A Tour of Dafny

K. Rustan M. Leino
Principal Researcher
Microsoft Research
Reasoning about programs

- Central to any programming task
  - From safety critical applications to scripting
  - From initial development to maintenance to debugging
- Minimizes faults, security problems, time/cost to market
- Thinking skill

- How do we teach?
Program verification

- Functional correctness
  - Dafny and others
  - Limited checking
    - Extended static checking
      - Decision procedures (SMT solvers)
  - Interactive proof assistants
    - Traditional mechanical program verification
  - No machine assistance
    - Hand proofs (or hand waving)
Dafny

- Object-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
Demo

Dafny
Use tools without installation

RiSE4fun

Click on a tool to load a sample then ask!

taggle bec boogie code contracts concurrent revisions dafny esm fine heapdbg poirot

method Main() {
    print "hello, Dafny\n";
    assert 10 < 2;
}

Is this program correct? Click 'ask dafny'! Read more or watch the video.

explore projects live permalink developer about

© 2011 Microsoft Corporation - Terms of Use - Privacy

Microsoft Research
References

Tools:
- Dafny: research.microsoft.com/dafny
- Spec#: research.microsoft.com/specsharp
- VCC: research.microsoft.com/vcc

Tools in browser:
- Rise4fun.com

Verification Corner (videos on verification)
- research.microsoft.com/verificationcorner
© 2011 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.