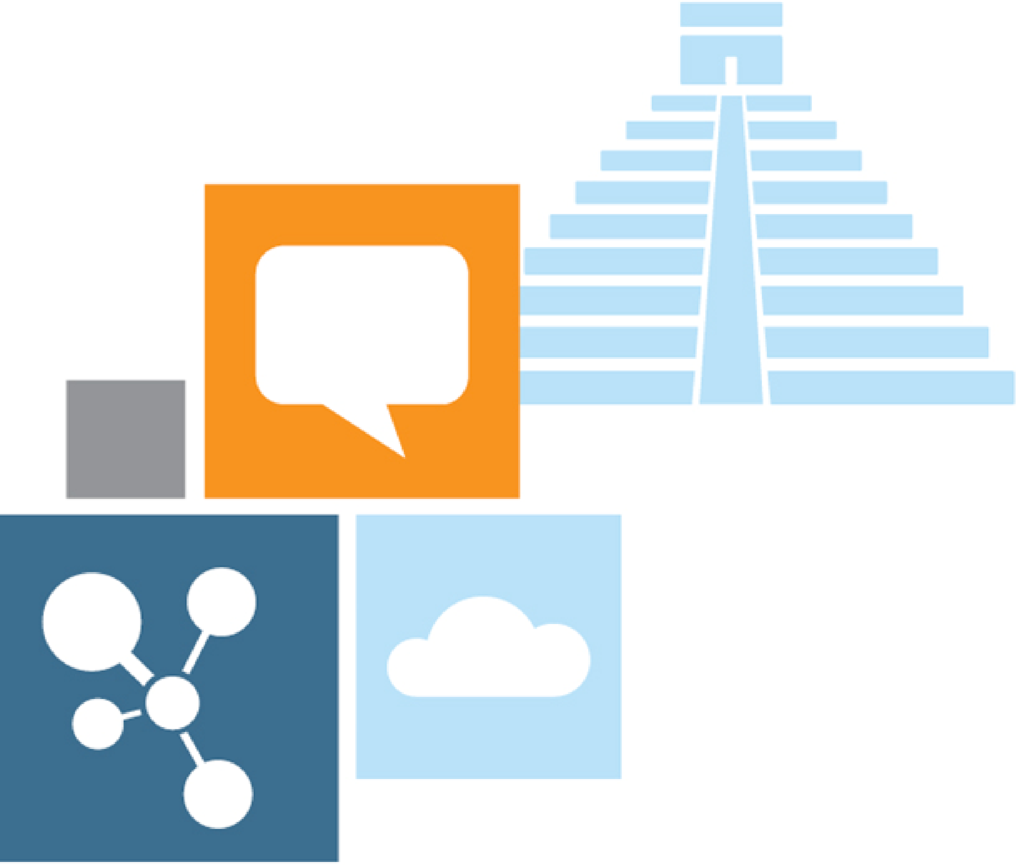
Microsoft



Microsoft® Research

Faculty Summit 2012

Riviera Maya, Mexico | May 23-25 | In partnership with CONACYT

Engineering Methods for Ensuring Program Correctness

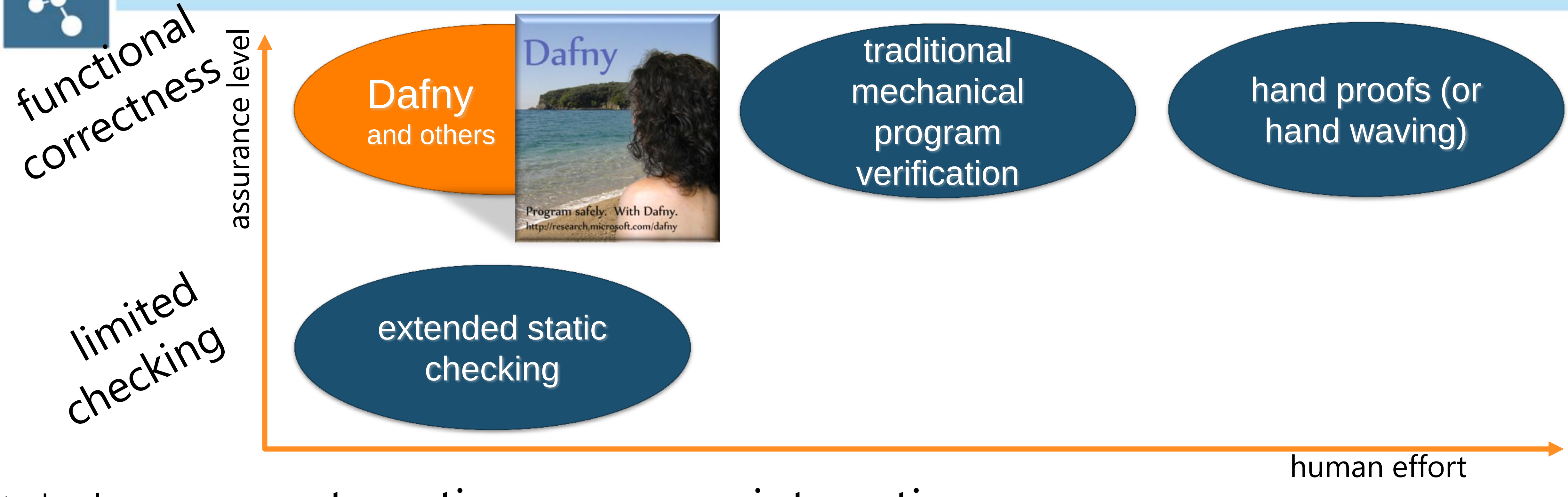
K. Rustan M. Leino
Principal Researcher

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



functional correctness

limited checking

assurance level

Dafny
and others

Dafny

Program safely. With Dafny.
http://research.microsoft.com/dafny

traditional mechanical program verification

hand proofs (or hand waving)

extended static checking

human effort

technology:

automatic decision procedures (SMT solvers)

interactive proof assistants

no machine assistance

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

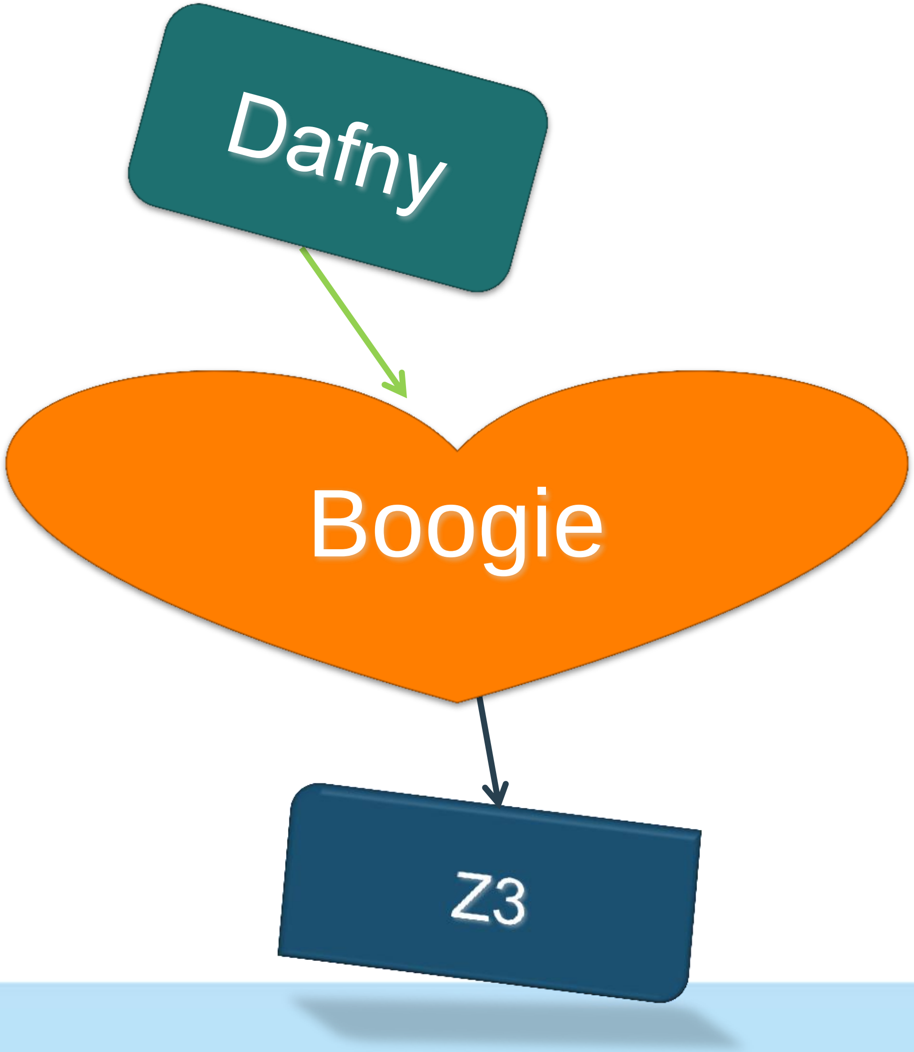
Counter.dfy

Proving lemmas

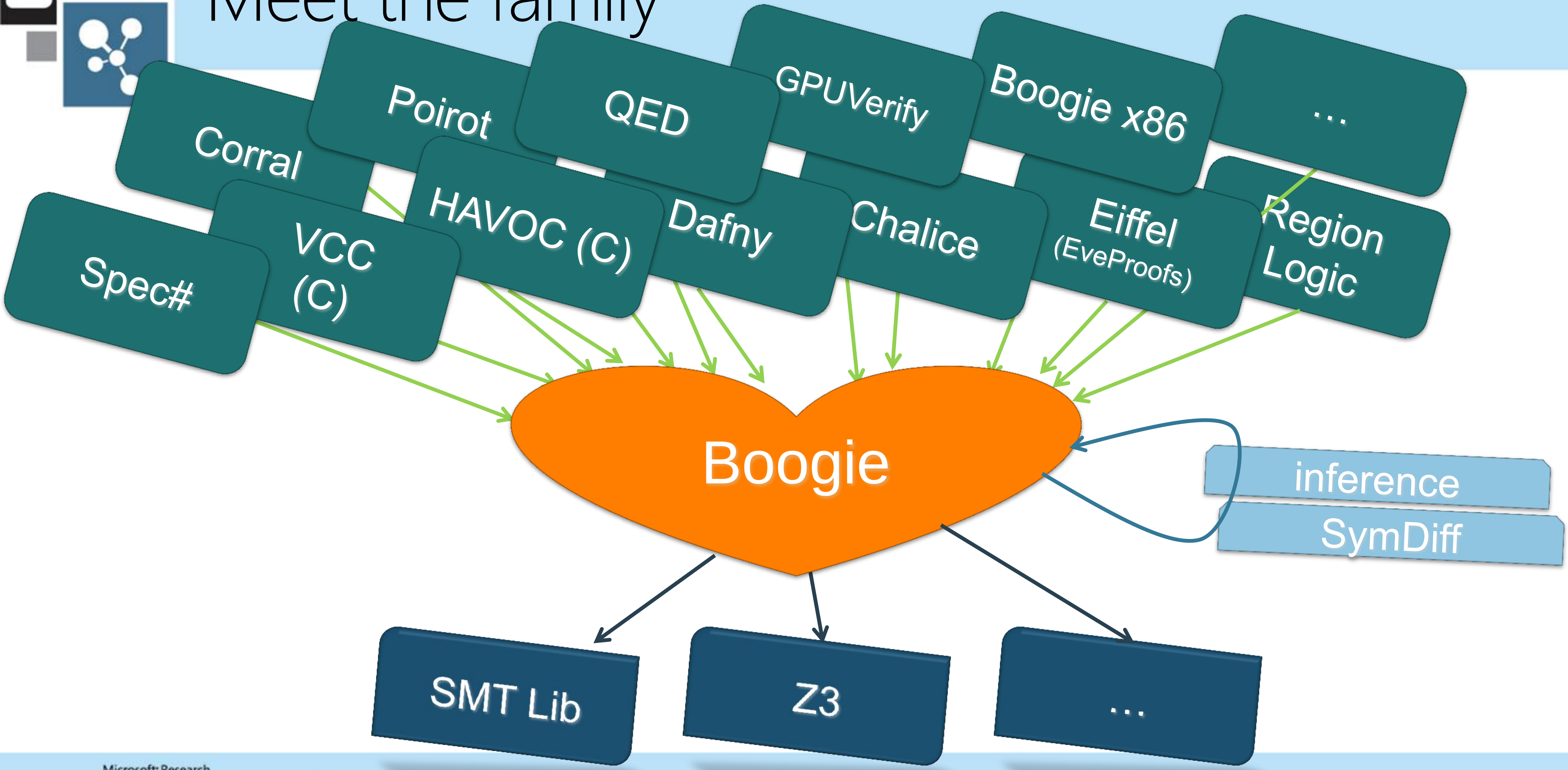
demo

Induction.dfy, TortoiseHare.dfy

Verification architecture



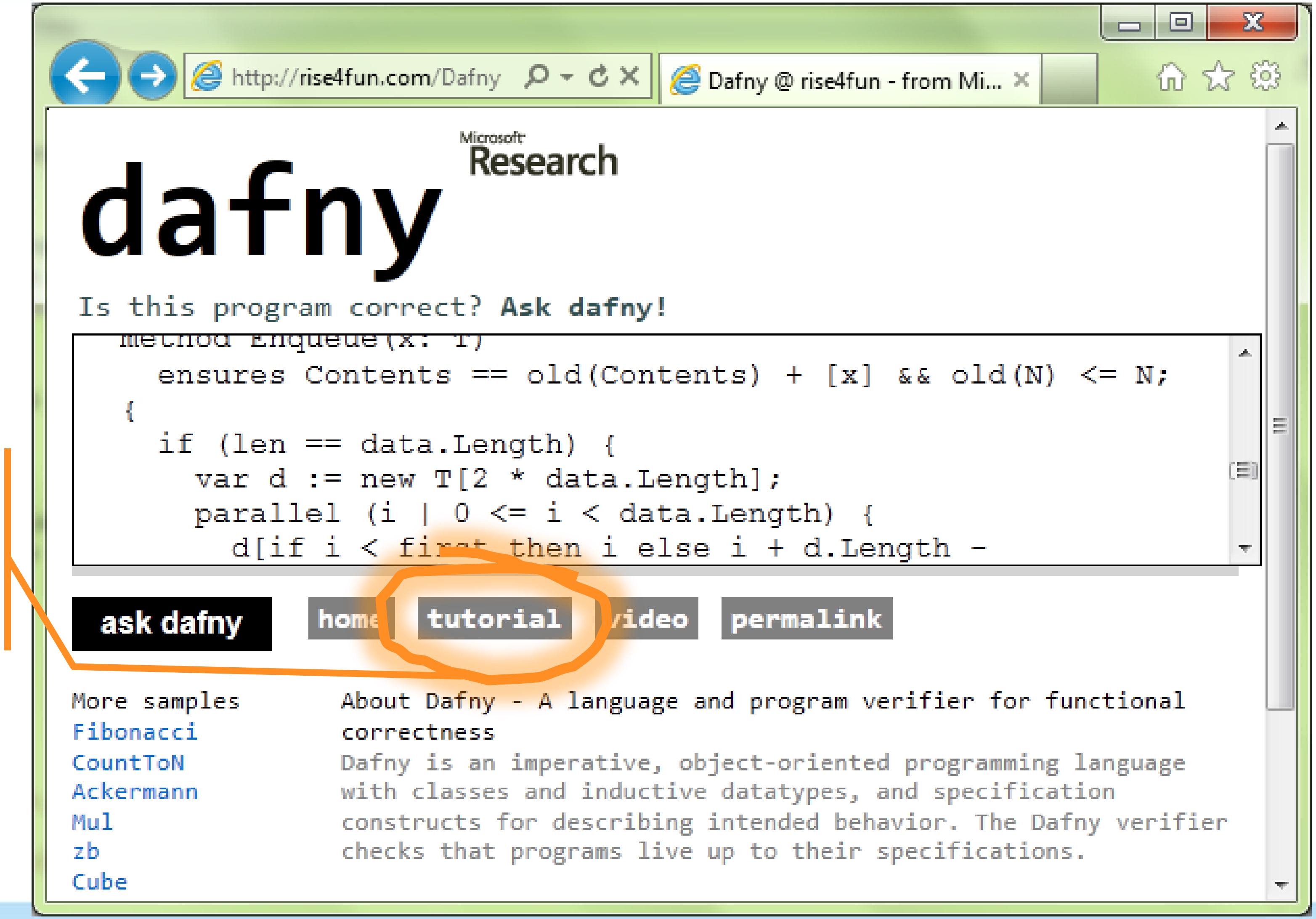
Meet the family



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



Is this program correct? **Ask dafny!**

```
  method Enqueue(x: T)
    ensures Contents == old(Contents) + [x] && old(N) <= N;
  {
    if (len == data.Length) {
      var d := new T[2 * data.Length];
      parallel (i | 0 <= i < data.Length) {
        d[if i < first then i else i + d.Length -
```

More samples
Fibonacci
CountToN
Ackermann
Mul
zb
Cube

About Dafny - 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.

Dafny tutorial

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

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

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

Verification Corner

Microsoft®

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.