Microsoft® Research
FacultySummit

A Tour of Dafny

K. Rustan M. Leino
Principal Researcher
Microsoft Research

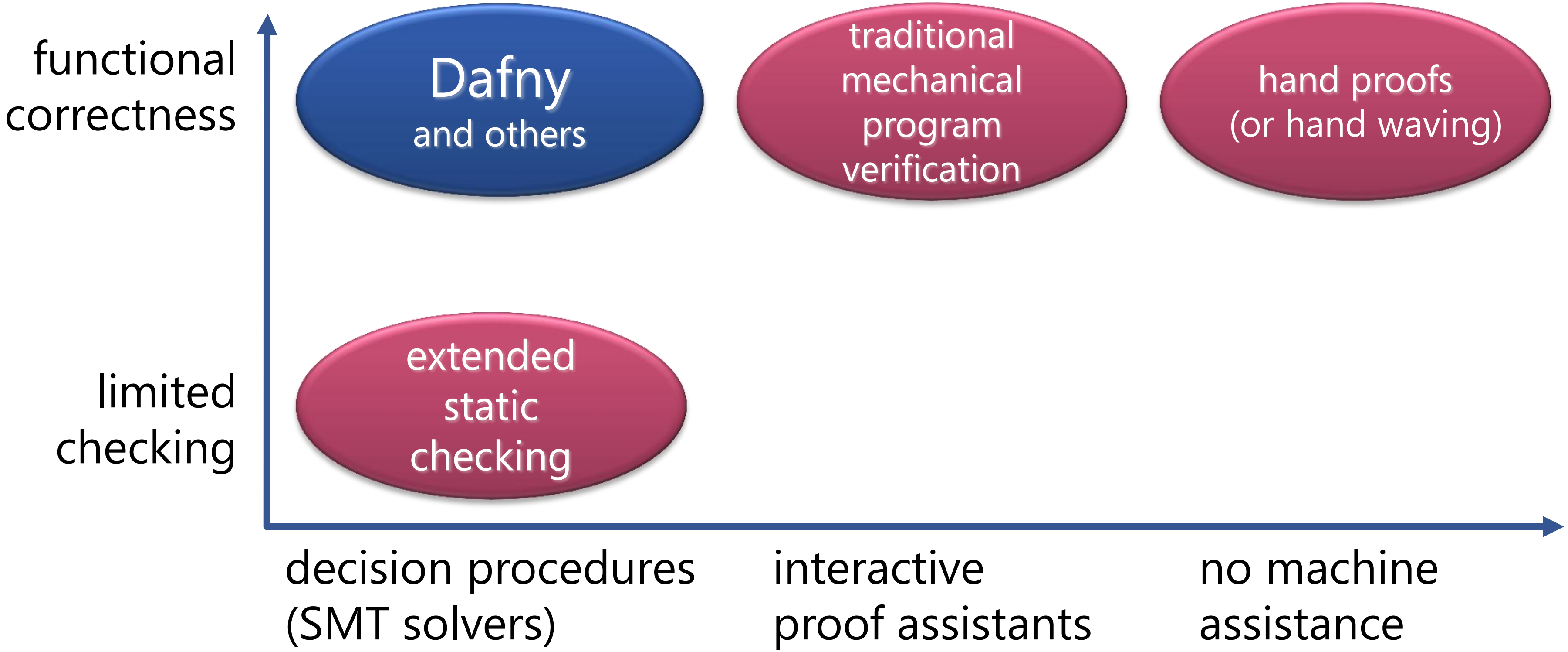
2031
FUTURE WORLD
2011

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
limited checking
Dafny
and others
traditional mechanical program verification
hand proofs (or hand waving)
extended static checking
decision procedures (SMT solvers)
interactive proof assistants
no machine assistance

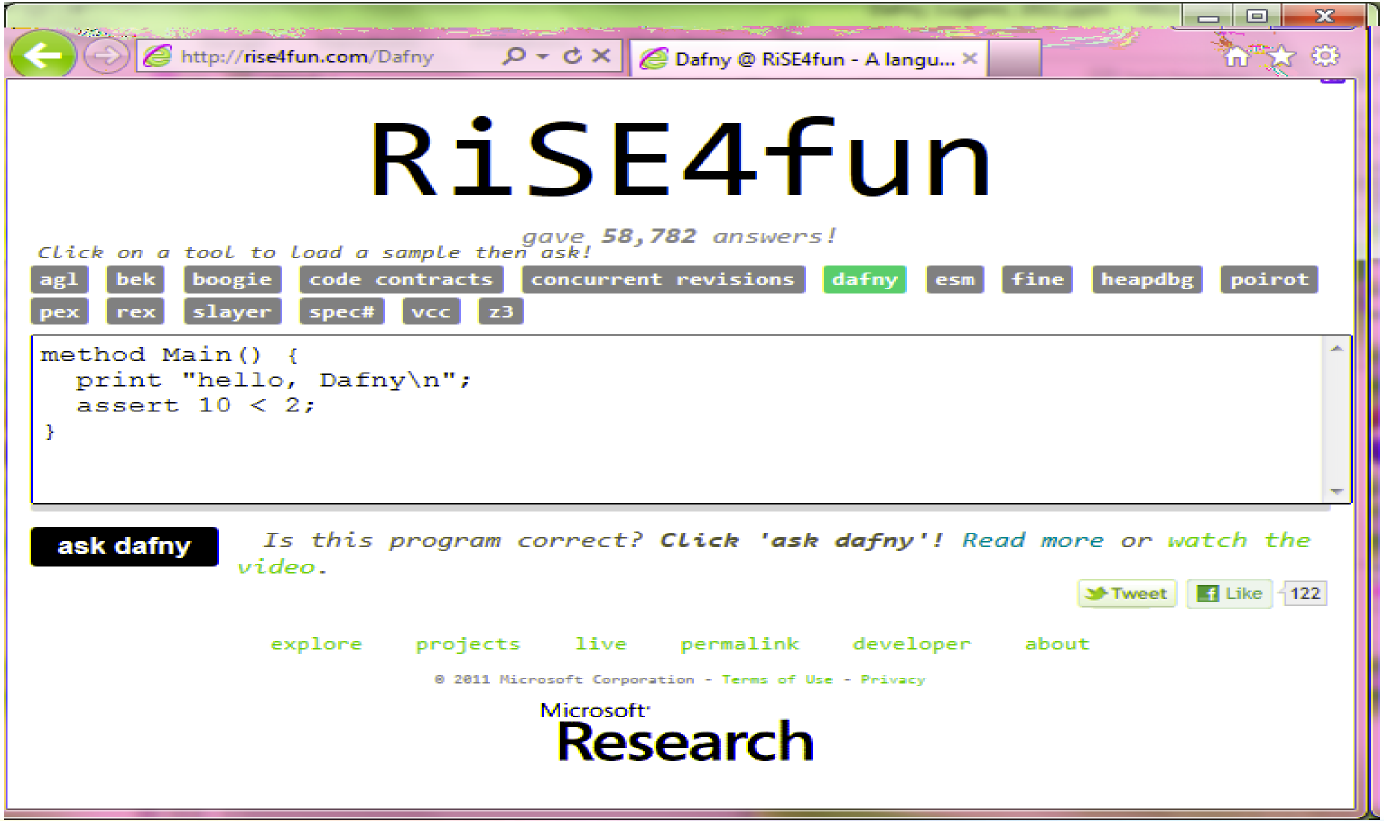
Dafny

- 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

gave 58,782 answers!

Click on a tool to load a sample then ask!

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

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

© 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

Microsoft Research
FacultySummit

2031
FUTURE WORLD
2011

Microsoft® Research
FacultySummit

2031

FUTURE WORLD

2011