Formal verification for Scala with Leon

Romain Ruetschi

EPFL - Laboratory for Automated Reasoning and Analysis

Outline

- Bugs and crashes can be expensive
- Formal verification to the rescue
- Leon, a verification system for Scala
- Demo

Bugs and crashes can be expensive

The Cryosat satellite was lost soon after launch due to a software failure.

Cost: $135 millions

http://news.bbc.co.uk/1/hi/sci/tech/4381840.stm

Formal verification to the rescue

- Traditionally, errors in hardware and software have been discovered empirically, by testing them in many possible situations.

- The number of situations to account for is usually so large that it becomes impractical.

- Formal verification is an alternative that involves mathematically proving that a computer system will function as intended.

Formal verification of sofware

- Process of proving that a program satisfies a formal specification of its behavior, thus making the program safer and more reliable.

- Catches bugs such as integer overflows, divide-by-zero, out-of-bounds array accesses, buffer overflows, etc.

- Also helps making sure that an algorithm is properly implemented.

Leon, a verification system for Scala

Leon takes as input a Scala program where functions are annotated with contracts.

```
def neg(x: Int): Int = {
  require(x > 0)
  -x
} ensuring(res => res < 0)
```

Leon will try to prove that the post-condition always hold, assuming that the pre-condition does hold.

Repair and synthesis

- Leon can automatically repair your program if it doesn't satisify its specification.
- More importantly, it can also synthesize code from a specification!
- It does so by attempting to find a counter-example to the claim that no program satisfying the given specification exists.

Demo

https://leon.epfl.ch

Thank you!

https://lara.epfl.ch/w/leon
https://github.com/epfl-lara/leon

Under the hood

- Leon itself is written in Scala (~30k lines of code)
- It relies on an SMT solver to prove or disprove contracts.
- An SMT instance is a first-order logic formula over various theories such as real numbers, integers, lists, arrays, algebraic data types, and others.