SCIENCESPRINGDAY

FCT FACULDADE DE CIÊNCIAS E TECNOLOGIA UNIVERSIDADE NOVA DE LISBOA

DEPARTAMENTO DE INFORMÁTICA

Functional Programming Assertions

SOFTWARE SYSTEMS / PLASTIC Team

CHI CENTER FOR INFORMATICS AND INFORMATION TECHNOLOGIES

Tiago Santos

(PhD Student)

Advised by Luís Caires

Research Focus on Program Verification

Objectives

We aim at providing an **effective support** for **reasoning about imperative programs** with **data structures** and **aliasing**, by extending the expressiveness of more familiar type-based verification towards more informative logical reasoning, without compromising soundness and completeness.

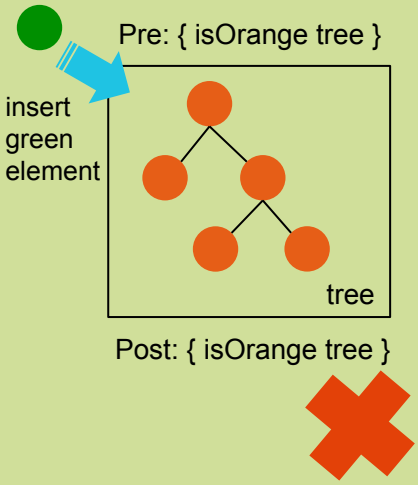
Reasoning about this type of programs, in particular about the global and shape properties of data structures, is still a major challenge for program verification. Existing tools require too much effort, a lot of experience from the user (e.g. jStar, Dafny), and rely on mechanisms that don't scale.

```
decl rec isOrange t =
  case t of
  null → true
  | {e:x, l:t1, r:t2} →
      x = "orange"
      and isOrange t1
      and isOrange t2
```

Methodology

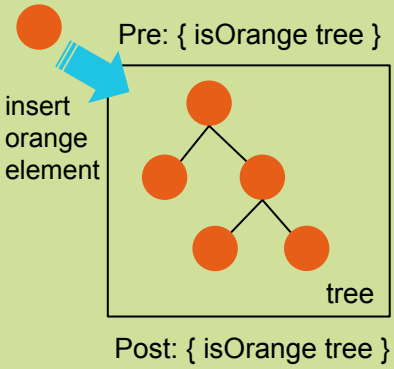
We propose an **assertion language** that is a **purely functional programming language** to express assertions (preconditions, postconditions, and invariants) in object-based imperative programs with data structures and aliasing.

We develop a **novel formal system** composed by a set of **inference rules** based on Hoare Logic, where we **reason statically** about programs using an algorithmic approach with an equational system. In order to express global and shape properties of data structures we rely on abstractions of the functional programming language (e.g. iterators and recursive functions).



Expected Results

- A core imperative programming language that manipulates data structures;
- A functional specification language for specifying imperative programs;
- A formal system to reason about global/shape properties of programs that manipulate data structures and a decision procedure to automate proofs with this approach;
- Correctness results for the formal system;
- A prototype of a programming language that uses this verification process.



Funding:

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

PEst-OE/EEI/UI0527/2011