Certified Programming in the heavy presence of pointers
The case for Union-Find

Simão Melo de Sousa
Departamento de Informática
Universidade da Beira Interior

This document in pdf (link).

Abstract

We present a methodology to get correct-by-construction OCaml programs using the Why3 tool.

First, a formal behavioral specification is given in the form of an OCaml module signature extended with type invariants and function contracts, in the spirit of JML.

Second, an implementation is written in the programming language of Why3 and then verified with respect to the specification.

Finally, an OCaml program is obtained by an automated translation.

Several data structures and algorithms have been designed and proved correct within this setting. We will take the opportunuty in this talk to illustrate our methodology with the design and proof of a union-find library.

Slides

Slides for the tutorial talk "Certified Programming in the heavy presence of pointers - The case for Union-Find"(link)

Slides for the short talk "Certified Programming in the heavy presence of pointers - The case for Union-Find"(link) any comments are welcomed and appreciated: (please make the obvious changes to the email address) : desousa_ @ _di.ubi.pt