Inductive proofs in proof assistants

Anders Mörtberg – Programming Logic group

April 9, 2013

“Program testing can be used to show the presence of bugs, but never to show their absence!”

Dijkstra (1970) (EWD249)

Proofs using proof assistants?

- Proving is hard – can computers help us?

Proofs using proof assistants?

- Proving is hard – can computers help us?
- Proof assistants: Agda, Coq, Isabelle, HOL, PVS, ...

Induction/recursion

- Many structures in computer science are inductively defined: numbers, lists, trees, ...
- Can we use proof assistants to reason about them?

Agda Demo!

Formal proofs: Some success stories

- Paris Métro Line 14 – Automated subway line, verified using B-method
- seL4 operating system kernel – absence of buffer overflows, memory leaks, etc. proved using HOL/Isabelle
- CompCert – Certified C compiler written in Coq
- Big mathematical theorems: Four color theorem (map coloring), Odd-order theorem (classification of finite groups), Kepler conjecture (sphere packing), ...

Questions?