Lab 3: Dafny

Tom

1 安装软件

下面的粉红色字是超链接。

1. 本次 lab 使用 dafny 形式化验证真实程序。
2. Microsoft research 提供了 教程。你需要通过这个教程学习如何使用 Dafny。要完成这个 lab，你需要理解第 1、2、3、6、8、9 和 10 节。
3. 教程中有很多练习，如果你感兴趣，答案在这里。
4. 你不需要安装软件，因为你可以直接在网页右边的框里写代码，然后点击紫色按钮就可以进行形式化验证了。过段时间会输出程序验证通过或者程序有错误。图 1和图 2是示例。

2 Problem

本次 lab 有 3 个小问题，你需要编写前置条件等。

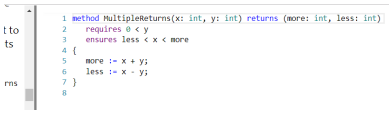

图 1: Write code.

图 2: Push button and verify code.

2.1 method1

```
method method1(x: int, y: int) returns (z: int)
// Add a precondition here.
   ensures z > 0
{
   if x < 0
     { return y; }
   else
     { return x; }
}
```

编写合适的前置条件，保证返回值是正数。

2.2 method2

```
method method2(a: array<int>, v: int) returns (b: int)
// Add a precondition here.
{
   return a[v] / v;
}
```

编写合适的前置条件，使程序能验证通过，保证运行时不产生数组越界、除数是 0 等错误。

2.3 method3

```
predicate notzero(a: array<int>)
  reads a
{
// Add a predicate here.
}

method method3(a : array<int>, n : int) returns (b : int)
  requires n == a.Length && notzero(a)
  ensures b == 0;
{
  var i := 0;
  while i < n
      invariant 0 <= i <= a.Length
      invariant n == a.Length
      invariant forall k :: 0 <= k < i ==> a[k] != 0
  {
    if a[i] == 0
    { return 1; }
```

```
    i := i + 1;
  }
  return 0;
}
```

写一个合适的 predicate 让程序一定返回 0。

3 提交

3 段代码分别放在名字是 method1.dfy、method2.dfy、method3.dfy 的文件中，写完后请把它们打包为 lab3.zip，提交 zip 文件。注意：压缩包解压后应该直接就是只有 3 个 dfy 文件，不要把 dfy 文件放在文件夹中进行压缩。违反本要求将酌情扣分。