Using Dafny to reason about programs

K. Rustan M. Leino
Principal Researcher, Microsoft Research, Redmond
Visiting Professor, Imperial College London
What is Dafny?

A programming language and a program verifier and an integrated development environment (IDE)
Dafny

Dafny is a programming language designed for reasoning.

It has features drawn from:
- Imperative programming
  - `if, while, :=, class, ...`
- Functional programming
  - `function, datatype, codatatype, ...`
- Proof authoring
  - `lemma, calc, ...

Gentle learning curve

High automation
- Verifier built on Boogie/Z3
Some applications

IronClad (MSR, 30,000+ lines)
CloudMake (Microsoft)
Specification and refinement of FreeRTOS (Cleveland State U.)
ExpressOS (UIUC)
Static verification and dynamic testing (ETH Zurich)
Standard POPL verification applications from Coq textbooks (EPFL, MSR)
Education

Used in teaching at a growing number of universities
  Imperial College London, Rice, Moscow State U.,
  Caltech, CMU, Princeton, ETH Zurich, KSU, U. Toronto, U. Iowa, Koç U.,
  UNSW, NUI Maynooth, UW, Eindhoven Technical U., Ohio State U.,
  U. Lisboa, U. Basque Country, Yale, ...

140,000 uses on rise4fun last fall

Textbook in progress (authored using Madoko)
Dafny IDE
Conclusions

Dafny is a programming language and program verifier
Its language features are used for both programs and proofs
Use, teach, extend

Run Dafny in your browser:
rise4fun.com/dafny

Binary download, sources, test cases, discussion board
dafny.codeplex.com

Verification Corner on youtube:
research.microsoft.com/verificationcorner
Also, see Nada Amin’s talk “How to write your next POPL paper using Dafny”