《软件工程理论基础》项目二

2025 年 5 月 15 日

项目提交说明

- 提交内容：报告（.pdf）和代码（.c）。
- 提交方式：将所有文件打包为一个压缩包（.zip 格式），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/ac5c786924c345d69b5f/`。
- 截止时间：2025 年 5 月 29 日 23:59:59。

自动化验证

Frama-C (`https://www.frama-c.com`) 是一个用于 C 语言程序静态分析的开源平台，主要用于验证程序的安全性、可靠性和功能正确性，特别适用于嵌入式系统和高安全性要求的软件（如航空航天、汽车、核能等领域）。

ACSL (`https://frama-c.com/html/acsl.html`)(ANSI/ISO C Specification Language) 是一种用于为 C 程序添加形式化规范的注释语言，主要用于程序验证。它在 Frama-C 等静态分析工具中得到了广泛应用，能够描述程序函数的前置条件、后置条件、不变式、断言等。

1) 考虑图 1所示程序，回答下列问题：

   a. 当该程序执行结束，存在函数 f, g 使得 $a = f(n), b = g(n)$，请给出这样的 f, g。

   b. 将问题 a 中的 f, g 作为后置条件，使用 Frama-C 和 ACSL 证明其完全正确性。

```
// assume( n>=0 && n<=100 )
// assume( a==0 )
// assume( b==0 )
int i = n;
while(i<100) {
  if(a<=5) a++;
  else a-=4;
  b+=a;
  i++;
}
```

图 1: 数值程序

2) 针对图 2所示算法，完成以下问题：

   a. 使用 ACSL 描述该算法的输入输出要求，运行 Frama-C，查看验证结果。

   b. 完善问题 a 中 ACSL，使得验证通过。

```
void selection_sort(int arr[], int n) {
  int i, j, min_idx, temp;

  for (i = 0; i < n - 1; i++) {
    min_idx = i;
    for (j = i + 1; j < n; j++) {
      if (arr[j] < arr[min_idx]) {
        min_idx = j;
      }
    }
    if (min_idx != i) {
      temp = arr[i];
      arr[i] = arr[min_idx];
      arr[min_idx] = temp;
    }
  }
}
```

图 2: 选择排序