Lab 3: Dafny

Tom

1 安装软件

```
os@ubuntu:~/cdm$ ./dafny/dafny method*.dfy

Dafny program verifier finished with 6 verified, 0 errors
Compiled assembly into method1.dll
os@ubuntu:~/cdm$
```

```
os@ubuntu:~/cdm$ ./dafny/dafny method*.dfy
/home/os/cdm/method2.dfy(5,11): Error: index out of range
Execution trace:
    (0,0): anon0
/home/os/cdm/method2.dfy(5,15): Error: possible division by zero
Execution trace:
    (0,0): anon0

Dafny program verifier finished with 4 verified, 2 errors
```

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，你需要从中学习如何使用 Dafny。你需要重点阅读其中的 Introduction，Methods，Pre- and Postconditions、Quantifiers、Array 和 Predicates 节。其它部分和本次 lab 关系不大。

3. dafny 的安装包在 lab3 附件中，你只需要将其解压到你的 lab 代码所在目录下，保证最外层的 dafny 文件夹和你的 dfy 文件在一个目录下，不需要额外的安装操作。这一安装包仅支持 linux 环境。

4. dafny 的可执行文件为 dafny/dafny，在你的 dfy 代码文件所在目录下打开终端，并输入以下命令以验证你写的程序: ./dafny/dafny xxx.dfy（其中 xxx.dfy 是你写的 dafny 代码文件名）。

5. 如果代码写对了，你会看到上面第一张图的输出，否则会看到类似上面第二张图的报错信息。

6. 你也可以使用通配符来验证你所有的 dafny 程序：./dafny/dafny method*.dyf（意思是验证全部 3 个 dfy 文件的代码）。

2 Problem

本次 lab 有 3 个小问题，你需要编写前置条件等。

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。