Engineering Methods for Ensuring Program Correctness

K. Rustan M. Leino
Principal Researcher

24 Mayo 2012
Some formal methods at Microsoft

- Model checking: Static Driver Verifier
- White-box fuzzing: SAGE
- Semantic differencing: SymDiff
- Program verification: VCC, Dafny
Program verification

- Automatic decision procedures (SMT solvers)
- Interactive proof assistants
- Hand proofs (or hand waving)

Technology:
- Dafny and others
- Extended static checking
- Traditional mechanical program verification

Human effort vs. Assurance level:
- Functional correctness
- Limited checking
Dafny

- Class-based language
  - generic classes, no subclassing
  - object references, dynamic allocation
  - sequential control
- Built-in specifications
  - pre- and postconditions
  - framing
  - loop invariants, inline assertions
  - termination
- Specification support
  - Sets, sequences, inductive datatypes, ...
  - User-defined recursive functions
  - Ghost variables
Basic features
demo
TreeFill.dfy, BinarySearch.dfy, SchorrWaite.dfy
Classes

demo

Counter.dfy
Proving lemmas

demo

Induction.dfy, TortoiseHare.dfy
Meet the family

- Boogie
- Boogie x86
- Region Logic
- Eiffel (EveProofs)
- Chalice
- Dafny
- HAVOC (C)
- VCC (C)
- Spec#
- Corral
- QED
- GPUVerify
- Poirot

Related tools:
- SMT Lib
- Z3
- SymDiff
- Inference

Microsoft Research Faculty Summit 2012
Riviera Maya, Mexico | May 23-25 | In partnership with CONACYT
Dafny users

- Used in teaching
- >100,000 unique Dafny programs submitted to rise4fun.com
- 6 teams of out 29 made use of Dafny at the VSTTE 2012 program verification competition
- 2 of 6 medalists at the competition used Dafny
Using Dafny on the web

Dafny tutorial

Dafny is a language and program verifier for functional correctness. Dafny is an imperative, object-oriented programming language with classes and inductive datatypes, and specification constructs for describing intended behavior. The Dafny verifier checks that programs live up to their specifications.
What’s next

• More use
• More teaching
• Refinement – programming in stages
• Synthesis – programming by specification
Conclusions

• Full functional-correctness verification is becoming more automatic

• Dafny
  • Use
  • Teach
  • Extend

• Dafny (download, source, documentation)
  http://research.microsoft.com/dafny
  http://rise4fun.com/Dafny/tutorial/guide

• rise4fun
  http://rise4fun.com

• Verification Corner
  http://research.microsoft.com/verificationcorner