A Heap of Problems

Thomas Tuerk

University of Cambridge

May 5th, 2009

Motivation

- there is a number of good separation logic / shape analysis tools
  - Smallfoot
  - Smallfoot RG
  - SLAyer
  - Space Invader
  - ...
- however, reasoning about content remains a challenge
- even full-functional verification of *list-reversal* is not trivial
- tools use different languages / methods
- so, comparing tools is difficult

A Heap of Problems

- *A Heap of Problems* (`http://wiki.heap-of-problems.org`) collects benchmark examples
- these examples might help to compare different tools
- hopefully, this will further communication
- *A Heap of Problems* is realised as a wiki
- everyone is welcome to contribute
- there are tool-descriptions and discussion pages as well
- other contributions are welcome as well

Examples

- examples usually consist of
  - a natural language description
  - a pseudo-code implementation
  - a C-implementation
  - proofs using different tools
  - these proofs might contain different implementations as well
  - e. g. there are Java and ACL2 implementations
- at the moment there are just single-linked list examples
  - list reverse
  - list copy
  - list filter
  - mergesort
  - ...
- more examples are about to come
- you are welcome to contribute your own examples

Tools

- all examples are originally *Smallfoot* examples
- *Smallfoot* is able to prove specifications of them that just consider the shape
- *Holfoot* is able to prove full-functional specifications
- *Jahob* can be used to verify properties of Java-programs
- Rockwell-Collins contributed their proof of list-reversal using *ACL2*
- *lightweight-separation* examples are about to be added by Holger Gast