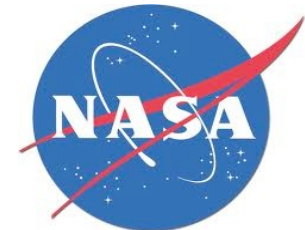
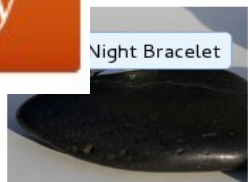


Experience Report: a Do-it-Yourself High-Assurance Compiler

Lee Pike Galois, Inc. <leepike@galois.com>
Nis Wegmann University of Copenhagen
Sebastian Niller Unaffiliated
Alwyn Goodloe NASA Langley Research Center



Do-It-Yourself

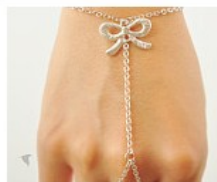


Night Bracelet

Ring Sterling Silver and Aqu...
BelViaggioD... \$64.00 USD



Delicate Ball Chain, Neon P...
Bumhemian \$15.95 USD



Textured Ribbon Pendant, E...
Bumhemian \$18.60



Necklace "tree of words"
BEATAREN \$20.00 USD



Leaf Branch and Metal Bird ...
SujinSimple... \$16.50 USD

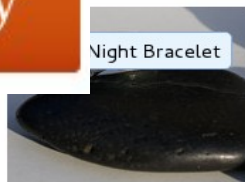


Sterling Silver Chain & Rho...
SenseYou \$22.00



Do-It-Yourself

Etsy



Ring Sterling Silver and Aqu...
BelViaggioD... \$64.00 USD



Delicate Ball Chain, Neon P...
Bumhemian \$15.95 USD



Textured Ribbon Pendant, B...
Bumhemian \$18.60



Necklace "tree of words"
BEATAREN \$20.00 USD



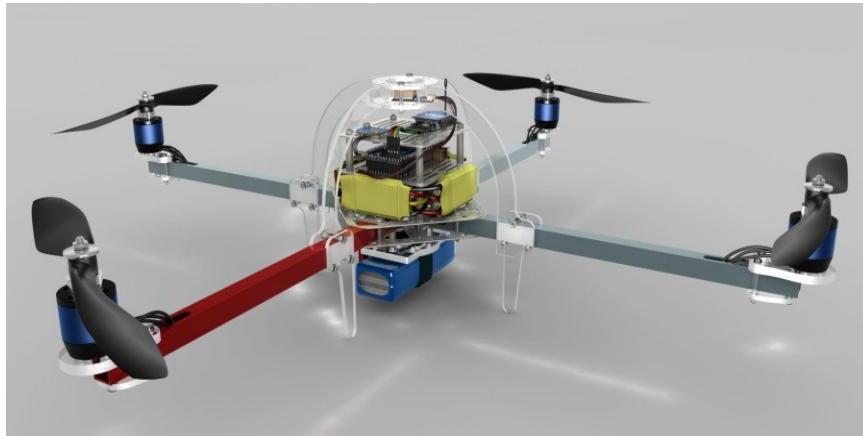
Leaf Branch and Metal Bird ...
SujinSimple... \$16.50 USD



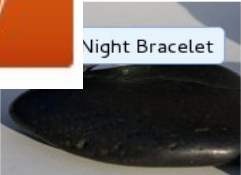

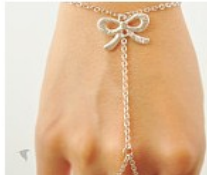






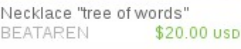
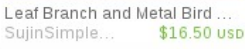



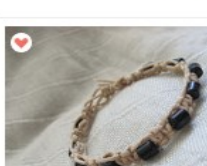
Sterling Silver Chain & Rho...
SenseYou \$22.00



Do-It-Yourself



Etsy

 <p>Night Bracelet</p>	 <p>Delicate Ball Chain, Neon P...</p>	 <p>Textured Ribbon Pendant, B...</p>
 <p>Ring Sterling Silver and Aqu...</p>	 <p>Delicate Ball Chain, Neon P...</p>	 <p>Textured Ribbon Pendant, B...</p>
 <p>Necklace "tree of words"...</p>	 <p>Leaf Branch and Metal Bird ...</p>	 <p>Sterling Silver Chain & Rho...</p>
 <p>Necklace "tree of words"...</p>	 <p>Leaf Branch and Metal Bird ...</p>	 <p>Sterling Silver Chain & Rho...</p>
 <p>Necklace "tree of words"...</p>	 <p>Leaf Branch and Metal Bird ...</p>	 <p>Sterling Silver Chain & Rho...</p>

The Anthrax Killer: Did They Get the Wrong Guy? | The Cocaine Smuggler's Submarine | 10 Cool New Gadgets, Tested and Rated | INSIDE THE SHAKE-UP AT GOOGLE

WIRED

The DIY Revolution Starts Now

HOW TO Make Stuff

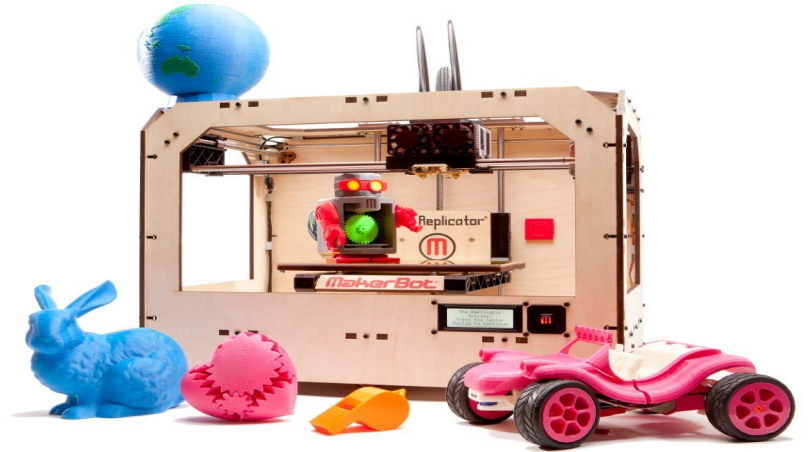
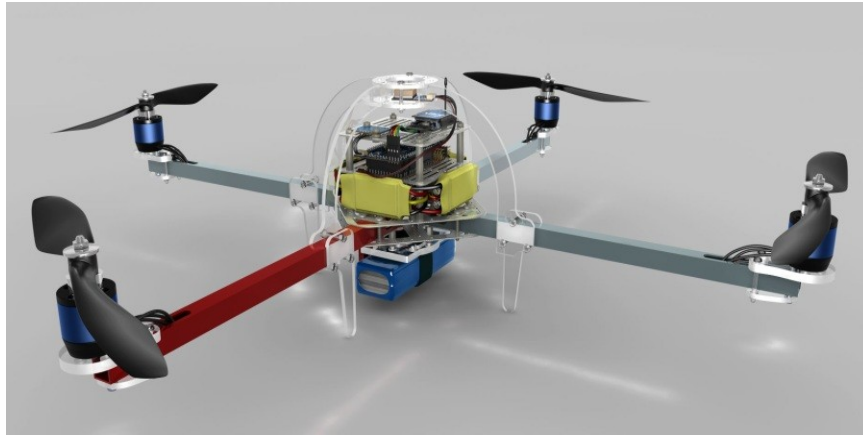
25 AWESOME PROJECTS

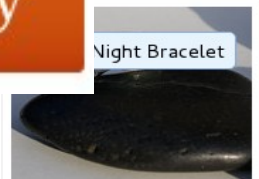

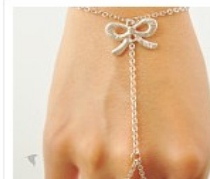


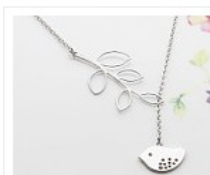


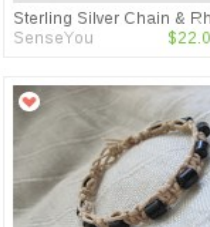
under construction | april 2011

If You Can Think It, You Can Build It!

Maker Hero
Lance Priod

Do-It-Yourself



 <p>Night Bracelet</p>	 <p>Delicate Ball Chain, Neon P...</p>	 <p>Textured Ribbon Pendant</p>
<p>Ring Sterling Silver and Aqu... BelViaggioD... \$64.00 USD</p>	<p>Bumhemian \$15.95 USD</p>	<p>Bumhemian \$18.60 USD</p>
 <p>Necklace "tree of words" BEATAREN \$20.00 USD</p>	 <p>Leaf Branch and Metal Bird ... SujinSimple... \$16.50 USD</p>	 <p>Sterling Silver Chain & Rh... SenseYou \$22.00 USD</p>
		



WIREHEAD

The DIY Revolution Starts Now

HOW TO Make Stuff

25 AWESOME PROJECTS

under construction | april 2013

If You Can Think It, You Can Build It!

Maker Hero
Lance Priddy

High-Assurance

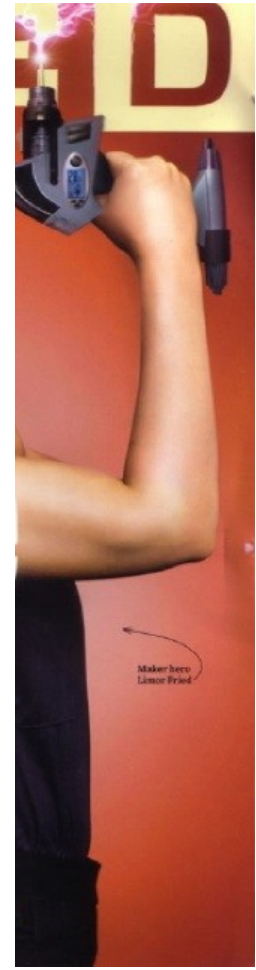
Compilers

Principles, Techniques,
and Tools

Alfred V. Aho
Ravi Sethi
Jeffrey D. Ullman



DIY



3 Not-So-Secret Weapons

1. Embedded domain-specific languages (EDSLs)
2. A *verifying* (not verified) compiler approach
3. Open source testing/verification libraries & tools

National ?? and Space Administration

National **Aeronautics** and Space Administration



Copilot: a Run-Time Monitoring DSL

- Embedded DSL in Haskell
- Synthesize monitors for real-time embedded systems
- Stream language
- Generates Misra-like C
- Constant time, constant memory
 - Synthesized scheduler
 - No RTOS needed

Sample Copilot specification

Haskell

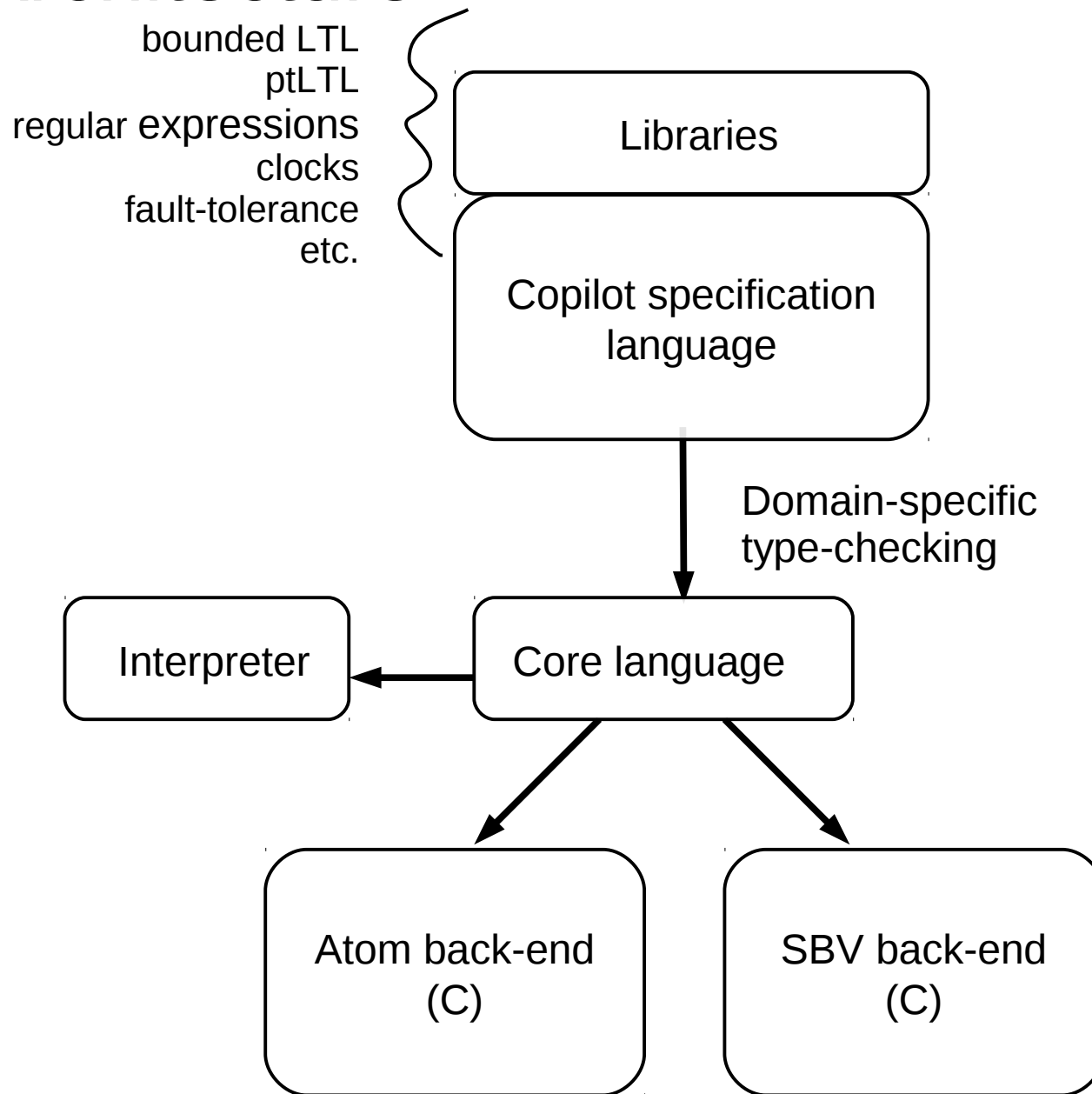
```
fib :: [Word32]
fib = [0, 1] ++ zipWith (+) fib (drop 1 fib)
```

Copilot

```
fib :: Stream Word32
fib = [0, 1] ++ (fib + drop 1 fib)
```

Special constructs for input (*sampling*) and output (*triggers*)

Copilot Architecture



Lessons in DIY Assurance

- Who monitors the monitor?



- Challenges:
 - EDSLs encourage rapid language design changes
 - Industrial work often doesn't “pay” for assurance (but wants it)

Lessons in DIY Assurance

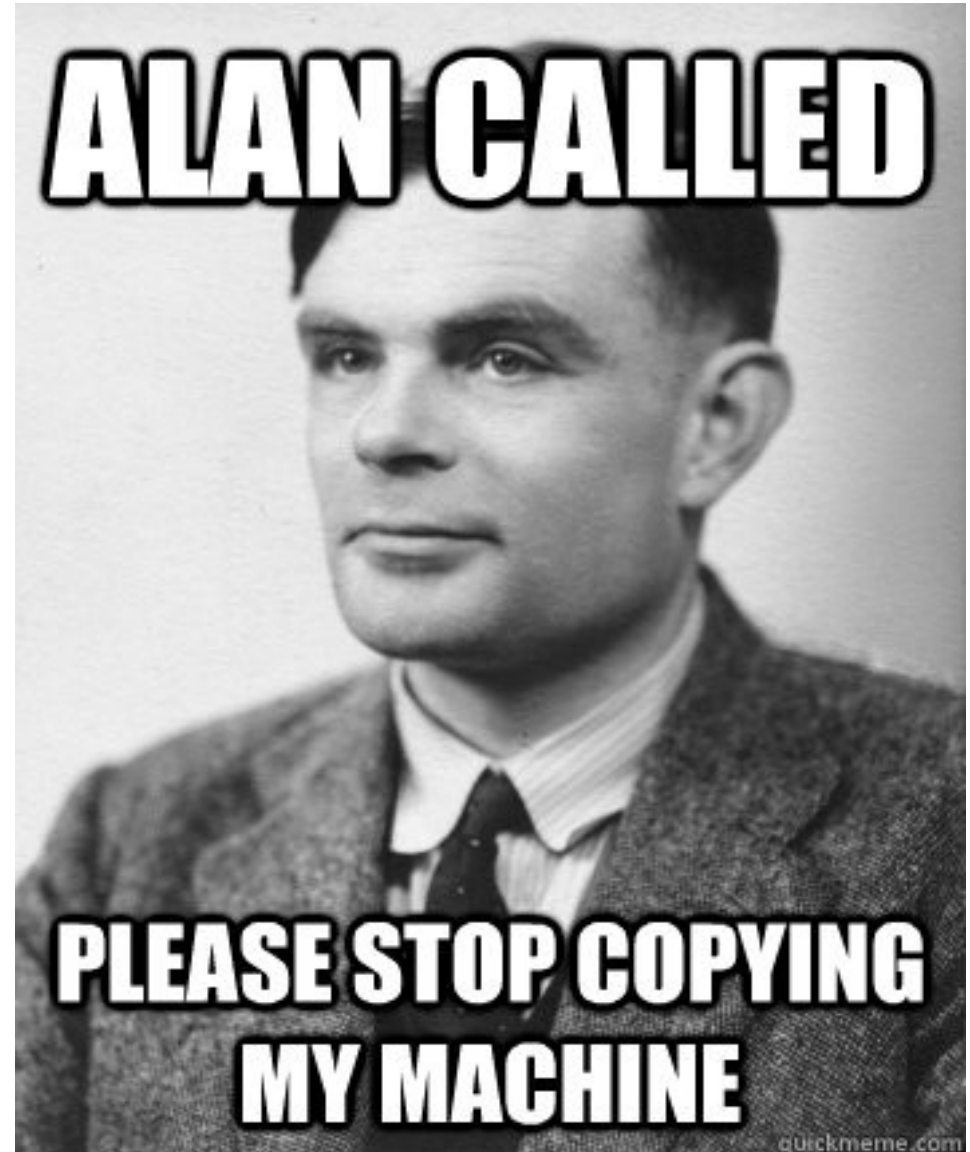
Solution: DIY assurance

- Turing *incomplete* DSLs, Turing complete macros
- Multi-level type-checking
- Cheap testing & proofs
- Unified host language

Lesson #1: Turing-Incompleteness

Turing *incompleteness* means:

- Compiler writing is simplified
- Compiler reasoning is better (e.g., termination analysis)
- Security is improved
- Automated verification has a chance of working!



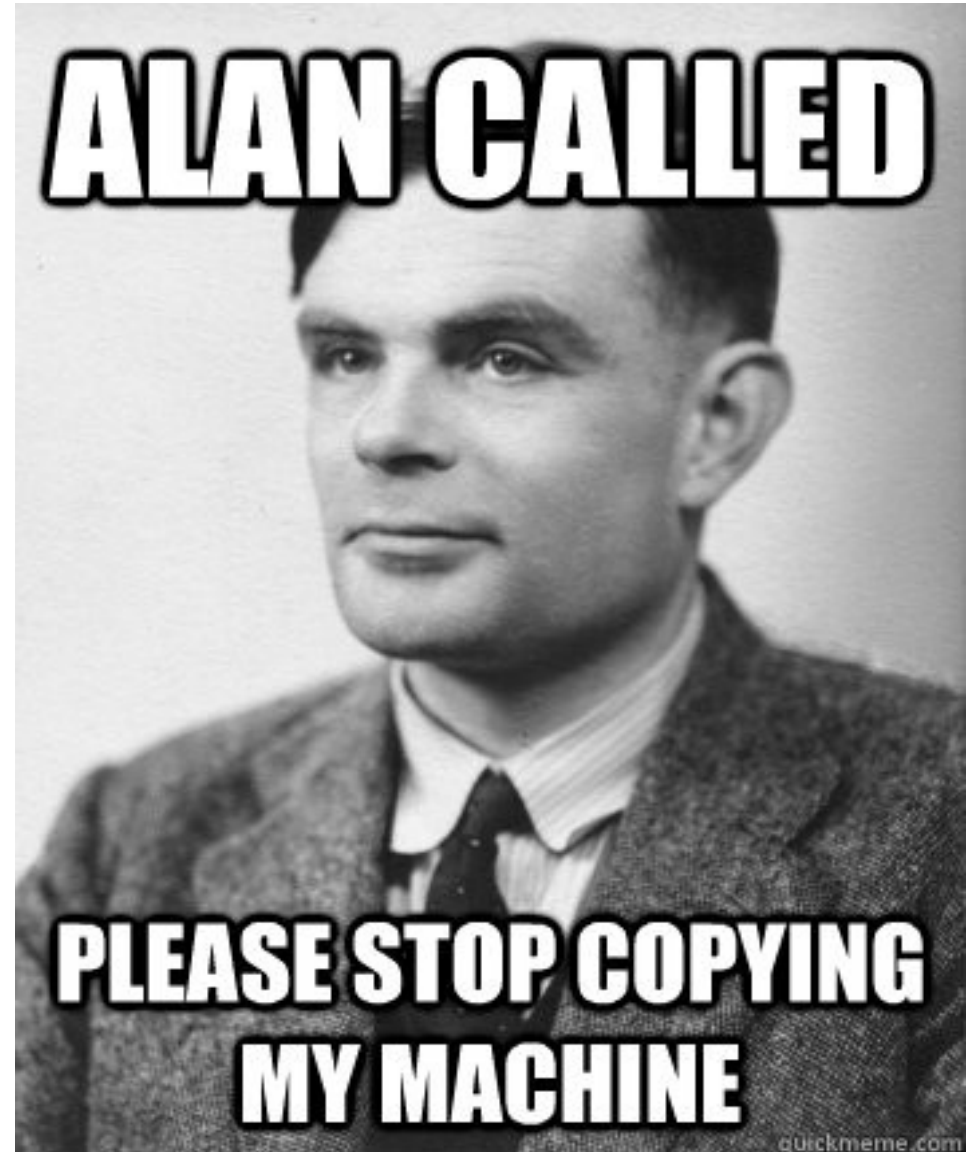
Lesson #1: Turing-Incompleteness

Turing *incompleteness* means:

- Compiler writing is simplified
- Compiler reasoning is better (e.g., termination analysis)
- Security is improved
- Automated verification has a chance of working!

Have your cake and eat it, too:
In an embedded DSL, the *host* language is Turing-complete!

Programs specialized at compile time.





Lesson #2: Multi-Level Type-Checking

- Lean on Haskell's type system in the (DSL's) compiler's internal representations: e.g., GADTs
 - Leave the type system twice:
 - Pretty-print C
 - Translating between EDSLs (type-safe dynamic typing*).
 - And ensure you aren't abusing it: **Safe Haskell**

Lesson #2: Multi-Level Type-Checking

- Lean on Haskell's type system in the (DSL's) compiler's internal representations: e.g., GADTs
 - Leave the type system twice:
 - Pretty-print C
 - Translate between EDSLs (type-safe dynamic typing*).
 - And ensure you aren't abusing it: **Safe Haskell**

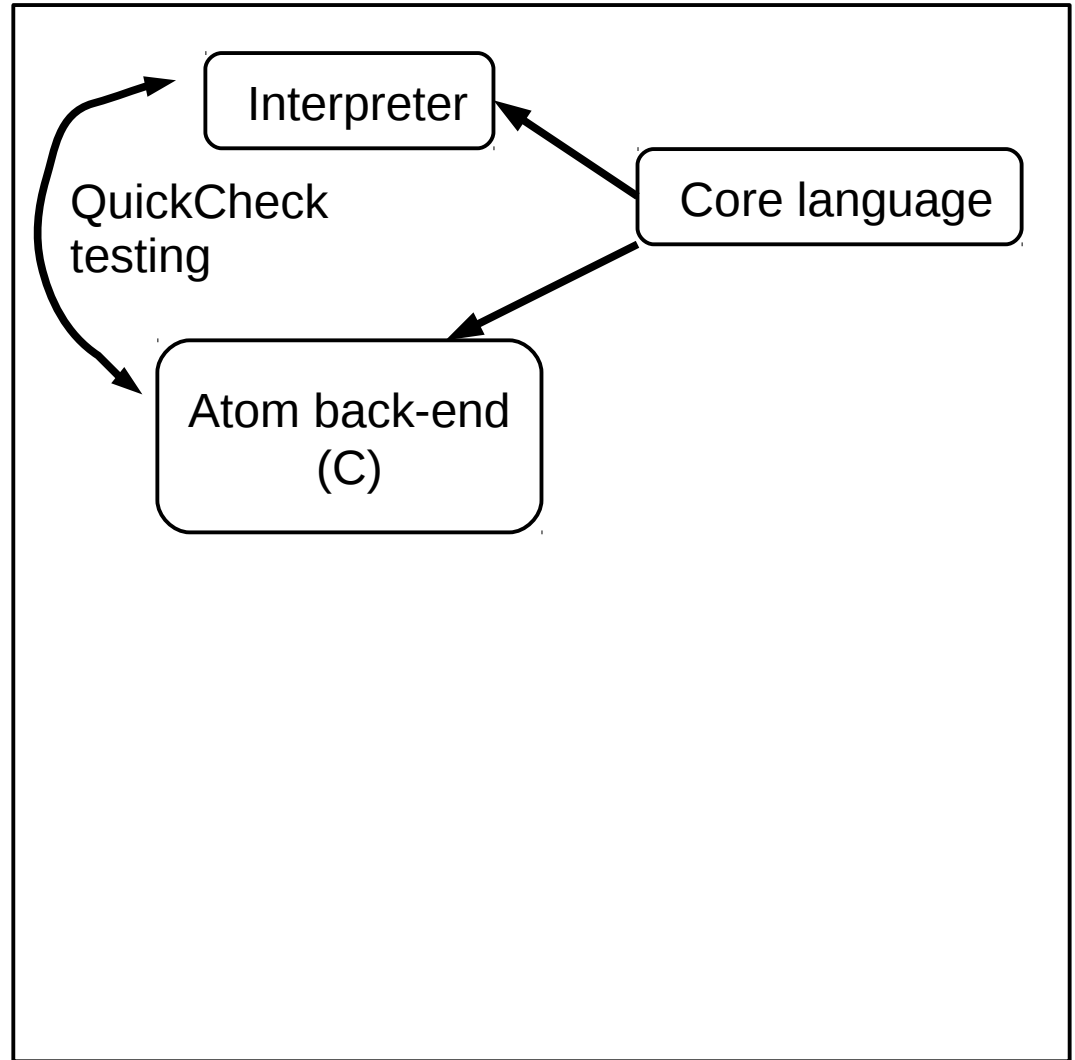
- Then a little domain-specific type-checking:
 - Productiveness:


```
x :: Stream Word64
x = [0] ++ drop 1 x
```
 - Inputs are consistently typed (e.g., external functional calls)

Lesson #3: Cheap Testing & Proofs

QuickCheck:

- Small DSLs make program generation easy with good coverage
- Test ~1.5M programs/day



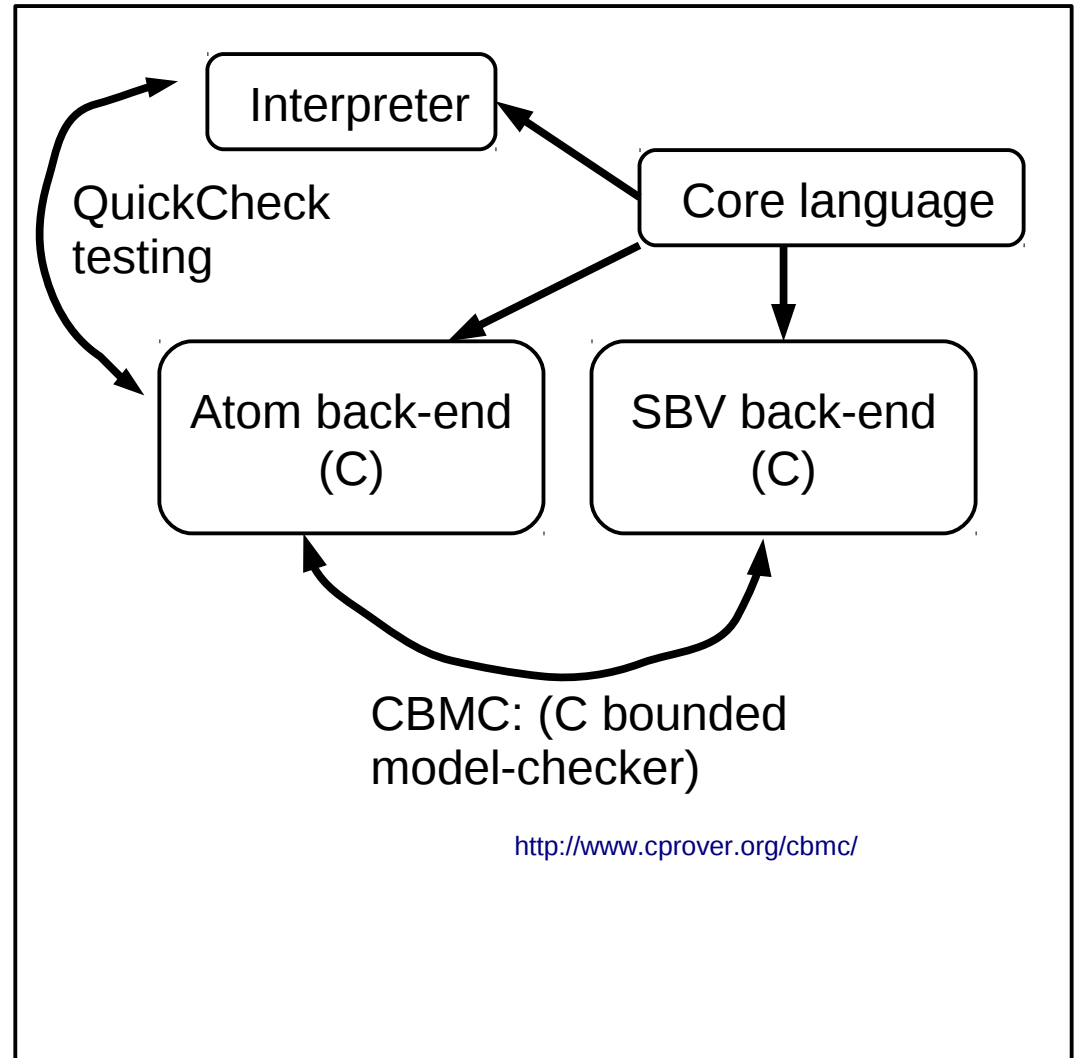
Lesson #3: Cheap Testing & Proofs

QuickCheck:

- Small DSLs make program generation easy with good coverage
- Test ~1.5M programs/day

Then **prove** back-ends agree:

- Model-checking works (better) with Turing incomplete DSLs
- EDSL simplifies driver generation



Lesson #4: a Unified Host Language

Embedded DSLs are a paradigm shift for safety-critical languages

- Fewer front-end, type-checker bugs
- “Bolting-on” new tools *within* the type system (no marshalling)
- The macro language is a build system, too!

Conclusions



Conclusions

Verified compiler

- Expensive
- Specialized skills
- Hard to make repairs
- But flawless when it works



Conclusions

Verified compiler

- Expensive
- Specialized skills
- Hard to make repairs
- But flawless when it works



Conclusions

Verified compiler

- Expensive
- Specialized skills
- Hard to make repairs
- But flawless when it works



DIY assurance

- Cheap
- Quick to build
- Easy to repair
- An “90% solution”

src: <http://designthatmatters.org/news/press/dtm-in-the-news/>