Deep Strictness: Milestone 1

Kenny, Hengchu

November 7, 2017

We aim to extend QuickCheck with the ability to probabilistically verify the laziness/strictness behavior of Haskell functions. That is, we will allow users to write a specification of the strictness behavior of a particular function, and by fuzzing inputs to the function, determine if the function is *exactly* as strict as the user has specified.

Before describing in detail how our proposed tool will work, we give several definitions regarding laziness in Haskell:

A lazy function takes an *input* to an *output*. For now, we consider only inputs and outputs restricted to single algebraic datatypes which do not contain functions (that is, all functions we can speak about are unary first-order functions). We plan to extend this to multi-argument and higher-order functions in later stages of this project.

When a lazy function is applied to an input, it is done so in a *context* which makes use of some part of its output—that is, the context may not use the entire output data structure to continue its own computation. We call the portion of the input which is used by the context the *demand* on the output. The semantics of lazy evaluation dictate that any portion of the input which is not required to compute the demanded portion of the output are not evaluated in the first place—that is, evaluation only occurs as much as is necessary to satisfy the demand of the calling context.

For example, let us consider a function `f :: Int -> Int -> Int` where `f x n = fst (x, fib n)`. Although computing the second component of the pair in `f 1 100000000` would be very expensive, this computation never occurs because the demand placed upon the pair (extracting the first component) only requires the first component to be evaluated. We say that `f` is *strict* in its first parameter (`x`) and *lazy* in its second parameter (`n`).

We can capture this notion formally as a function from a given demand of the output to a demand of the input. We call this a *demand specification*. Here, we can concretely represent a demand as a *subshape* of the input/output—that is, a data structure corresponding to one of these data types, but which can be truncated at any arbitrary position in the structure of the data type. We call this derived data type the *demand type* corresponding to a data type.

For example, the corresponding demand type for the type `(Int, Int)` would be:
`Demand (Demand Int, Demand Int)`
where

```
data Demand a = ~   -- ^ Not demanding
              | ! a -- ^ Demanding the constructor at this level
              | *   -- ^ Demanding a primitive or nullary constructor
```

All the values of these types are: `~`, `(~, ~)`, `! (*, ~)`, `! (~, *)`, and `! (*, *)`. These represent all of the possible demands which a context could place on the type `(Int, Int)`.

Suppose we have a function `g :: (Int, Int) -> Int`. The corresponding demand specification for g would be a function `gSpec :: Demand Int -> Demand (Demand Int, Demand Int)`.

Concretely, consider the function `fst` (for integers):

```
fst :: (Int, Int) -> Int
fst (a, b) = a
```

An accurate demand specification for `fst` is:

```
fstSpec :: Demand Int -> Demand (Demand Int, Demand Int)
fstSpec ~ = ~
fstSpec * = ! (*, ~)
```

This states that if we demand nothing from the result of `fst`, we do not need to evaluate its argument at all. (This is true for *every* function in a lazy language!) However, if we demand the resultant integer from `fst`, we must evaluate the first integer in the input pair, but we do not need to evaluate the second element of the pair.

For functions like `fst`, the demand on input is a *static demand*: that is, for each demand on the output, any input to the function will be evaluated to the same degree.

This is not true in general, and not merely in pathological examples. Many (perhaps most!) useful functions have dynamic demand behavior—that is, their demand specification depends on the values of the input. We say that such functions have *dependent demand*: that is, the demand specification of these functions must consider the input values of the function as well.

```
take :: (Int, [Int]) -> [Int]
take (n, xs) =
  case (n, xs) of
    (0, _)     -> []
    (n',x:xs') -> x:(take ((n'-1), xs'))
    (n', [])   -> []
```

Just given some demand on the output list, we can't guess the demand on the second element of the input pair, although we do know that the first element of the pair will always be evaluated.

Suppose we have demand the first 2 elements of some result of take, there is no one input demand that corresponds to this output demand. However, if we know what the first argument to `take` is, we can determine the degree to which the input list must be evaluated. Note that the demand on the output still is another factor in determining the demand on the input, since if we demand nothing on the output, then nothing on the input will be demanded.

The demand specification of `take` could be

```
takeSpec :: (Int, [Int]) -> Demand [Demand Int] -> Demand (Demand Int, Demand [Demand Int])
takeSpec _        ~    =  ~
takeSpec (0, _)  ![]   =  !(*, ~)
takeSpec (n, xs) !ds   =
  case (ds, xs) of
    ([],     _)    -> !(*, ![])
    (d:ds', x:xs') ->
      let !(_, !ds'') = takeSpec (n-1, xs') !ds' in
      !(*, !(d:ds''))
```

Determining statically whether a function meets its demand spec is undecidable due to the Halting Problem. So, instead of statically approximating these behavior, we choose to apply runtime instrumentation with randomized testing, this gives a high level of confidence.

We choose to implement this as an extension to QuickCheck (CITATION). We will use generic programming to derive the demand types of functions under consideration. We will use existing QuickCheck generator infrastructure to fuzz inputs to the function, and demands on the output of the function. Because only certain shapes of demand are realizable on a given output, we specialize the demand generators to produce only sensible demands on each invocation of the function. We then run the function on the random input to obtain un-evaluated output, and place a random demand on this output while instrumenting the function to determine the resultant demand on the input. We can then use the demand specification to check whether the demand specification exactly matches what the actual demand behavior of the function was in this trial.

Because we integrate with the existing functionality of QuickCheck, we can employ its *shrinking* abilities to produce minimal counterexamples of input/demand pairs which fail to satisfy a given demand specification, if this specification is faulty.

Note that there are two ways in which a specification may be faulty: it may fail to produce an input demand which exactly matches the real observed input demand, or it may fail to cover all possible realizable combinations of input and demand.

To avoid unnecessary metaprogramming, we choose not to calculate an instrumented version of the function under consideration. We do not need to resort to such strategies because we can instead instrument the input data structure to report to us how it is evaluated by the function. As such, we may treat our functions as a black box.

In order to instrument a lazy data structure, we must use so-called "unsafe" features of Haskell—in particular, the function `unsafePerformIO` which allows us to attach a callback to a particular lazy value so that the callback is run when that value is evaluated. We may traverse the generated input data structure to add such a callback to every node in that structure. By tracking which of these callbacks are invoked when we demand a particular part of the output of some function applied to the instrumented structure, we produce an exact representation of the input demand of this function given a particular output demand and input value.

Once we have obtained a pair of generated output demand and observed input demand, it's trivial to run the demand specification on the output demand and check whether it exactly matches the observed demand. If it does not, we may repeat this process by shrinking inputs to the function to compute a minimal example exhibiting the detected violation of the demand specification.

We need not only to consider how to *check* such specifications, but also how to specify them in the first place! To that end, we will use Haskell's generic programming features to provide a syntax for users to succinctly write these demand specifications without worrying about the details of our implementation. Ideally, this syntax would look very similar to the syntax we use above, but we may need to make some concessions due to the limitations of the implementation strategy we choose for this interface.

Moving forward, we want to allow users to check demand specifications of multi-argument functions, higher-order functions, and functions on data structures which themselves contain functions.