

《软件工程理论基础》项目一

2025 年 4 月 3 日

项目提交说明

- 建模工具：NuSMV 2.7.0 (<https://nusmv.fbk.eu>)。
- 提交内容：
 - 项目报告 (PDF 文件)：简明扼要地描述各模型的设计思路和运行效果，建议包含问题分析、迁移模型和运行截图等内容。
 - 模型文件 (*.smv 文件)：各任务对应的模型文件，建议放置在不同的文件夹，例如 1/*.smv, 2/*.smv 和 3/*.smv。
- 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/6a217c58019c4415b65a/>。
- 截止时间：2025 年 4 月 24 日 23:59:59。

1 等价性判断

考虑下面四组逻辑公式，某些组里的两个逻辑公式是不等价的，请选出这样的组，并用 NuSMV 证明你的结论。(提示：如果两个公式是不等价的，那么能设计出一个模型，使得一个公式为真而另一个为假。)

- a. $\mathbf{EF}\phi$ 和 $\mathbf{EG}\phi$
- b. $\mathbf{EF}\phi \vee \mathbf{EF}\psi$ 和 $\mathbf{EF}(\phi \vee \psi)$
- c. $\mathbf{AF}\phi \vee \mathbf{AF}\psi$ 和 $\mathbf{AF}(\phi \vee \psi)$
- d. $\mathbf{A}(\phi_1 \mathbf{UA}(\phi_2 \mathbf{U}\phi_3))$ 和 $\mathbf{A}(\mathbf{A}(\phi_1 \mathbf{U}\phi_2) \mathbf{U}\phi_3)$

2 冒泡排序建模

图 1是冒泡排序算法，请完成以下问题：

- 假设数组长度始终为 3，元素的范围是 0-7，请使用 NuSMV 建模该算法。
- 使用 NuSMV 验证问题 a 的模型是否完成了排序。
- 在问题 a 的基础上，禁止使用整数域的 “+”，“-”，“>”，“=” 和 “<” 五个操作符，请重新建模该算法。

```
bubble_sort(array):  
    n = len(array)  
    for i in range(n):  
        # 标记是否发生了交换  
        swapped = False  
        for j in range(0, n-i-1):  
            if array[j] > array[j+1]:  
                # 交换位置  
                array[j], array[j+1] = array[j+1], array[j]  
                swapped = True  
        # 如果没有发生交换，说明列表已经有序，提前退出  
        if not swapped:  
            break  
    return array
```

图 1: 冒泡排序

3 Raft 算法建模

- 背景：在分布式环境中，一致性是指数据在多个副本之间是否能够保持一致的特性。
- Raft 算法
 - 主页：<https://raft.github.io>。
 - 可视化：<https://thesecretlivesofdata.com/raft/>。
- 要求
 - 三个节点，均不会 offline。
 - 不考虑通信丢失的情况。
 - 只需要建模 Leader Election 和 Heartbeat 过程，即，正确建模所有节点在 Follower, Candidate 和 Leader 三个“角色”之前的切换。
 - Leader 节点会在一定时间后切换为 Follower。（如不做此条约束，那么第一个 Leader 被选出后便保持不变。）
 - Timeout 可以选取一些较小值，但要保证随机性。
 - 编写并验证以下规约：
 - * 三个节点都可能成为 Leader；
 - * 不会出现多个 Leader；
 - * 可能有多个节点同时想成为 Leader。