Dafny I

Program Verification

FMI · Denisa Diaconescu · Spring 2022

Dafny

- Created by Rustan Leino at Microsoft Research
- An imperative compiled language
- Is open source
- Supports formal specification through preconditions, postconditions, loop invariants.

- Proves that there are no runtime errors, such as index out of bounds, null dereferences, division by zero, etc
- Also proves the termination of code.

Dafny

- Programming language designed for reasoning
- Program verifier
- Language features drawn from:
  - Imperative programming
    `if, while, :=, class,...`
  - Functional programming
    `function, datatype,...`
  - Proof authoring
    `Lemma, calc, refines, inductive predicate,...`

Dafny

- Dafny's homepage
- The Github page which includes sources and binary downloads for Windows, Mac, GNU/Linux

Using Dafny

- Dafny IDE in Visual Studio
- Dafny mode in Emacs
- Dafny IDE in VS Code
- In web browser at
  `http://cse-212294.cse.chalmers.se/courses/tdv/dafny/`

Dafny tutorial

Exercise: Read the Dafny Guide and experiment with Dafny.

https://dafny-lang.github.io/dafny/OnlineTutorial/guide

Read the following sections:

- Introduction
- Methods
- Pre- and post-conditions
- Assertions
- Functions
- Loop invariants

Solve Exercises 0-4 and 7-9 from the Guide.

Dafny

Exercise: Write a method in Dafny

```
method SumMaxBackwards(s: int, m: int) returns (x: int, y: int)
```

which returns the values `x` and `y` such that

- `s` is the sum of `x` and `y` and
- `m` is the maximum of `x` and `y`.

Write the post-conditions for this method.

Do you need any pre-conditions?