From definitional interpreter to symbolic executor

Mensing, Adrian D.; Van Antwerpen, Hendrik; Poulsen, Casper Bach; Visser, Eelco

DOI
10.1145/3358502.3361269

Publication date
2019

Document Version
Final published version

Published in
META 2019 - Proceedings of the 4th ACM SIGPLAN International Workshop on Meta-Programming Techniques and Reflection, co-located with SPLASH 2019

Citation (APA)

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.
From Definitional Interpreter to Symbolic Executor

Adrian D. Mensing  
Delft University of Technology  
Netherlands  
a.d.mensing-1@student.tudelft.nl

Casper Bach Poulsen  
Delft University of Technology  
Netherlands  
c.b.poulsen@tudelft.nl

Hendrik van Antwerpen  
Delft University of Technology  
Netherlands  
h.vanantwerpen@tudelft.nl

Eelco Visser  
Delft University of Technology  
Netherlands  
e.visser@tudelft.nl

Abstract
Symbolic execution is a technique for automatic software validation and verification. New symbolic executors regularly appear for both existing and new languages and such symbolic executors are generally manually (re)implemented each time we want to support a new language. We propose to automatically generate symbolic executors from language definitions, and present a technique for mechanically (but as yet, manually) deriving a symbolic executor from a definitional interpreter. The idea is that language designers define their language as a monadic definitional interpreter, where the monad of the interpreter defines the meaning of branch points. Developing a symbolic executor for a language is a matter of changing the monadic interpretation of branch points. In this paper, we illustrate the technique on a language with recursive functions and pattern matching, and use the derived symbolic executor to automatically generate test cases for definitional interpreters implemented in our defined language.

CCS Concepts  
• Theory of computation → Program schemes;  
• Software and its engineering → Formal methods; Automatic programming.

Keywords  
Symbolic Execution, Monads, Haskell, Definitional Interpreter

1 Introduction
Symbolic execution [27] is a meta-programming technique that is at the core of techniques for boosting developer productivity, such as automated testing [3, 9, 17, 19, 38] and program synthesis [14, 20, 35]. A symbolic executor allows exploration of possible execution paths by running a program with symbolic variables in place of concrete values. By strategically instantiating symbolic variables, a symbolic executor can be used to systematically analyze which parts of a program are reachable, with which inputs.

Constructing symbolic executors is non-trivial, and enabling support for symbolic execution for general-purpose languages, such as C [4, 19, 38], C++ [31], Java [1, 37], PHP [2], or Rust [33], is the topic of entire publications at major software engineering conferences. We propose that techniques for symbolic execution are reusable between languages, and investigate the foundations of how to define and implement symbolic executors, by deriving them from definitional interpreters. Our long-term goal is to integrate these techniques into language workbenches, such as Spoofax [25], Rascal [29], or Racket [15], to enable the automatic generation of programmer productivity boosting tools, such as automated testing frameworks and program synthesizers.

In this paper we explore how to mechanically derive symbolic executors that explore possible execution paths through programs by instantiating and specializing symbolic variables, following a breadth-first search strategy. Our exploration revolves around a dynamically-typed language with recursive functions and pattern matching. Using Haskell as our meta-language, and working with its integrated support for generic and monadic programming, we implement a definitional interpreter for this language. This definitional interpreter is parameterized with an interface which we instantiate in two different ways to obtain first a concrete interpreter, and then a symbolic executor. The “derivation” thus amounts to instantiating the interface operations in a manner that yields a symbolic executor.

The symbolic executor we derive allows us to explore the solution space for constraints such as the following constraint that a list `xs` must be a palindrome:

\[ xs \equiv reverse \ xs \]
Symbolic execution explores all execution paths through the `reverse` function that satisfy the constraint, and instantiates `xs` accordingly, thereby generating palindromes. This paper is a literate Haskell file, and we invite interested readers to download the Haskell version of the paper to experiment with, and extend, the framework we present.  

### Related Previous Lines of Work

The techniques that we develop in this paper are closely related to the techniques used for relational programming, pioneered by Friedman and Byrd in miniKanren [5, 8, 16, 22], a language for relational programming and constraint logic programming, which has been implemented in a wide range of different languages; notably Scheme [7, 16], but also, e.g., OCaml [30]. The miniKanren language and many of its implementations have been developed and researched for more than a decade, with new developments and improvements appearing each year, such as new and better heuristics for guiding the exploration of execution paths [34]. The motivation for this paper is to bring similar benefits as found in miniKanren to programming languages at large, by automatically deriving symbolic executors from definitional interpreters.

Rosette [40, 41] is a solver-aided language that extends Racket [15] to provide framework for implementing solver-aided domain-specific languages, by means of a symbolic virtual machine and symbolic compiler. This VM brings the benefits of symbolic execution and model checking to languages implemented in Rosette via general-purpose symbolic abstractions that support sophisticated symbolic reasoning, beyond the relatively simple constraints found in (most variants of) miniKanren. A main goal of Rosette is to implement solver-aided languages, but the symbolic abstractions and techniques that Rosette implements could also be used to address the problem that is the motivation for this paper, namely the problem of automatically deriving symbolic executors from “traditional” definitional interpreters.

There has been much work on symbolic execution in the literature on software engineering; e.g., [1, 2, 4, 19, 31, 33, 37, 38]. Many of these frameworks are so-called concolic frameworks that work by instrumenting a concrete language runtime to track symbolic path constraints. After each concrete execution, these path constraints are collected and solved in order to cover a different path through the program in a subsequent run of the program. Concolic testing is typically implemented by generating test inputs randomly, rather than systematically solving path constraints. In this paper, we explore a symbolic execution strategy which interleavingly explores multiple execution paths concurrently, rather than a concolic testing approach which would require a relatively sophisticated constraint solver in order to explore execution paths in an equally systematic manner.

### Contributions

- Techniques (in § 3) for deriving symbolic executors from definitional interpreters, by using free monads to compile programs into command trees, and interpreting these using a small-step execution strategy.
- A symbolic executor (in § 4) for a language with algebraic datatypes that illustrates these techniques.
- A simple example application (in § 6): automated test generation for definitional interpreters.

The rest of this paper is structured as follows. In § 2 we introduce a definitional interpreter for a language with recursion and pattern matching. In § 3 we present a definitional interpretation of the effects, by means of a free monad, using a small-step semantics execution strategy. In § 4 we generalize the definitional interpretation of effects from § 3, to obtain a symbolic executor, whose correctness we discuss in § 5. Finally, in § 6 we discuss a case study application of the symbolic executor: generating tests for definitional interpreters, and § 7 concludes.

## 2 Definitional Interpreter for a Language With Pattern Matching

Definitional interpreters define the meaning of a (new) object language by implementing an interpreter for it in an existing, well-understood, language. We use Haskell to implement a definitional interpreter for a functional language with pattern matching.

### 2.1 Syntax

The abstract syntax of the language we consider is summarized in Fig. 1. The expression constructors for `Var`, `Lam`, and `App` are standard expressions for variables, unary functions, and function application. An expression constructor expression `Con f [e₁, ..., eₙ]` represents an n-ary term whose head symbol is `f`, and whose sub-term values are the results of evaluating each expression `e₁` ... `eₙ`. Case `e [(p₁, e₁), ..., (pₙ, eₙ)]` is a pattern match expression which first evaluates `e` to a value and then attempts to match the resulting value against the patterns `p₁` ... `pₙ`, where patterns are given by the type `Patt`. `Letrec` expressions are restricted to bind value expressions, given by the type `ValExp`.

### 2.2 Prelude to a Definitional Interpreter: Effects and Values

The definitional interpreter for the language we consider in this paper is given in Fig. 2. The interpreter depends on the `EffVal` type class which in turn depends on a number of type classes that constrain the polymorphic notion of effects (defined by a monad `m`) and values (defined by a value type `val`) of the interpreter. The `EffVal` type class is thus a polymorphic embedding [23] of a language that allows us to define a family of interpreters for the same language.
There are two reasons why we use a specialized version. The MonadEnv is a specialized version of the classical reader Monad m class operation for branching:

\[
\text{branch} :: \text{cval} \rightarrow \text{fork} m \text{ rval} \rightarrow m \text{ rval}
\]

This type class is parameterized by: (1) a value type cval that branch selection is conditional upon; (2) a value type rval for the return type of computations in branches; and (3) a fork type, an abstract notion of branches comprising computations described by m and val. To illustrate, consider the following instance of MonadBranch which represents a classical if-then-else expression:

\[
\text{newtype IfThenElse } m a = \text{ITE} (m a, m a)
\]

\[
\text{instance Monad } m \Rightarrow
\text{MonadBranch } \text{Bool rval IfThenElse } m \text{ where}
\]

\[
\begin{align*}
\text{branch True } (\text{ITE } (t, \_)) &= t \\
\text{branch False } (\text{ITE } (\_, f)) &= f
\end{align*}
\]

For our interpreter, which branches on values and returns values of the same type, we rely on the following more restrictive version of MonadBranch:\(^2\)

\[
\text{class Monad } m \Rightarrow \text{MonadMatch } \text{val fork m where}
\]

\[
\text{match :: val } \rightarrow \text{fork m val } \rightarrow m \text{ val}
\]

And our interpreter uses the following notion of fork over a list of pairs consisting of a pattern and a (monadic) computation where each computation has the return type a:

\[
\text{newtype Cases } m a = \text{Cases} [(\text{Patt, m a})]
\]

Values The following type classes define the constructors for term values con, and function closures clos, as well as operation app for applying a function to an argument and operation eq for checking equality between two term values.

\[
\begin{align*}
\text{class TermVal } \text{val where} \\
\text{con} \_ :: \text{String } \rightarrow \text{[val]} \rightarrow \text{val}
\end{align*}
\]

\[
\text{class FunVal } \text{val where}
\]

\[
\text{clos} \_ :: \text{String } \rightarrow \text{Expr } \rightarrow \text{Env val } \rightarrow \text{val}
\]

\[
\text{class FunApp } \text{val where}
\]

\[
\text{app} :: \text{val } \rightarrow \text{val } \rightarrow m \text{ val}
\]

\[
\text{class TermEq } \text{val where}
\]

\[
\text{eq } :: \text{val } \rightarrow \text{val } \rightarrow m \text{ val}
\]

2.3 A Definitional Interpreter for a Language with Pattern Matching

The interpreter in Fig. 2 relies on the effect and value type classes summarized in the previous section. Additionally, the interpreter makes use of a few auxiliary functions whose definitions we elide: mmap maps a monadic function over a list; mapSnd maps a function over the second element of a tuple; and resolve resolves a name in an association list, or fails. The implementation of Letrec uses Haskell’s support for

\(^2\)The main motivation for using the more specific notion of MonadMatch here is to help Haskell’s type class resolution engine (using GHC v8.6.4). Morally, MonadBranch should do.
The type class instances for this notion of value and monad are defined in the obvious way. MonadMatch attempts to pattern match a value against a list of cases by attempting each from left-to-right until a match succeeds:

**Figure 2.** A definitional interpreter for a language with pattern matching

Using these type class instances, our definitional interpreter can be run as follows:

```
runSteps :: Expr → Env ConcreteValue → Either String a
runSteps e nv = runExcept (runReaderT (interp e) nv)
```

### 3 Towards a Symbolic Executor

The definitional interpreter presented in § 2.3 uses standard monads and monad transformers to implement the definitional interpreter given in Fig. 2. But it gives meta-programmers little control over how interpretation proceeds. Our goal is to implement a symbolic executor for running a program in a way that interleavingly explores all possible execution paths. To this end, we want a symbolic executor that can operate on a pool of concurrently running threads where each thread represents a possible path through the program. We will approach this challenge by adopting a small-step execution strategy for each thread. In this section we provide alternative type class instances that give meta-programmers more fine-grained control over how interpretation proceeds. Concretely, we adopt a small-step execution strategy for effect interpretation, by using free monads.

Following Kiselyov and Ishii [28] and Swierstra and Bannen [39], the following data type defines a family of free monads:

```
data Free c a = Stop a
   | ∀ b. Step (c b) (b → Free c a)
```

(lazy) recursive definitions to define a recursive environment \( \text{Env} \) that \( \text{ValExprs} \) are evaluated under.

To run our definitional interpreter we must provide concrete instances of the abstract type classes from § 2.2. We use the following notion of value and monad:

```haskell
data ConcreteValue = ConV String [ConcreteValue]
   | ClosV String Expr (Env ConcreteValue)
type ConcreteMonad = ReaderT (Env ConcreteValue) (Except String)
```

Here \( \text{ReaderT} \) is a monad transformer [32] for the classical reader monad, and \( \text{Except} \) is the exception monad. So \( \text{ConcreteMonad} \) is isomorphic to:

```
type ConcreteMonad' a = Env ConcreteValue → Either String a
```

The type class instances for this notion of value and monad are defined in the obvious way. MonadMatch attempts to pattern match a value against a list of cases by attempting each from left-to-right until a match succeeds:

```
instance MonadMatch ConcreteValue Cases
   ConcreteMonad where
      match v (Cases ((p, m) : bs)) = case vmatch v p of
         Just nv → local (λnv₀ → nv + nv₀) m
         Nothing → match v (Cases bs)
      match _ (Cases []) = throwError "Match failure"

vmatch :: (ConcreteValue, Patt) → Maybe (Env ConcreteValue)
```

```
interp :: EffVal m val ⇒ Expr → m val
interp (Con c es) = do
   vs ← mmap interp es
   return (con, c vs)
interp (Case e bs) =
   let vbs = map (mapSnd interp) bs in do
      v ← interp e
      match v (Cases vbs)
interp (Var x) = do
   nv ← ask
   return (resolve x nv)
interp (Lam x e) = do
   nv ← ask
   return (clos x e nv)
interp (App e₁ e₂) = do
   f ← interp e₁
   a ← interp e₂
   app f a
```

```
runSteps :: Expr → Env ConcreteValue → Either String a
runSteps e nv = runExcept (runReaderT (interp e) nv)
```

```
interp (Let xes e) = do
   nv ← mmap interpSnd xes
   local (λnv₀ → nv + nv₀) (interp e)
where interpSnd (x, e) = do
      v ← interp e
      return (x, v)
interp (Letrec xes e) = do
   nv ← ask
   let nv_b = map (mapSnd (interpVal nv)) xes
      nv_ = nv_b + nv in
   local (λ_ → nv_) (interp e)
interp (EEq e₁ e₂) = do
   v₁ ← interp e₁
   v₂ ← interp e₂
   eq v₁ v₂
interpVal :: (TermVal val, FunVal val) ⇒ Env val → ValExpr → val
interpVal nv (VLam x e) = clos x e nv
interpVal nv (VCon x es) =
   con x (map (interpVal nv) es)
```

Following Hancock and Setzer [21], we call values of this data type command trees: each Step represents an application of a command \( c b \), corresponding to a monadic operation, which yields a value of type \( b \) when interpreted. This value is passed to the continuation \( (b \to \text{Free} \ c \ a) \) of Step. The Free data type is a monad:

```haskell
instance Monad (Free c) where
  return = Stop
  Step a ≜ k = k a
  Step c f ≜ k = Step c (\x → f x ≜ k)
```

By defining a suitable notion of command, we can define a free monad instance which satisfies the type class constraints for our definitional interpreter from Fig. 2. The following data type defines such a notion of command:

```haskell
data Cmd val :: → → = + where
  Match :: val → Cases (Free (Cmd val)) val →
  Env val → Free (Cmd val) val →
  Ask :: Cmd val (Env val)
  Eq :: val → Expr val →
  Fail :: String → Cmd val
```

By instantiating each of the type classes we obtain a compiler from expressions into command trees:

```haskell
comp :: (TermVal val, FunVal val) Expr → Free (Cmd val) val
```

The command trees that \( \text{comp} \) yields are the sequences (or rather trees) of effectful operations that define the meaning of object language expressions. But the meaning of command trees is left open to interpretation. We define the meaning of command trees by means of a small-step transition function and a driver loop for the transition function. This small-step transition function operates on a single command tree (whose type we abbreviate \( \text{Thread}, \) since the command tree represents a thread of interpretation), and yields a single command tree as result (or raises an exception). For brevity, we show just a few cases of the \( \text{step} \) function:

```haskell
type Thread = Free (Cmd ConcreteValue)
step :: Thread ConcreteValue →
  ConcreteMonad (Thread ConcreteValue)
step (Stop x) = return (Stop x)
step (Step (Match _ (Cases []))) =
  throwError "pattern match failure"
```

The driver loop for the step function is straightforwardly defined to continue interpretation until the current thread of interpretation terminates successfully (or fails):

```haskell
drive :: Thread ConcreteValue →
  ConcreteMonad ConcreteValue
drive (Stop x) = return x
drive c = do r ← step c; drive r
```

Thus an alternative definitional interpreter for the language in Fig. 2 is given by the following function:

```haskell
runSteps :: Expr → Env ConcreteValue →
  Either String ConcreteValue
runSteps e nv = runExcept (runReaderT (drive (comp e)) nv)
```

## 4 From Definitional Interpreter to Symbolic Executor

In this section we derive a symbolic executor from the definitional interpreter in § 3, by: (1) generalizing the notion of value from previous sections to also incorporate symbolic variables; and (2) generalizing the semantics (monad and small-step transition function) to support instantiation of symbolic variables and fork new threads of interpretation.

### Symbolic Values

The updated notion of value is an extension of the notion of ConcreteValue data type from § 2.3 with a symbolic variable constructor, SymV:

```haskell
data SymbolicValue = ConV' String [SymbolicValue]
  | ClosV' String Expr
  | SymV String
```

### Monad

The monad for evaluating a step of symbolic execution has an environment and may raise an exception, just like the monad in § 3 for evaluating a step of concrete execution. Additionally, the monad has a stateful \( \text{Int} \) field for keeping track of a fresh supply of symbolic variable names:

```haskell
type SymbolicMonad =
  ReaderT (Env SymbolicValue)
  (StateT Int (Except String))
```

Since symbolic execution should explore all possible execution paths through a program, we generalize the small-step transition relation from § 3 by letting the transition relation take a single thread of interpretation as input, but return a set of possible continuation threads. Each step may result in unifying a symbolic variable in order to explore a possible execution path. Our generalized notion of monad is thus given by the following types:

```haskell
type Unifier = [(String, SymbolicValue)]
type UnifierN = [(SymbolicValue, SymbolicValue)]
```
type SymbolicSetMonad = 
  StateT (Unifier, UnifierN) (ListT SymbolicMonad)

Here, Unifier witnesses how symbol variables must be in-
stantiated in order to complete a single transition step, rep-
resenting a particular execution path of the program being
symbolically executed. UnifierN represents a set of negative
unification constraints. We motivate the use and need for
these shortly. The ListT monad transformer generalizes the
return type of a monadic computation m a to return a list of
as; i.e., m [ a]. Note that, although we call ListT a monad
transformer, it is well-known that ListT in Haskell is not
guaranteed to yield a monad that satisfies the monad laws.

For the purpose of this paper, it is not essential whether the
particular definition of SymbolicSetMonad above actually sat-
sifies the monad laws.

**Small-Step Transition Function** Our symbolic executor
is derived from the concrete semantics of effects in § 3 by
altering how we Match and Eq₂ effects are interpreted. Thus
case all cases of the transition function stepₙ (below) are identical
to the small-step transition function from § 3, except for the
cases for the Match and Eq₂. Furthermore, the definitional
interpreter from Fig. 2 is unchanged. We summarize the in-
teresting cases for the stepₙ function, which takes a symbolic
interpretation thread, Threadₙ, as input, and returns a set of
threads (note the use of SymbolicSetMonad):

```
<table>
<thead>
<tr>
<th>Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match</td>
<td>SymbolicSetMonad (Threadₙ, SymbolicValue)</td>
</tr>
<tr>
<td>Eq₂</td>
<td>StateT (Unifier, UnifierN) (ListT SymbolicMonad)</td>
</tr>
<tr>
<td>mzero</td>
<td>do (nv, u) ← vmatch₁ (v, p) (applySubst u (Step (Local (λnv₀ → nv + nv₀) m) k)) 'mplus' stepₙ (Step (Match v (Cases bs) k)) 'catchError' (λ_ → stepₙ (Step (Match v (Cases bs) k)) k)</td>
</tr>
<tr>
<td>vmatch₁</td>
<td>case unify v₁, v₂ of Just [] → return (k (ConV' &quot;true&quot; [])) Just u → do (applySubst u (k (ConV' &quot;true&quot; []))) 'mplus' (constrainUnify₁ u (k (ConV' &quot;false&quot; []))) Nothing → return (k (ConV' &quot;false&quot; []))</td>
</tr>
</tbody>
</table>
```

As in § 3, there are two cases for Match: one for the case
where we have exhausted the list of patterns to match a value
against, and one for the case where there are more cases
to consider. In case we have exhausted the list of patterns
to match a value against, we now use mzero to return an
empty set of result threads. Otherwise, we match a value
against a pattern, using the side-effectful vmatch₁ function,
elided for brevity). If the value contains symbolic variables,
that contain symbolic variables gives rise to a breadth-first search over possible instantiations of symbolic variables, to synthesize concrete terms. We provide programmers with control over which parts of a program (s)he wishes to synthesize by defining a small constraint language on top of the definitional interpreter from Fig. 2.

The syntax for this constraint language is summarized in Fig. 3. `CTake n c x` is a “top-level” constraint for picking `n` solutions to a constraint `c x` that contains existentially quantified symbolic variables. `CEx x c` introduces an existentially quantified symbolic variable, by populating the environment of a symbolic interpreter with a symbolic variable value binding `SymV x y` for `x`, where `y` is a fresh symbolic variable name. `CEq e1 e2` is a constraint that `e1` and `e2` evaluate to the same value, and `CNEq e1 e2` is a constraint that `e1` and `e2` evaluate to different values.

Our approach to constraint solving is given by the `solve` function in Fig. 4 which, in turn, calls the `searchs` function whose type signature is shown in the figure, but whose implementation we omit for brevity. `searchs e t s c eq n` implements a naive constraint solving strategy which uses a symbolic executor to search for `n` different instantiations of symbolic variables that make the result of symbolic execution of the input expression `e` equal to the result of symbolic execution of a configuration in `ts`, modulo a custom notion of `SymbolicEquality`.

**Example: Synthesizing Append Expressions** To illustrate what we can do with our derived symbolic executor and small constraint language, let us consider list concatenation as an example, inspired by the relational programming techniques and examples given by Byrd et al. [6]. The `append0` program below grabs a single solution to the constraint which equates "q" and the result of concatenating (append) a list consisting of three atoms (a, b, c) with a list of two atoms (d, e):

```
data Constraint = CTake Int ExConstraint
  data ExConstraint = CEx String ExConstraint
                      | CEq Expr Expr
                      | CNEq Expr Expr

Figure 3. Syntax for a tiny constraint language
```

```
solve :: Constraint → SymbolicMonad [Env SymbolicValue]
solve (CTake n c x) = solves c x n
solvev s :: ExConstraint → Int →
    SymbolicMonad [Env SymbolicValue]
solvev (CEx x c) n = do
  n x ← fresh'
  Reader.local (λnv n v → (x, SymV n x) : nv) (solvev c x n)
  solvev (CEq e1 e2) n = do
    n v ← ask
    searchv e1 (((interp e2, nv, []),) unify n
    solvev (CNEq e1 e2) n = do
      nv ← ask
      searchv e1 (((interp e2, nv, []),)
      (λv1 v2 → case unify v1 v2 of
        Just _ → Nothing
        Nothing → Just [ ])
      n

type SymbolicEq =
    SymbolicValue → SymbolicValue → Maybe Unifier

searchv s :: Expr →
    [Config, (Thread, SymbolicValue)] →
    SymbolicEq →
    Int →
    SymbolicMonad [Env SymbolicValue]
```

```
Figure 4. A constraint solver for symbolic execution constraints
```

sugar for ‘App’. Solving the `append0` constraint yields the instantiation of `q` to the list containing all input atoms in sequence.

We can also use symbolic execution to synthesize inputs to functions:

```
append01 :: Constraint
append01 =
  grab 1 (exists "q")
  ((append @ (var "q")
    @@ (atom "d" 'cons' (atom "e" 'cons' nil))
    'CEq' (atom "a" 'cons' (atom "b" 'cons' (atom "c" 'cons' (atom "d" 'cons' (atom "e" 'cons' nil)))))
  )
```

Solving the `append01` constraint yields the instantiation of `q` to the list containing the atoms `a, b, c`.

We can even use symbolic execution to synthesize multiple inputs:

```
append02 :: Constraint
append02 =
  grab 6 (exists "x" (exists "y")
  ((append @ (var "x") @ (var "y")))
```

```
append0 :: Constraint
append0 =
  grab 1 (exists "q")
  ((append @ (atom "a" 'cons' (atom "b" 'cons' (atom "c" 'cons' nil)))
```

Here, `append` is a recursive function defined in the language we are symbolically executing (Fig. 1), and `@` is syntactic
We conjecture that, for any pair of concrete environment and symbolic environment 
we have shown how to derive a symbolic executor from a concrete semantics. The derivation was driven by an intuitive understanding of what needs to happen in a symbolic executor (instanti 1ng and refining symbolic variables, forking new threads of interpretation) in order to ensure that the symbolic executor explores all possible execution paths, but only possible execution paths (i.e., no execution paths that do not correspond to an actual execution path). In this section we conjecture a correctness proposition for our symbolic evaluator, and discuss directions for making this correctness proposition more formal.

Let \( \text{runSteps} \) be a function that uses the \( \text{drive} \) function to drive an expression to a final value and pool of alternative execution paths that may yet yield a final result:

\[
\text{runSteps} :: \text{Expr} \rightarrow \text{Env} \rightarrow \text{SymbolicValue} \rightarrow \\
\quad \text{Either String (SymbolicValue, [ Config, (Thread, SymbolicValue) ])}
\]

We conjecture that, for any pair of concrete environment \( n_v \) and symbolic environment \( n_v' \) that are equal up-to-unification:

1. Any concrete execution path, given by calling \( \text{runSteps} \) from §3 under \( n_v \) with any \( e :: \text{Expr} \) either yields a value that is equal up-to-unification to the \( \text{SymbolicValue} \) that \( \text{runSteps} \) returns; or yields a value that one of the configurations in \( \text{runSteps} \), will eventually yield, if we were to iterate that configuration.
2. Any symbolic execution path, given by calling \( \text{runSteps} \), under \( n_v' \) with any \( e :: \text{Expr} \) yields a symbolic value and set of configurations that exhaustively describe any concrete execution path resulting from evaluating \( e \) under any \( n_v' \) that is equal up-to-unification to \( n_v' \).

We believe that abstract interpretation [13] is a suitable framework for formalizing the correspondence between concrete and symbolic execution.\(^3\) The methodology due to Keidel et al. [26] for defining static analyzers with compositional soundness proofs is attractive to consider for this purpose. But it is an open question how the small-step interpretation strategy, suitable for forking threads of interpretation and doing breadth-first search over how to instantiate symbolic variables in ways that correspond to execution paths through a program, subject to constraints. We introduced a small constraint language on top of our symbolic executor, and used this language to derive test cases for definitional interpreters for the simply-typed lambda calculus. In future work, we will investigate how to port their verification technique to the development in this paper.

\(^3\)Indeed, it seems Cousot [12] has considered how to formalize symbolic execution within the framework of abstract interpretation. This formalization is only available in French [11].
References


