

A Tour of Dafny

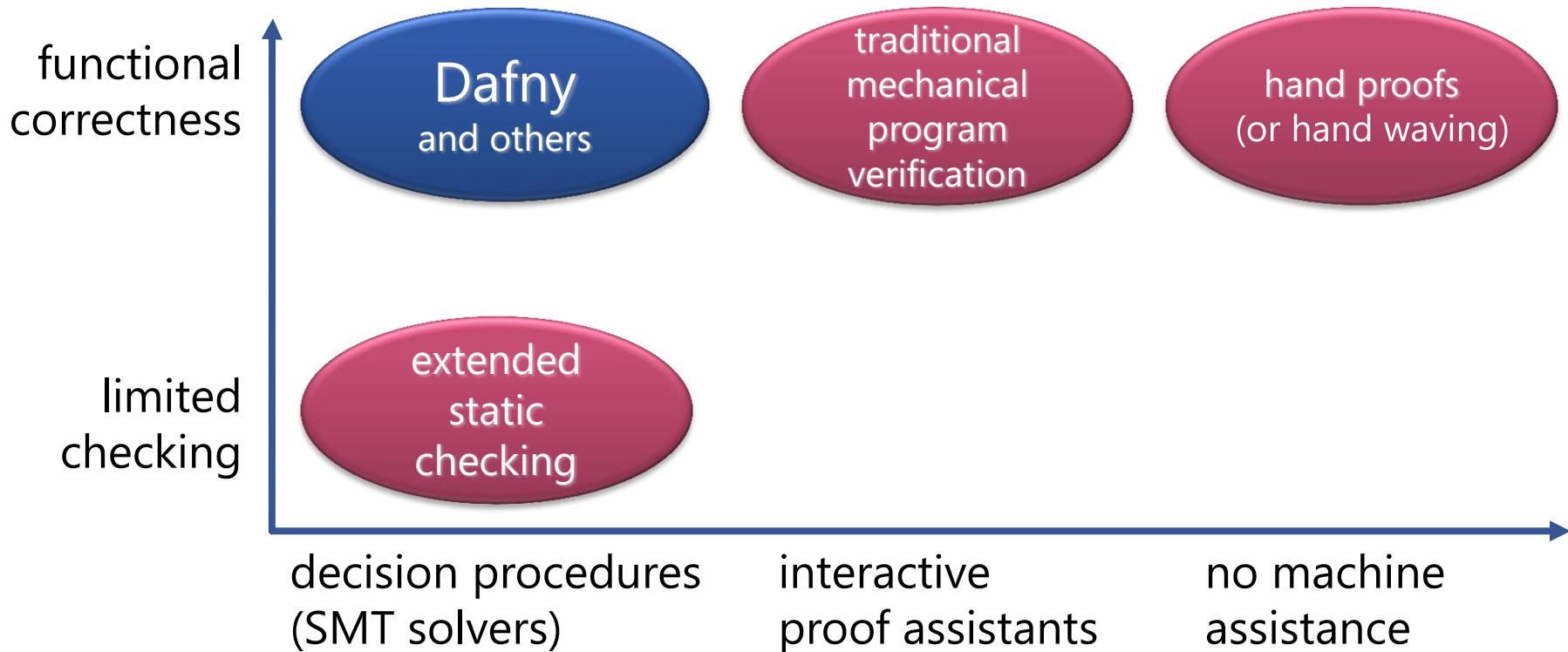
K. Rustan M. Leino
Principal Researcher
Microsoft Research

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



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



Microsoft Research
FacultySummit

DEMO

Dafny

FUTURE WORLD
2011 ————— 2031

Use tools without installation

The screenshot shows a web browser window with the URL `http://rise4fun.com/Dafny`. The page content includes:

- Header: **RiSE4fun**
- Text: *gave 58,782 answers!*
- Text: *Click on a tool to load a sample then ask!*
- Buttons: `agl`, `bek`, `boogie`, `code contracts`, `concurrent revisions`, `dafny` (highlighted), `esm`, `fine`, `heapdbg`, `poirot`, `pex`, `rex`, `slayer`, `spec#`, `vcc`, `z3`
- Code Editor:

```
method Main() {
  print "hello, Dafny\n";
  assert 10 < 2;
}
```
- Text: **ask dafny** *Is this program correct? Click 'ask dafny'! Read more or watch the video.*
- Social Media: `Tweet` and `Like` (122)
- Footer: `explore`, `projects`, `live`, `permalink`, `developer`, `about`
- Copyright: © 2011 Microsoft Corporation - [Terms of Use](#) - [Privacy](#)
- Logo: Microsoft Research

References

- Tools:
 - Dafny: research.microsoft.com/dafny
 - Spec#: research.microsoft.com/specsharp
 - VCC: research.microsoft.com/vcc
- Tools in browser:
 - [Rise4fun.com](https://rise4fun.com)
- Verification Corner (videos on verification)
 - research.microsoft.com/verificationcorner



Microsoft Research
Faculty Summit

© 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.

Microsoft Research

Faculty Summit



FUTURE WORLD

2011 ← → 2031