Verificação Dedutiva de Programas em Why3

Simão Melo de Sousa
Departamento de Informática
Universidade da Beira Interior

Este documento na versão pdf (link).

Aviso

Parte significativa do material a seguir apresentado foi retirado de duas formações Why3 ministradas (e gentilmente cedidas) pelo *Jean-Christophe Filliâtre* (link)

- Deductive Program Verification with Why3 - A Tutorial, Jean-Christophe Filliâtre, Lecture at EJCP 2015 (link)
- An Introduction to Deductive Program Verification, Jean-Christophe Filliâtre, Lecture at the Sixth Summer School on Formal Techniques (link)

Site da plataforma Why3: *Why3 - Where Programs Meet Provers (link)*

Interface web Why3: *Try why3 online (link)*

Resumo

Esta aula introduz os conceitos elementares e as técnicas próprias da verificação dedutiva de programas, como os invariantes de ciclo, contratos de

funções, provas de terminação, código *ghost*, modelação de estruturas de dados, pre-condições mais fracas, etc.

É dada particular atenção ao uso de sistemas de prova automática no processo de verificação e no omnipresente compromisso entre especificações elegantes e provas totalmente automáticas.

Os exemplos apresentados na aula usam a plataforma Why3 e a componente prática, que propõe verificação deductiva de pequenos programas desafiantes, que segue deve ser resolvida nesta mesma plataforma

Material

- Slides - Contexto da Verificação de Programas (PDF)
- Slides - Verificação Dedutiva de Programas em Why3 (PDF)

Ficheiros usados na aula:

- `demo_logic.why`
- Checking Large Routine (Turing, 1949)
- John McCarthy's 91 function
- Boyer and MJRTY algorithm
- Same fringe
- Ring buffer
- Hash tables
- Binary search

Práticas Laboratoriais

Estas aulas laboratoriais podem usar a versão online da plataforma why3 (link) ou então o executável que pode ser instalado localmente no computador (ver neste (link) um resumo do processo de instalação).

No caso do uso da versão online, terá de selecionar o exercício no menú no topo da interface web e em seguida de completar o ficheiro carregado.

As questões associadas ao exercício estão apresentadas no topo do ficheiro (em inglês).

Caso necessário, poderá consultar a biblioteca *standard* Why3 (link).

No caso do uso do aplicativo *standalone*, o aplicativo poderá ser invocado via o comando: `why3 ide file.mlw`

Os exercícios

- Euclidean division: `ex1_eucl_div.mlw` (solução)
- Factorial: `ex2_fact.mlw` (solução)
- Ancient Egyptian multiplication: `ex3_multiplication.mlw` (solução)
- Two way sort: `ex4_two_way.mlw` (solução)
- Dijkstra's Dutch national flag: `ex5_flag.mlw` (solução)
- Ring buffer: `ex6_buffer.mlw` (solução)
- Inorder traversal of a tree: `ex7_fill.mlw` (solução)

Leituras auxiliares recomendadas

- Alan M. Turing. Checking a large routine. 1949.
- C. A. R. Hoare. An Axiomatic Basis for Computer Programming. Communications of the ACM. 1969.

Enviar comentários e dúvidas para (retire os UUU) : desousaUUU@UUUdi.ubi.pt