 23:59:59。

1 公平性（Fairness）

进程 A 和 B 分别使用如图 1和图 2所示方法申请被调度执行，图 3所示调度器则用来调度进程 A 和 B。假设进程 A 和 B 可以同时执行，请问分别在哪些公平性（fairness）条件下，A 和 B 不会被“饿死”。

```
while(true) {
  is_A_ready = true;
  for i:= 1 to 10 {
    if is_A_scheduled {
      // do something
      break;
    }
  }
  is_A_ready = false;
}
```

图 1: 进程 A

```
while(true) {
  is_B_ready = true;
  wait until is_B_scheduled {
    // do something
  }
  is_B_ready = false;
}
```

图 2: 进程 B

```
while(true) {
  if is_A_ready == true
    is_A_scheduled = true;
  if is_B_ready == true
    is_B_scheduled = true;
}
```

图 3: 调度器

2 Binary Decision Diagram（BDD）

1) 针对布尔函数 $f(a,b,c) = (a \wedge b \wedge c) \vee (a \wedge (\neg b) \wedge c) \vee ((\neg a) \wedge b \wedge (\neg c)) \vee ((\neg a) \wedge (\neg b) \wedge (\neg c))$，完成以下问题：

   a. 以 $a < b < c$ 为顺序，写出对应的 BDD；

   b. 写出该 BDD 的 reduced form。

2) 对于布尔函数 $f(x,y) = x \vee y$ 和 $f(x,y) = x \wedge y$，回答下列问题：

   a. 分别写出对应的 BBD；

   b. 执行 $f \wedge g$ 运算，合并为一个 BDD。

3 霍尔三元组（Hoare Tripe）

在下列霍尔三元组的空白处填写恰当的前置条件，使得对应的三元组成立。注意，前置条件应尽可能弱。

- $\{\quad\}x := x + 1\{\quad\}y := y + 2 * x - 1\{y = x^2\}$
- $\{\quad\}x := x + y; y := x - y; x := x - y\{x = z \wedge y = w\}$
- $\{\quad\}$**while** $a < b$ **do** $\{a := a + 1; y := x + y\}\{y = b * x\}$

4 完全正确性

请证明图 4所示函数的完全正确性，即部分正确性和终止性。

```
// assume x>=0
int f(int x){
  int n = 0, y = 1
  while(n!=x) {
    n = n + 1;
    y = y*n;
  }
  // assert y==x!
  return y;
}
```

图 4: 阶乘

5 推理规则

Rust 是一种系统编程语言，旨在提供内存安全、并发支持和高性能，同时避免 C/C++ 中常见的安全问题（如空指针、数据竞争等）。Rust 通过所有权（Ownership）、借用（Borrowing）和生命周期（Lifetimes）等特性，在编译期防止空指针、悬垂引用和数据竞争，无需垃圾回收器。

在本题中，请针对图 5所定义的程序，给出恰当的推理规则，进行“类型”和“借用”的检查。

示例：以 Γ 表示程序上下文，谓词 $\text{Type}(x,T)/\text{Type}(e,T)$ 表示变量 x/表达式 e 的类型为 T，谓词 $\text{Equal}(T_0,T_1)$ 表示类型 T_0 和 T_1 相同，则有

$$\frac{\Gamma \models (\texttt{Type}(e,T_e) \land \texttt{Equal}(T_e,T)),\ \texttt{let x : T = e}}{\Gamma \models \texttt{Type}(x,T)}$$

$$\frac{\Gamma \models (\texttt{Type}(e,T_e) \land \neg\texttt{Equal}(T_e,T)),\ \texttt{let x : T = e}}{\Gamma \models \texttt{Error}}$$

```
变量  x ∈ Identifier

整数值 n ∈ ℤ

布尔值 b ::= true | false

类型 T ::= int | bool
         | &T | &mut T      // 不考虑多重引用

表达式 e ::= n | b | x | &x | &mut x | *x
         | e1 + e2 | e1 == e2   // 三地址代码

语句 s ::= skip | x = e | *x = e
         | let x : T = e;       // 变量声明
         | s1 ; s2
         | if (e) { s1 } else { s2 }
```

图 5: MiniRust