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.

```
method DutchFlag(a: array<Color>)
  requires a ≠ null modifies a
» ensures ∀ i,j · 0 ≤ i < j < a.Length ⟹ Ordered(a[i], a[j])
  ensures multiset(a[..]) == old(multiset(a[..]))
{
  var r, w, b := 0, 0, a.Length;
» while w ≠ b
    invariant 0 ≤ r ≤ w ≤ b ≤ a.Length;
    invariant ∀ i · 0 ≤ i < r⟹a[i] == Red
    invariant multiset(a[..]) == old(multiset(a[..]))
  {  match a[w]
       case Red ⇒
         a[r], a[w] := a[w], a[r];
         r, w := r + 1, w + 1;
       case White ⇒
         w := w + 1;
       case Blue ⇒
         b := b - 1;
```

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

```
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))
}
```

```
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)}
```

CS 116 is a companion course to
CS 118: *Logic Model Checking* (Holzmann, Winter)

Instructor:

Rajeev Joshi (NASA / JPL)

Tue/Thu 1 - 2:25 P.M.
Annenberg 107

1st lecture on 9/26 will be in ANB-106

9 units (3 - 0 - 6)
Prerequisite: CS1 or equivalent