Formal verification of Scala programs with Stainless

Romain Ruetschi

Laboratory for Automated Reasoning and Analysis, EPFL

Typelevel Summit Lausanne 2019

About me

- Romain Ruetschi (Romac)
- MSc in Computer Science from EPFL
- ~2 years as an engineer at LARA

Outline

- Stainless: Verification framework for Scala
- What Stainless verifies
- Termination checker
- Case study: Verifying typeclasses
- More case studies
- Bonus
- Coming soon / further work

Stainless: Verification framework for Scala

Stainless is a verification framework for higher-order programs written in a subset of Scala, named *PureScala*:

- Traits, abstract classes, case classes, implicit classes, methods
- Higher-order functions, lambdas
- Any, Nothing, co-/contra-variant type parameters
- Single inheritance
- Anonymous and local classes, inner functions

- Type members, type aliases
- GADTs
- `PartialFunctions`
- Set, Bag, List, Map, Array, Byte, Short, Int, Long, BigInt
- Local state, `while`, traits/classes with `vars`, and more...

Currently supports Scala 2.12.x.

Some Dotty-specific features:

- Intersection and union types
- Dependent function types
- Extension methods
- Opaque types

Currently only supports Dotty 0.12.0, will try to catch up.

What Stainless verifies

- **Assertions** which should hold at the place where they are stated, **checked statically**
- **Postconditions** using `ensuring` function: assertions for return values of functions
- **Preconditions** using `require` function: assertions on function parameters
- **Loop invariants**: inductive assertions that hold in each loop iteration after the while condition check passes
- **ADT/Class invariants**: assertions on constructors parameters (which remain true for all constructed values)

Stainless also automatically performs **automatic checks for the absence of runtime failures**:

- Exhaustiveness of pattern matching (taking guards into account)
- Division by zero, array bounds checks
- Map domain checks

Moreover, Stainless also prevents *PureScala* programs from:

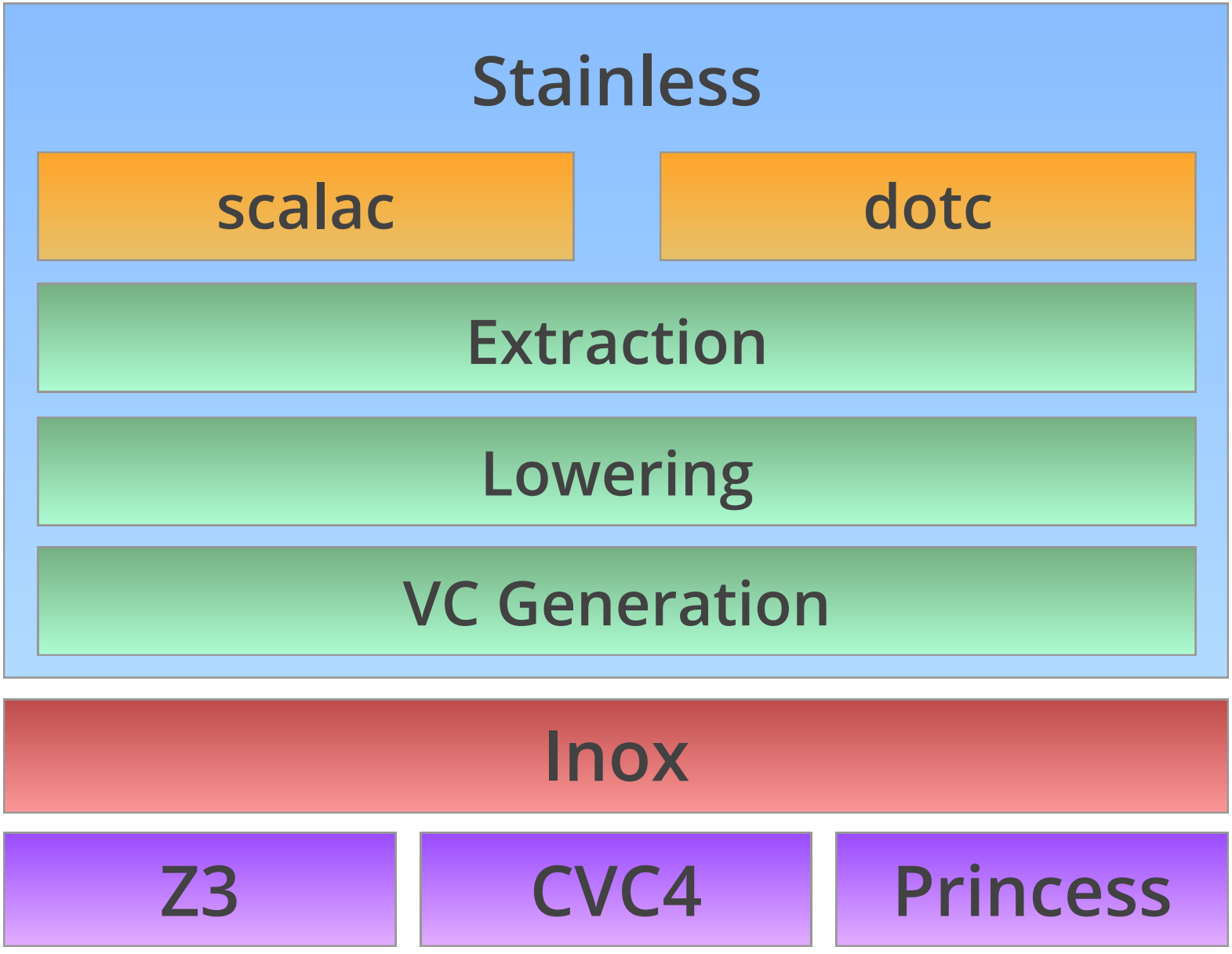
- Creating null values or unininitalized local variables or fields
- Explicitly throwing an exception
- Overflows and underflows on sized integer types

Termination checker

A *verified* function in stainless is guaranteed to never crash, however, it can still lead to an infinite evaluation.

Stainless therefore provides a termination checker that complements the verification of safety properties.

Pipeline


Stainless
scalac
dotc
Extraction
Lowering
VC Generation
Inox
Z3
CVC4
Princess

Case study: Verifying typeclasses

```
Seq(1, 2, 3, 4).par.fold(10)(_ - _)

// ((((10 - 1) - 2) - 3) - 4) => 0
// (10 - 1) - (2 - (3 - 4))   => 6
```

```
Seq(1, 2, 3, 4).par.fold(0)(_ + _)

// ((((10 + 1) + 2) + 3) + 4) => 10
// (10 + 1) + (2 + (3 + 4))   => 10
```

```
abstract class Semigroup[A] {
  def combine(x: A, y: A): A

  @law def law_assoc(x: A, y: A, z: A) =
    combine(x, combine(y, z)) == combine(combine(x, y), z)
}
```

```
abstract class Monoid[A]
  extends Semigroup[A] {

  def empty: A

  @law def law_leftIdentity(x: A) =
    combine(empty, x) == x

  @law def law_rightIdentity(x: A) =
    combine(x, empty) == x
}
```

```scala
case class Sum(get: BigInt)

implicit def sumMonoid = new Monoid[Sum] {
  def empty = Sum(0)
  def combine(x: Sum, y: Sum) = Sum(x.get + y.get)
}
```

```
val A: (Object) => Boolean = (x: Object) => x is Sum
val x: { x: Object | @unchecked A(x) } = Sum(x)
val y: { x: Object | @unchecked A(x) } = Sum(y)
val z: { x: Object | @unchecked A(x) } = Sum(z)

val res: Boolean = {
  combine(A, thiss, x, combine(A, thiss, y, z)) ==
  combine(A, thiss, combine(A, thiss, x, y), z)
}

assume(res == law_assoc(thiss, x, y, z))

res
```

```
 stainless summary

law_leftIdentity    law   valid   nativez3   0.223
law_rightIdentity   law   valid   nativez3   0.407
law_assoc           law   valid   nativez3   0.944

total: 3  valid: 3  invalid: 0  unknown: 0  time: 1.574
```

```scala
implicit def optionMonoid[A](implicit S: Semigroup[A]) =
  new Monoid[Option[A]] {
    def empty: Option[A] = None()

    def combine(x: Option[A], y: Option[A]) =
      x match {
        case None()   => y
        case Some(xv) => y match {
          case None()   => x
          case Some(yv) => Some(S.combine(xv, yv))
        }
      }
  }
```

```scala
implicit def optionMonoid[A](implicit val S: Semigroup[A]) =
  new Monoid[Option[A]] {
    // ...

    override def law_assoc(@induct x: Option[A], y: Option[A],
      super.law_assoc(x, y, z) because {
        (x, y, z) match {
          case (Some(xv), Some(yv), Some(zv)) =>
            S.law_assoc(xv, yv, zv)

          case _ => true
        }
      }
  }
```

```
val A: (Object) => Boolean = (x: Object) =>
  x is Option && isOption[Object](x.value, A)

val x: { x: Object | @unchecked A(x) } = Option(x)
val y: { x: Object | @unchecked A(x) } = Option(y)
val z: { x: Object | @unchecked A(x) } = Option(z)

x is Some ==> {
  (x, y, z) match {
    case (Some(xv), Some(yv), Some(zv)) =>
      law_assoc(A, thiss.S, xv, yv, zv)
    case _ =>
      true
  } && {
    val res: Boolean = {
      combine(A, thiss, x, combine(A, thiss, y, z)) ==
      combine(A, thiss, combine(A, thiss, x, y), z)
    }
    assume(res == law_assoc(thiss, x, y, z))
```

```
x$569 is None$0 ==> {
  // snip...
}
```

```
def foldMap[M, A](xs: List[A])(f: A => M)(implicit M: Monoid[A
  xs.map(f).fold(M.empty)(M.append)

@extern
def parFoldMap[M, A](xs: List[A])(f: A => M)(implicit M: Monoi
  xs.toScala.par.map(f).fold(M.empty)(M.append)
} ensuring { res =>
  res == foldMap(xs, f)
}
```

More case studies

Conc-Rope

Verified data-structure which provides

- Worst-case $O(logn)$ time lookup, update, split and concatenation operations
- Amortized O(1) time append and prepend operations

Very useful for efficient data-parellel operations!

[ConcRope] TODO: Ref

Parellel Map-Reduce pipeline

Fully verified implementation of the previous running example, using a Conc-Rope under the hood instead of Scala's 'par' operator.

Built by Lucien Iseli, BSc student, as a semester project. TODO: Benchmarks

Actor systems

```
case class Primary(backup: ActorRef, counter: BigInt) extends
  def processMsg(msg: Msg): Behavior = msg match {
    case Inc =>
      backup ! Inc
      PrimBehav(backup, counter + 1)

    case _ => this
  }
}
```

```
case class Backup(counter: BigInt) extends Behavior {
  def processMsg(msg: Msg): Behavior = msg match {
    case Inc => BackBehav(counter + 1)
    case _   => this
  }
}
```

```
def invariant(s: ActorSystem): Boolean =
  val primary = s.behaviors(PrimaryRef)
  val backup  = s.behaviors(BackupRef)
  val pending = s.inboxes(PrimaryRef -> BackupRef).length

  primary.counter == backup.counter + pending
}
```

```
def preserveInv(s: ActorSystem, n: ActorRef, m: ActorRef) = {
  require(invariant(s))

  val next = s.step(n, m)

  invariant(next)
}.holds
```

Smart contracts

We also maintain a fork of Stainless, called *Smart* which supports:

- Writing smart contracts in Scala
- Specifying and proving properties of such programs, including precise reasoning about the `Uint256` data type
- Generating Solidity source code from Scala, which can then be compiled and deployed using the usual tools for the Ethereum software ecosystem

[0] https://github.com/epfl-lara/smart

Bonus: Refinement types

```
type Nat = { n: BigInt => n >= BigInt(0) }
```

```
def sortedInsert(
  xs: { List[Int] => xs.nonEmpty },
  x:  { Int => x <= xs.head }
): { res: List[Int] => isSorted(res) } = {
  x :: xs // VALID
}
```

Bonus: Dependent function types

```
trait Entry {
  type Key
  val key: Key
}

def extractKey(e: Entry): e.Key = e.key

def extractor: (e: Entry) => e.Key = extractKey(_)
```

```scala
case class IntEntry() extends Entry {
  type Key = Int
  val key: Int = 42
}

assert(extractor(entry) == 42) // VALID
```

There is more!

- sbt plugin + metals integration
- Ghost context (think Dotty's erased terms but more general)
- Partial evaluation

Coming soon(ish)

- Higher-kinded types
- Better support for refinement types and type members
- VC generation via type-checking

Coming later

- Scala 2.13 / latest Dotty support
- WebAssembly backend
- and more...

Learn more

- Installation
- Tutorial
- Ghost context
- Imperative features
- Working with existing code
- Proving theorems
- Stainless library
- and more...

=> stainless.epfl.ch

Acknowledgments

Stainless is the latest iteration of our verification system for Scala, which was built and improved over time by many EPFL PhD students: Nicolas Voirol, Jad Hamza, Régis Blanc, Eva Darulova, Etienne Kneuss, Ravichandhran Kandhadai Madhavan, Mikaël Mayer, Emmanouil Koukoutos, Ruzica Piskac, Philippe Suter, as well as Marco Antognini, Ivan Kuraj, Lars Hupel, Samuel Grütter, and myself.

Many thanks as well to our friends at TripleQuote for their help with the compiler and sbt plugins.

References I