

Dafny

Testing, Quality Assurance, and Maintenance
Winter 2018
Prof. Arie Gurfinkel

based on slides by K. Rustan M. Leino and Gudmund Grov



Wasn't that easy?!

Problems with bugs in your code?
Doctor Rustan's tool to the rescue!

When: Tuesday March 20, 2012 at 13:15 - 15:00

Where: E1, Osquars backe 2, KTH

<http://www.csc.kth.se/tcs/seminarsevents/rustanleino.php>

Get to know how debugging your code gets the simple look and feel of spell checking in Word.*
See some of the latest and most exciting research in formal verification deployed in action.
This will be a hands-on tutorial, so bring your own laptop to try it out for yourself.

Rustan Leino from Microsoft Research is a world-leading expert in the area. Those who have seen his presentations know why programming is cool.

You don't want to miss this!



*1 Your mileage may vary. Do not use when operating heavy machinery.
Prolonged excitement from using programming tools may cause drowsiness.
Some users report a sensation of increased and irresistible social attraction.
If you experience bug withdrawal, consider collecting pet armadillos.

Dafny

Programming language
designed for *reasoning*

Language features drawn from:

Imperative programming

if, while, :=, class, ...

Functional programming

function, datatype, codatatype, ...

Proof authoring

lemma, calc, refines, inductive predicate, ...

Program verifier

Integrated development environment (IDE)



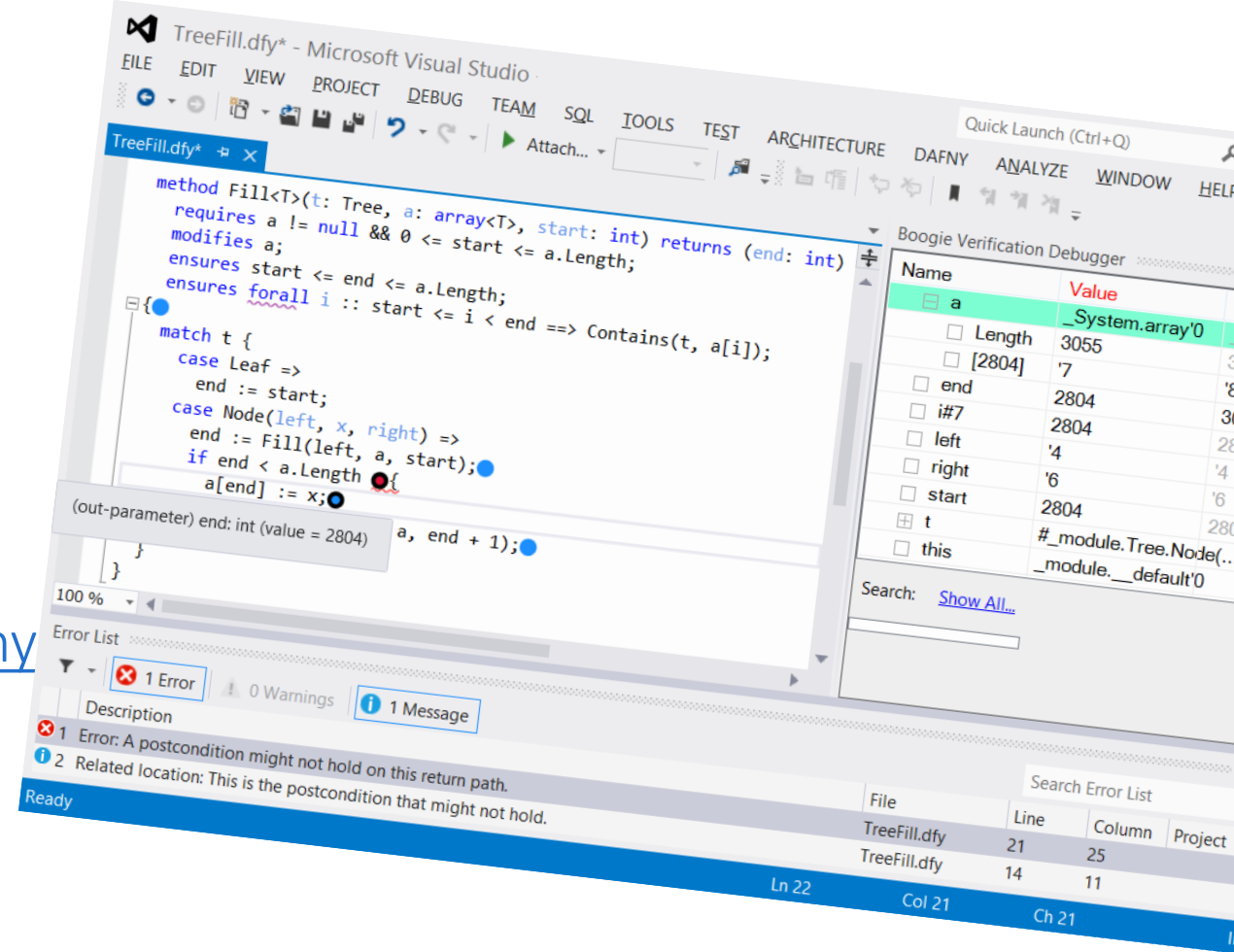
Using Dafny

Dafny IDE in Visual Studio

Dafny mode in Emacs

In web browser at <http://rise4fun.com/dafny>

<http://github.com/Microsoft/Dafny>

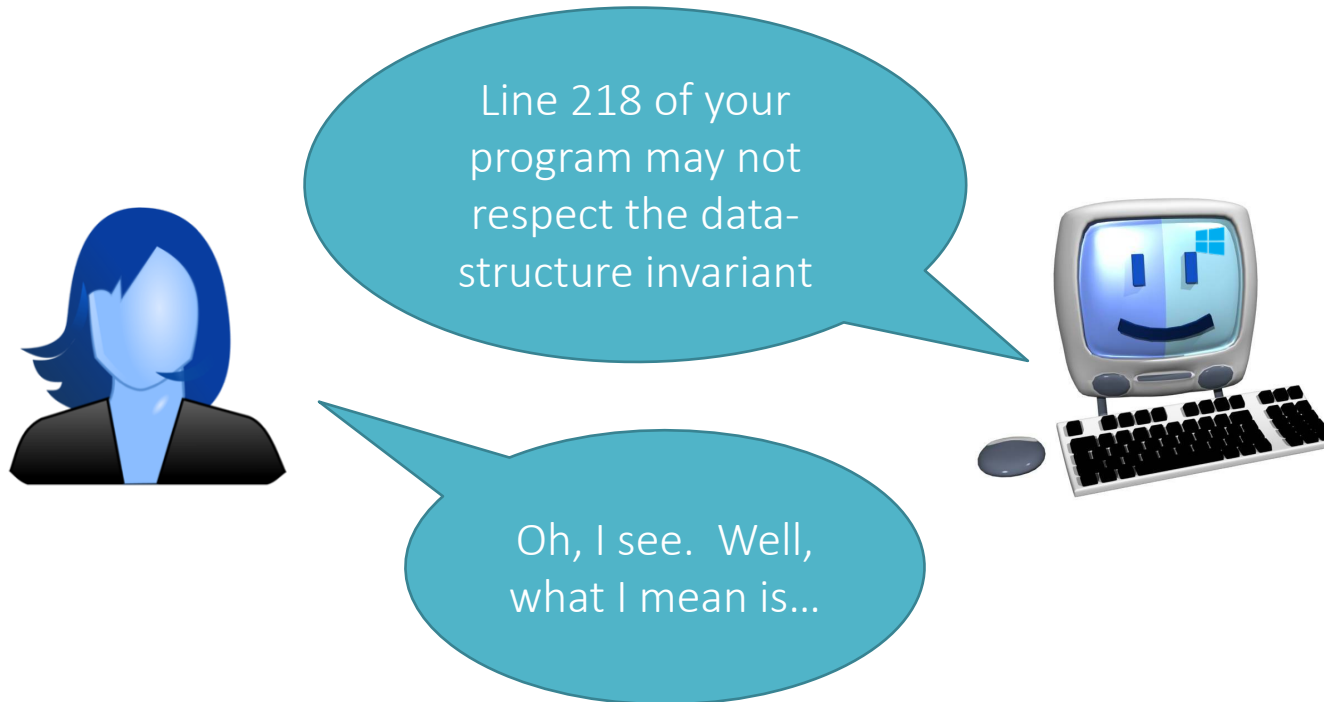


Involving the programmer

Opportunities

Tool's analysis can be customized and targeted

Allows interaction with tool, like a programmer's apprentice



Projects that involve the programmer

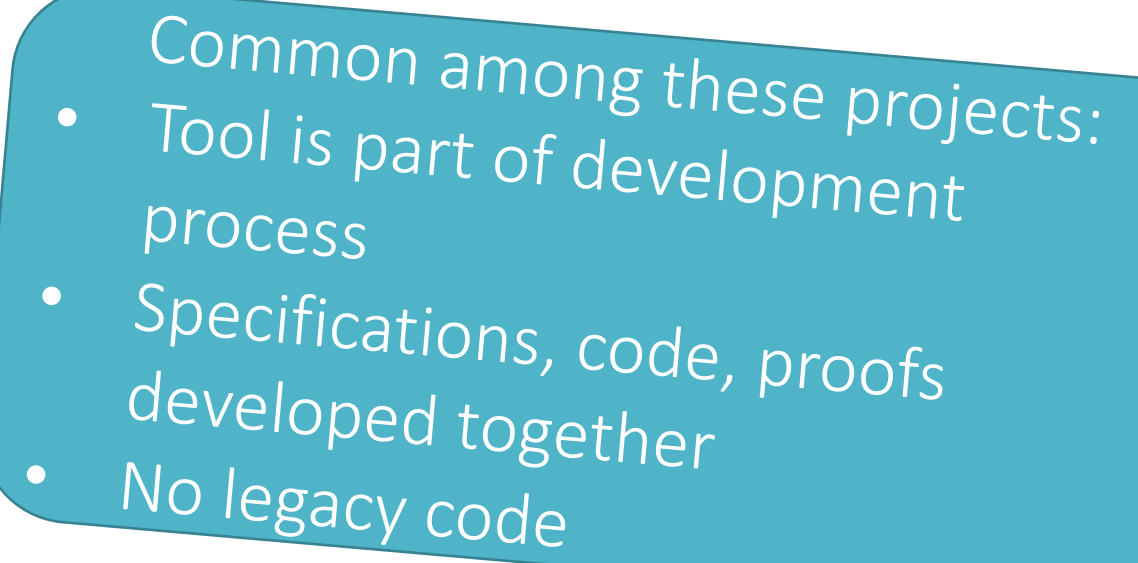
Paris Metro line 14 brake system (B)

seL4 Verified (Haskell, Isabelle/HOL, C)

CompCert (Coq)

Ironclad (Dafny)

...

- 
- Common among these projects:
- Tool is part of development process
 - Specifications, code, proofs developed together
 - No legacy code

Involving the programmer

- Paris Metro line 14 brake system (B)
- seL4 Verified (Haskell, Isabelle/HOL, C)
- CompCert (Coq)

Verification done
by formal-method
experts

- Ironclad (Dafny)

Verification done
by systems
programmers

Uses of Dafny

In projects

- ExpressOS [ASPLOS 2013]

- CloudMake algorithms [FM 2014]

- Ironclad Apps [OSDI 2014]

- IronFleet [SOSP 2015]

In teaching

- At over 30 universities

Dafny pipeline



Reasoning about loops

A loop invariant

holds at the top of every iteration

is the *only* thing the verifier remembers from one iteration to another
(about the variables being modified)

It is as if the loop body were not available

```
while B
{
    S;
}
```

Loop invariant holds here

A diagram illustrating the concept of a loop invariant. It shows a code snippet for a while loop. A curved blue arrow starts from a point labeled 'Loop invariant holds here' and points back to the condition 'B' of the while loop, indicating that the invariant is maintained across iterations.

Use Dafny on your machine

Install Dafny

<http://github.com/Microsoft/dafny>

-> binary downloads and Setup

Install Visual Studio (Windows)

<https://www.visualstudio.com/vs/community/>

-> run DafnyLanguageService.vsix in Dafny distribution

On Linux and OS X platforms, **install Mono**

Use in your web-browser

<http://rise4fun.com/dafny>

Conclusions

Functional-correctness
verification is becoming
more automatic

Dafny

Use

Teach

Extend

research.microsoft.com/dafny

Papers

rise4fun.com/dafny

Use in your web browser

On-line tutorial

github.com/Microsoft/dafny

Binaries

Sources

Discussion forum

research.microsoft.com/verificationcorner

Videos

-- now on YouTube

