## CS 116 FALL 2017 REASONING ABOUT PROGRAM CORRECTNESS

http://rjoshi.org/cs116

This course provides an introduction to formal reasoning about correctness of computer programs. We will cover both the theory and the practice of program reasoning, focusing more on the *practice*.

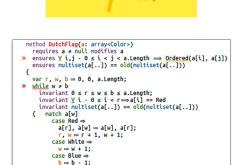
We will look at representative programming problems and discuss how to verify program correctness using automated verifiers Dafny and Stainless. Grading will be based on take-home assignments. Handouts and notes will be given to supplement class material as needed.

## Topics include

- writing formal specifications of program behavior
- fundamentals of program reasoning using weakest preconditions and strongest postconditions
- introduction to program semantics using predicate transformers
- fundamentals of verification condition generation for automated proofs
- reasoning about object-oriented programs

CS 116 is a companion course to

CS 118: Logic Model Checking (Holzmann, Winter)



```
def isSorted(l: List): Boolean = l match {
   case Nil => true
   case Cons(_,Nil) => true
   case Cons(x1, Cons(x2, rest)) =>
     x1 < x2 && isSorted(Cons(x2,rest))
}</pre>
```

```
def sInsert(x : BigInt, l : List) : List = {
    require(isSorted(l))
    l match {
        case Nil ⇒ Cons(x, Nil)
        case Cons(e, rest) if (x == e) ⇒ l
        case Cons(e, rest) if (x < e) ⇒ Cons(x, Cons(e, rest))
        case Cons(e, rest) if (x > e) ⇒ Cons(e, sInsert(x, rest))
    }
} ensuring {(res:List) ⇒ isSorted(res)}
```

## **INSTRUCTOR:**

RAJEEV JOSHI (NASA / JPL)

TUE/THU 1 - 2:25 P.M. Annenberg 107

9 UNITS (3 - O - 6)

PREREQUISITE: CS1 OR EQUIVALENT



