Refinement Reflection
(or, how to turn your favorite language into a proof assistant using SMT)

Niki Vazou  Ranjit Jhala
University of California, San Diego

Abstract
Refinement Reflection turns your favorite programming language into a proof assistant by reflecting the code implementing a user-defined function into the function’s (output) refinement type. As a consequence, at uses of the function, the function definition is unfolded into the refinement logic in a precise, predictable and most importantly, programmer controllable way. In the logic, we encode functions and lambdas using uninterpreted symbols preserving SMT-based decidability verification. In the language, we provide a library of combinators that lets programmers compose proofs from basic refinements and function definitions. We have implemented our approach in the Liquid Haskell system, thereby converting Haskell into an interactive proof assistant, that we used to verify a variety of properties ranging from arithmetic properties of higher order, recursive functions to the Monoid, Applicative, Functor and Monad type class laws for a variety of instances.

1. Introduction
Wouldn’t it be great to write proofs of programs in your favorite language, by writing programs in your favorite language, allowing you to avail of verification, while reusing the libraries, compilers and run-times for your favorite language?

Refinement types [9, 26] offer a form of programming with proofs that can be retrofitted into several languages like ML [5, 24, 37], C [8, 25], Haskell [32], TypeScript [34] and Racket [13]. The retrofitting relies upon restricting refinements to so-called “shallow” specifications that correspond to abstract interpretations of the behavior of functions. For example, refinements make it easy to specify that the list returned by the append function has size equal to the sum of those of its inputs. These shallow specifications fall within decidable logical fragments, and hence, can be automatically verified using SMT based refinement typing.

Refinements are a pale shadow of what is possible with dependently typed languages like Coq, Agda and Idris which permit “deep” specification and verification. These languages come equipped with mechanisms that represent and manipulate the exact descriptions of user-defined functions. For example, we can represent the specification that the append function is associative, and we can manipulate (unfold) its definition to write a small program that constructs a proof of the specification. Dafny [15], F* [30] and Halo [35] take a step towards SMT-based deep verification, by encoding user-defined functions as universally quantified logical formulas or “axioms”. This axiomatic approach offers significant automation but is a devil’s bargain as by relying heavily upon brittle heuristics for “triggering” axiom instantiation, it gives away decidable, and hence, predictable verification [16].

Refinement Reflection In this paper, we present a new approach to retrofitting deep verification into existing languages. Our approach reconciles the automation of SMT-based refinement typing with decidable and predictable verification, and enables users to reify pencil-and-paper proofs simply as programs in the source language. Our key insight is dead simple: the code implementing a user-defined function can be reflected into the function’s (output) refinement type, thus converting the function’s (refinement) type signature into a deep specification of the functions behavior. This simple idea has a profound consequence: at uses of the function, the standard rule for (dependent) function application yields a precise, predictable and most importantly, programmer controllable means of instantiating the deep specification that is not tethered to brittle SMT heuristics. Reflection captures deep specifications as refinements, but poses challenges for the logic and language.

Logic: Algorithmic Verification Our first challenge: how can we encode terms from an expressive higher order language in a decidable refinement logic in order to retain decidability, and hence, predictable, verification? We address this problem by using ideas for defunctionalization from the theorem proving literature which encode functions and lambdas using uninterpreted symbols. This encoding lets us use (SMT-based) congruence closure to reason about equality (§ 4). Of course, congruence is not enough; in general, e.g. to prove two functions extensionally equal, we require facilities for manipulating function definitions.

Language: Proof Composition Thus, as we wish to retrofit proofs into existing languages, our second challenge: how can we design a library of combinators that lets programmers compose proofs from basic refinements and function definitions? We develop such a library, wherein proofs are represented simply as unit-values refined by the proposition that they are proofs of. Refinement reflection lets us unfold definitions simply by applying the function to the relevant inputs, and finally, we show how to build up sophisticated proofs using a small library of combinators that permit reasoning in an algebraic or equational style.

Implementation & Evaluation We have implemented our approach in the Liquid Haskell system, thereby retrofitting deep verification into Haskell, converting it into an interactive proof assistant. Liquid Haskell’s refinement types crucially allow us to soundly account for the dreaded bottom by checking that (refined) functions produce (non-bottom) values [32]. We evaluate our approach by using Liquid Haskell to verify a variety of properties including arithmetic properties of higher order, recursive functions, textbook theorems about functions on inductively defined datatypes, and the Monoid, Applicative, Functor and Monad type class laws for a variety of instances. We demonstrate that our proofs look very much like transcriptions of their pencil-and-paper analogues. Yet, the proofs are plain Haskell functions, where case-splitting and induction are performed by plain pattern-matching and recursion.

To summarize, this paper describes a means of retrofitting deep specification and verification into your favorite language, by making the following contributions:
• We start with an informal description of refinement reflection, and how it can be used to prove theorems about functions, by writing functions (§ 2).
• We formalize refinement reflection using a core calculus, and prove it sound with respect to a denotational semantics (§ 3).
• We show how to keep type checking decidable (§ 4) while using uninterpreted functions and defunctionalization to reason about extensional equality in higher-order specifications (§ 5).
• Finally, we have implemented refinement reflection in Liquid Haskell, a refinement type system for Haskell. We develop a library of (refined) proof combinators and evaluate our approach by proving various theorems about recursive, higher-order functions operating over integers and algebraic data types (§ 6).

2. Overview
We begin with a fast overview of refinement reflection and how it allows us to write proofs of and by Haskell functions.

2.1 Refinement Types
First, we recall some preliminaries about refinement types and how they enable shallow specification and verification.

Refinement types are the source program’s (here Haskell’s) types decorated with logical predicates drawn from a(n SMT decidable) logic [9, 26]. For example, we can refine Haskell’s Int datatype with a predicate $0 \leq v$, to get a Nat type:

```
type Nat = {v: Int | 0 \leq v}
```

The variable $v$ names the value described by the type, hence the above can be read as the “set of Int values $v$ that are greater than 0”. The refinement is drawn from the logic of quantifier free linear arithmetic and uninterpreted functions (QF-UFLIA [4]).

Specification & Verification We can use refinements to define and prove the textbook Fibonacci function as:

```
fib :: Nat \rightarrow Nat
fib 0 = 0
fib 1 = 1
fib n = fib (n-1) + fib (n-2)
```

Here, the input type’s refinement specifies a pre-condition that the parameters must be Nat, which is needed to ensure termination, and the output type’s refinement specifies a post-condition that the result is also a Nat. Thus refinement type checking, lets us specify and (automatically) verify the shallow property that if $\text{fib}$ is invoked with non-negative Int values, then it (terminates) and yields a non-negative value.

Propositions We can use refinements to define a data type representing propositions simply as an alias for unit, a data type that carries no run-time information:

```
type Prop = ()
```

but which can be refined with desired propositions about the code. For example, the following states the proposition $2 + 2$ equals $4$.

```
type Plus_2_2_eq_4 = {v: Prop | 2 + 2 = 4}
```

For clarity, we abbreviate the above type by omitting the irrelevant basic type Prop and variable $v$:

```
type Plus_2_2_eq_4 = {2 + 2 = 4}
```

We represent universally quantified propositions as function types:

```
type Plus_com = x: Int \rightarrow y: Int \rightarrow (x + y = y + x)
```

Here, the parameters $x$ and $y$ refer to input values; any inhabitant of the above type is a proof that Int addition is commutative.

Proofs We can now prove the above theorems simply by writing Haskell programs. To ease this task Liquid Haskell provides primitives to construct proof terms by “casting” expressions to Prop.

```
data QED = QED
(***) :: a \rightarrow QED \rightarrow Prop
_ ** _ = ()
```

To resemble mathematical proofs, we make this casting post-fix. Thus, we can write $e^{**} \ QED$ to cast $e$ to a value of Prop. For example, we can prove the above propositions simply by writing:

```
 pf_plus_2_2 :: Plus_2_2_eq_4
 pf_plus_2_2 = trivial ** QED
 pf_plus_comm :: Plus_comm
 pf_plus_comm = \x y \rightarrow trivial ** QED
 trivial = ()
```

Via standard refinement type checking, the above code yields the respective verification conditions (VCs),

```
2 + 2 = 4
\forall x, y. x + y = y + x
```

which are easily proved valid by the SMT solver, allowing us to prove the respective propositions.

A Note on Bottom: Readers familiar with Haskell’s semantics may be feeling a bit anxious about whether the dreaded “bottom”, which inhabits all types, makes our proofs suspect. Fortunately, as described in [32], Liquid Haskell ensures that all terms with non-trivial refinements provably evaluate to (non-bottom) values, thereby making our proofs sound.

2.2 Refinement Reflection
Suppose that we wish to prove properties about the fib function, e.g. that $\text{fib} \ 2$ equals $1$.

```
type fib2_eq_1 = { \text{fib} \ 2 = 1 }
```

Standard refinement type checking runs into two problems. First, for decidability and soundness, arbitrary user-defined functions do not belong the refinement logic, i.e. we cannot even refer to $\text{fib}$ in a refinement. Second, the only information that a refinement type checker has about the behavior of $\text{fib}$ is its shallow type specification $\text{Nat} \rightarrow \text{Nat}$ which is far too weak to verify $\text{fib2_eq_1}$. To address both problems, we use the following annotation, which sets in motion the three steps of refinement reflection:

```
reflect fib
```

Step 1: Definition The annotation tells Liquid Haskell to declare an uninterpreted function $\text{fib} :: \text{Int} \rightarrow \text{Int}$ in the refinement logic. By uninterpreted, we mean that the logical $\text{fib}$ is not connected to the program function fib; as far as the logic is concerned, fib only satisfies the congruence axiom

```
\forall n, m. n = m \Rightarrow \text{fib} \ n = \text{fib} \ m
```

On its own, the uninterpreted function is not terribly useful, as it does not let us prove fib2_eq_1 which requires reasoning about the definition of fib.

Step 2: Reflection In the next key step, Liquid Haskell reflects the definition into the refinement type of fib by automatically strengthening the user defined type for fib to:
fib : n:Nat → (v:Nat | fibP v n)

where fibP is an alias for a refinement automatically derived from
the function’s definition:

\[
\text{predicate fibP } v \ n =
\begin{cases}
  v = \text{if } n = 0 \text{ then } 0 \text{ else } \\
  \text{if } n = 1 \text{ then } 1 \text{ else }
\end{cases}
\]

fib (n-1) + fib (n-2)

Step 3: Application With the reflected refinement type, each application
of fib in the code automatically unfolds the fib definition
once during refinement type checking. We prove fib2_eq_1 by:

\[
\begin{align*}
\text{pf_fib2} & :: \{ \text{fib 2 = 1} \} \\
\text{pf_fib2} & == \text{fib 2 == fib 1 + fib 0} \ \ \ \ \ \text{** QED}
\end{align*}
\]

We write f to denote places where the unfolding of f’s definition
is important. The proof is verified as the above is A-normalized to

\[
\begin{align*}
\text{let} & \ (t0 = \text{fib 0}; t1 = \text{fib 1}; t2 = \text{fib 2}) \\
\text{in} & \ (t2 == t1 + t0) \ \ \ \ \ \text{** QED}
\end{align*}
\]

Which via standard refinement typing, yields the following verifica-
tion condition that is easily discharged by the SMT solver, even
though fib is uninterpreted:

\[(\text{fib} (\text{fib 0}) 0) \land (\text{fib} (\text{fib 1}) 1) \land (\text{fibP (fib 2)} 2) \Rightarrow (\text{fib 2 = 1})\]

Note that the verification of pf_fib2 relies merely on the fact that
fib was applied to (i.e. unfolded at) 0, 1 and 2. The SMT solver
can automatically combine the facts, once they are in the
antecedent. Hence, the following would also be verified:

\[
\begin{align*}
\text{pf_fib2’} & :: \{ \text{fib 2 = 1} \} \\
\text{pf_fib2’} & == \text{fib 0 , fib 1 , fib 2} \ \ \ \ \ \text{** QED}
\end{align*}
\]

Thus, unlike classical dependent typing, refinement reflection does
not perform any type-level computation.

Reflection vs. Axiomatization An alternative axiomatic
approach, used by Dafny, F’ and HALO, is to encode the definition of
fib as a universally quantified SMT formula (or axiom):

\[
\forall n. \text{fibP}(\text{fib } n) \ n
\]

Axiomatization offers greater automation than reflection. Unlike
Liquid Haskell, Dafny will verify the equivalent of the following
by automatically instantiating the above axiom at 2, 1 and 0:

\[
\begin{align*}
\text{axP_fib2} & :: \{ \text{fib 2 = 1} \} \\
\text{axP_fib2} & == \text{trivial} \ \ \ \ \ \text{** QED}
\end{align*}
\]

However, the presence of such axioms renders checking the VCs
undecidable. In practice, automatic axiom instantiation can
easily lead to infinite “matching loops”. For example, the existence
of a term fib n in a VC can trigger the above axiom, which may
then produce the terms fib (n-1) and fib (n-2), which may
then recursively give rise to further instantiations ad infinitum. To
prevent matching loops an expert must carefully craft “triggers”
and provide a “fuel” parameter [1] that can be used to restrict
the numbers of the SMT unfoldings, which ensure termination, but
can cause the axiom to not be instantiated at the right places. In short,
the undecidability of the VC checking and its attendant heuristics
makes verification unpredictable [16].

2.3 Structuring Proofs

In contrast to the axiomatic approach, with refinement reflection,
the VCs are deliberately designed to always fall in an SMT-
decidable logic, as function symbols are uninterpreted. It is upto
the programmer to unfold the definitions at the appropriate places,

which we have found, with careful design of proof combinators,
to be quite a natural and pleasant experience. To this end, we have
developed a library of proof combinators that permits reasoning
about equalities and linear arithmetic, inspired by Agda [18].

“Equation” Combinators We equip Liquid Haskell with a family
of equation combinators \( \circ \). For each logical operator \( \circ \) in
\{\(\leq\), \(\geq\), \(<\), \(\leq\), \(>, \langle\), \(\rangle\}\}, the operators in
the theory QF-UFLIA. The refinement type of \( \circ \) \( \text{requires} \) that \( x \circ y \) holds and then \( \text{ensures} \) that the returned value is equal to \( x \). For example, we define \( \circ \) as:

\[
(\text{=}): \text{x:a } \rightarrow \text{y:a } \rightarrow (\text{a} | \text{x=} \text{y}) \rightarrow (\text{v:a} | \text{v=} \text{x})
\]

and use it to write the following “equational” proof:

\[
\begin{align*}
\text{eqP_fib2} & :: \{ \text{fib 2 = 1} \} \\
\text{eqP_fib2} & == \text{fib 2} \ \ \ \ \ \text{=} \ \ \ \ \ \text{fib 0} \ \ \ \ \ \text{=} \ \ \ \ \ \text{1} \ \ \ \ \ \text{** QED}
\end{align*}
\]

“Because” Combinators Often, we need to compose “lemmas”
into larger theorems. For example, to prove fib 3 = 2 we may
wish to reuse eqP_fib2 as a lemma. To this end, Liquid Haskell
has a “because” combinator:

\[
(\because): \text{(Prop \rightarrow a) } \rightarrow \text{Prop } \rightarrow \text{a} \\
\because : \text{y = f y}
\]

The operator is simply an alias for function application that lets us
write \( x \circ y :: p \) (instead of \( (\circ) x y p \)) where \( (\circ) \) is
extended to accept an optional third proof argument via Haskell’s
type class mechanisms. We can use the because combinator to
prove that fib 3 = 2 just by writing plain Haskell code:

\[
\begin{align*}
\text{eqP_fib3} & :: \{ \text{fib 3 = 2} \} \\
\text{eqP_fib3} & == \text{fib 3} \ \ \ \ \ \text{=} \ \ \ \ \ \text{fib 2} \ \ \ \ \ \text{+} \ \ \ \ \ \text{fib 1} \\
& == \text{2} \ \ \ \ \ \text{** QED}
\end{align*}
\]

Arithmetic and Ordering SMT based refinements let us go well
beyond just equational reasoning. Next, let’s see how we can use
arithmetic and ordering to prove that fib is (locally) increasing,
\(\text{i.e.}\) for all \( n, \text{fib n} \leq \text{fib (n+1)} \)

\[
\begin{align*}
\text{fibUp} & :: n:Nat \rightarrow \{ \text{fib n} \leq \text{fib (n+1)} \} \\
\text{fibUp} & n \\
| n == 0 & \text{fib 0} \leq \text{fib 1} \\
& \text{** QED}
\end{align*}
\]

\[
\begin{align*}
| n == 1 & \text{fib 1} \leq \text{fib 1} + \text{fib 0} \leq \text{fib 2} \\
& \text{** QED}
\end{align*}
\]

\[
\begin{align*}
| \text{otherwise} & \text{fib n} \\
& \text{fib (n-1)} + \text{fib (n-2)} \leq \text{fibUp (n-1)} \\
& \text{fib n} + \text{fib (n-1)} \leq \text{fibUp (n-2)} \\
& \text{fib (n+1)} \leq \text{fibUp (n+2)} \\
& \text{** QED}
\end{align*}
\]

Case Splitting and Induction The proof fibUp works by induction
on \( n \). In the base cases 0 and 1, we simply assert the rele-
vant inequalities. These are verified as the reflected refinement un-
foils the definition of fib at those inputs. The derived VCs are
We prove the theorem by induction on the function. For example, let's prove that every locally increasing function is monotonic, i.e., if \( f(z) \leq f(z+1) \) for all \( z \), then \( f(x) \leq f(y) \) for all \( x < y \).

Lower Order Theorems

We define the following:

\[
\begin{align*}
&\text{fMono} :: f : (\text{Nat} \to \text{Int}) \\
&\quad \to \text{fUp} : (\text{z:Nat} \to \{ f z \leq f (z+1) \}) \\
&\quad \to \text{x:Nat} \\
&\quad \to \{ x \leq y \} \\
&\quad \to \{ f x \leq f y \} / \{ y \}
\end{align*}
\]

\[
\text{fMono} f \text{ inc} x y
\]

\[
\begin{align*}
| x + 1 \Rightarrow y & \Rightarrow f x \leq f (x+1) \Rightarrow f y \\
& \Rightarrow f y \Rightarrow \text{fUp} x
\end{align*}
\]

\[
\begin{align*}
\text{fUp}_{(z:Nat} & \Rightarrow \text{fibUp}_{(z \to (\text{Int}) \\
& \Rightarrow \text{x:Nat} \\
& \Rightarrow \{ x \leq y \} \\
& \Rightarrow \{ f x \leq f y \} / \{ y \}
\end{align*}
\]

\[
\begin{align*}
&\text{fMono} :: f : (\text{Nat} \to \text{Int}) \\
&\quad \to \text{fUp} : (\text{z:Nat} \to \{ f z \leq f (z+1) \}) \\
&\quad \to \text{x:Nat} \\
&\quad \to \{ x \leq y \} \\
&\quad \to \{ f x \leq f y \} / \{ y \}
\end{align*}
\]

We prove the theorem by induction on \( y \), which is specified by the annotation \( / y \) which states that \( y \) is a well-founded termination metric that decreases at each recursive call [32]. If \( x+1 = y \), then we use \( \text{fUp} x \). Otherwise, \( x+1 < y \), and we use the induction hypothesis \( i.e. \) apply \( \text{fMono} \) at \( y-1 \), after which transitivity of the less-than ordering finishes the proof. We can use the general \( \text{fMono} \) theorem to prove that \( \text{fib} \) increases monotonically:

\[
\text{fibMono} :: n : \text{Nat} \Rightarrow m : \{ n = m \} \\
\Rightarrow \{ \text{fib} n \leq \text{fib} m \}
\]

\[
\text{fibMono} = \text{fMono} \text{ fib} \text{ fibUp}
\]

2.4 Case Study: Peano Numerals

Refinement reflection is not limited to programs operating on integers. We conclude the overview with a small library for Peano numerals, defined via the following algebraic data type:

\[
\text{data} \ Peano \ = \ Z \ | \ S \ Peano
\]

We can add two Peano numbers via:

\[
\text{reflect} \ add :: Peano \to Peano \to Peano
\]

\[
\begin{align*}
\text{add} & \ Z \ m = m \\
\text{add} & \ (S \ n) \ m = S \ (\text{add} \ n \ m)
\end{align*}
\]

In §3.5 we will describe exactly how the reflection mechanism (illustrated via \( \text{fibF} \)) is extended to account for ADTs like \( \text{Peano} \). Note that Liquid Haskell automatically checks that \( \text{add} \) is total [32], which lets us safely \( \text{reflect} \) it into the refinement logic.

Add Zero to Left

As an easy warm up, let's show that adding zero to the left leaves the number unchanged:

\[
\text{zeroL} :: n : \text{Peano} \Rightarrow \{ \text{add} \ Z \ n \Rightarrow n \}
\]

\[
\text{zeroL} \ n = \ \text{add} \ Z \ n
\]

\[
\begin{align*}
\text{zeroL} \ n & \Rightarrow n \Rightarrow \text{QED}
\end{align*}
\]

Add Zero to Right

It is slightly more work to prove that adding zero to the right also leaves the number unchanged.

\[
\text{zeroR} :: n : \text{Peano} \Rightarrow \{ \text{add} \ Z \ n \Rightarrow n \}
\]

\[
\text{zeroR} \ Z = \ \text{add} \ Z \ Z
\]

We can add (in the refinement logic) \( \text{add} \) is commutative:

\[
\begin{align*}
\text{add_com} :: a : \_ \to b : \_ \to \{ \text{add} \ a \ b \Rightarrow \text{add} \ b \ a \}
\end{align*}
\]

\[
\begin{align*}
\text{add_com} \ Z \ b & = \ \text{add} \ Z \ b \\
& = \ b
\end{align*}
\]

\[
\begin{align*}
\text{add_com} \ (S \ a) \ b & = \ \text{add} \ (S \ a) \ b \\
& = \ S \ (\text{add} \ a \ b)
\end{align*}
\]

Thus, reflection lets us prove properties of Haskell programs just by writing Haskell programs: lemmas are just functions, case-splittings just branching and pattern matching, and induction just recursion. Next, we formalize refinement reflection and describe how to keep type checking decidable and predictable.

3. Refinement Reflection

Our first step towards formalizing refinement reflection is a core calculus \( \lambda^R \) with an undecidable type system based on denotational semantics. We show how the soundness of the type system allows us to prove theorems using \( \lambda^R \).

3.1 Syntax

Figure 1 summarizes the syntax of \( \lambda^R \), which essentially is the calculus \( \lambda^E \) [32] with explicit recursion and a special \( \text{reflect} \) binding form to denote terms that are reflected into the refinement logic. In \( \lambda^R \) refinements \( r \) are arbitrary expressions \( e \) (hence \( r ::= e \) in Figure 1). This choice allows us to prove preservation and progress, but renders typechecking undecidable. In §4 we will see how to recover decidability by soundly approximating refinements.

The syntactic elements of \( \lambda^R \) are layered into primitive constants, values, expressions, binders and programs.

Constants

The primitive constants of \( \lambda^R \) include all the primitive logical operators \( \text{and}, \text{or}, \text{not} \), the set \( \{ =, \leq \} \). Moreover, they include the primitive booleans \( \text{True}, \text{False} \), integers \( -1, 0, 1, \text{etc.} \), and logical operators \( \land, \lor, \neg, \text{etc.} \).

Data Constructors

We encode data constructors as special constants. For example the data type \([\text{Int}]\), which represents finite lists of integers, has two data constructors: \([\text{nil}]\) and \((\text{cons}\)\).
Consider the output of the primitive constant operation. For example, constants \( \lambda x.e \) values. The expressions of let recursive definitions are allowed but cannot be inserted into the stratification of programs via binders is required so that arbitrary recursive definitions are allowed but cannot be inserted into the logic via refinements or reflection. (We can allow non-recursive let binders in \( e \), but omit them for simplicity.)

### 3.2 Operational Semantics

Figure 1 summarizes the small step contextual \( \beta \)-reduction semantics for \( \lambda^R \). We write \( e \to e' \) if there exist \( e_1, \ldots, e_j \) such that \( e \to e_1 \to \cdots \to e_j \). We write \( e \to^* e' \) if there exists some finite \( j \) such that \( e \to^* e' \). We define \( \approx \) to be the reflexive, symmetric, transitive closure of \( \to^* \).

#### Constants

Application of a constant requires the argument be reduced to a value; in a single step the expression is reduced to the output of the primitive constant operation. For example, consider \( = \), the equality operator on integers. We have \( \delta(=, n) \) is the same as \( n \). We assume that the equality operator is defined for all values, and, for functions, is defined as extensional equality. That is, for all \( f \) and \( f' \) we have \( (f = f') \to \text{True} \) if \( \forall x. f x \approx f' x \). We assume source terms only contain implementable equalities over non-function types; the above only appears in refinements and allows us to state and prove facts about extensional equality § 5.2.

### 3.3 Types

\( \lambda^R \) types include basic types, which are refined with predicates, and dependent function types. Basic types \( B \) comprise integers, booleans, and a family of data-types \( T \) (representing lists, trees, etc.) For example the data type \([\text{Int}]\) represents lists of integers.

We refine basic types with predicates (boolean valued expressions \( e \)) to obtain basic refinement types \( \{ v : B \mid e \} \). Finally, we have dependent function types \( x : \tau \to \tau \) where the input \( x \) has the type \( \tau \) and the output \( \tau \) may refer to the input binder \( x \). We write \( B \) to abbreviate \( \{ v : B \mid \text{True} \} \), and \( \tau \to \tau \to \tau \) to abbreviate \( x : \tau \to \tau \) if \( x \) does not appear in \( \tau \). We use \( \to \) to refer to refinements.

#### Denotations

Each type \( \tau \) denotes a set of expressions \( \{ \tau \} \), that are defined via the dynamic semantics [14]. Let \( \{ \tau \} \) be the type we get if we erase all refinements from \( \tau \) and \( e : [\tau] \) be the standard typing relation for the typed lambda calculus. Then, we define the denotation of types as:

\[
\{ c : B \mid \{ \tau \} \} = \{ e : B \mid e \to \text{True} \} \quad \text{s.t.} \quad [x : \tau \to \tau] \to \{ e : [\tau] \mid e c \} 
\]

#### Constants

For each constant \( c \) we define its type \( Ty(c) \) such that \( c \in [Ty(c)] \). For example,

\[
\begin{align*}
\text{Ty}(3) & = \{ v : \text{Int} \mid v = 3 \} \\
\text{Ty}(+) & = \{ x, y : \text{Int} \mid \{ v : \text{Int} \mid v = x + y \} \} \\
\text{Ty}(\leq) & = \{ x, y : \text{Int} \mid \{ v : \text{Bool} \mid v \leq x \} \}
\end{align*}
\]

So, by definition we get the constant typing lemma

**Lemma 1. Constant Typing.** Every constant \( c \in [Ty(c)] \).

Thus, if \( Ty(c) \subseteq \{ \tau \} \), then for every value \( w \in [\tau] \), we require \( \delta(c, w) \in [\tau[x \to w]] \).

### 3.4 Refinement Reflection

The simple, but key idea in our work is to strengthen the output type of functions with a refinement that reflects the definition of the function in the logic. We do this by treating each reflect-binder: \( \text{reflect } f : \tau = e \) in \( p \) as a let rec-binder: \( \text{let rec } \text{reflect } f : \tau = e \) in \( p \) during type checking (rule T-REFLECT in Figure 3).

#### Reflection

We write \( \text{Reflect}(\tau, e) \) for the reflection of term \( e \) into the type \( \tau \), defined by strengthening \( \tau \) as:

\[
\begin{align*}
\text{Reflect}(\{ x : B \mid \{ \tau \} \}, e) & = \{ x : B \mid x \wedge y = e \} \\
\text{Reflect}(\{ x : \tau \to \tau \mid \{ \tau \} \}, e) & = \{ x : \tau \to \text{Reflect}(\{ y : \tau \mid \{ \tau \} \}, e) \}
\end{align*}
\]

As an example, recall from § 2 that the reflect \( \text{fib} \) strengthens the type of \( \text{fib} \) with the reflected refinement \( \text{fib} ? \).

#### Consequences for Verification

Reflection has two consequences for verification. First, the reflected refinement is not trusted; it is itself verified (as a valid output type) during type checking. Second, instead of being tethered to quantifier instantiation heuristics or having to program “iggers” as in Dafny [15] or F’ [30] the programmer can predictably “unfold” the definition of the function during a proof simply by “calling” the function, which we have found to be a very natural way of structuring proofs § 6.

### 3.5 Refining & Reflecting Data Constructors with Measures

We assume that each data type is equipped with a set of measures which are unary functions whose (1) domain is the data type, and (2) body is a single case-expression over the datatype [32]:

\[
\text{measure } f : \tau = \lambda x. e \quad \text{y = x of } \{ D, \tau \to e_i \}
\]

For example, \( \text{len} \) measures the size of an [Int]:
Checking and Projection We assume the existence of measures that check the top-level constructor, and project their individual fields. In § 4.2 we show how to use these measures to reflect functions over datatypes. For example, for lists, we assume the existence of measures:

\[
\begin{align*}
\text{isNil} & \colon [] = \text{True} \\
\text{isNil} & \colon (x:\text{xs}) = \text{False} \\
\text{isCons} & \colon (x:\text{xs}) = \text{True} \\
\text{isCons} & \colon [] = \text{False} \\
\text{sel1} & \colon (x:\text{xs}) = x \\
\text{sel2} & \colon (x:\text{xs}) = \text{xs}
\end{align*}
\]

Refining Data Constructors with Measures We use measures to strengthen the types of data constructors, and we use these strengthened types during construction and destruction (pattern-matching). For example, we use the expression bindings:

\[
\begin{align*}
\text{len} & \colon \text{x} \rightarrow \text{case } \text{x} \text{ of} \\
[&] & \rightarrow 0 \\
(x:\text{xs}) & \rightarrow 1 + \text{len } \text{xs}
\end{align*}
\]

Next, we present the type-checking judgments and rules of \(\lambda^R\). For example, we have:

\[
\begin{align*}
\text{isCons } \text{x} \text{xs} & = \text{True} \\
\text{isNil } \text{x} \text{xs} & = \text{False} \\
\text{len } \text{x} \text{xs} & = 0 \\
\text{len } \text{x} \text{xs} & = 1 + \text{len } \text{xs}
\end{align*}
\]

Well-Formedness

\[
\begin{align*}
\Gamma, \forall \theta \in [\Gamma], \theta \cdot \{v : B | e_1\} & \subseteq \theta \cdot \{v : B | e_2\} \\
\Gamma & \vdash v : B | e_1 \\
\Gamma & \vdash v : B | e_2 \\
\Gamma & \vdash x : \tau \rightarrow \tau
\end{align*}
\]

Subtyping

\[
\begin{align*}
\forall \theta \in [\Gamma], \theta \cdot \{v : B | e_1\} & \subseteq \theta \cdot \{v : B | e_2\} \\
\Gamma & \vdash v : B | e_1 \\
\Gamma & \vdash v : B | e_2 \\
\Gamma & \vdash x : \tau \rightarrow \tau
\end{align*}
\]

Typing

\[
\begin{align*}
\text{T-V} & \colon \Gamma \vdash \text{x} : \tau \\
\text{T-CON} & \colon \Gamma \vdash c : \text{Ty}(c) \\
\text{T-SUB} & \colon \Gamma \vdash p : \tau' \rightarrow \tau \\
\Gamma & \vdash \text{reflect } f : \text{Reflect}(\tau_f, e) = e \text{ in } p : \tau \\
\text{T-APP} & \colon \Gamma \vdash e_1 : (x : \tau_x) \\
\Gamma & \vdash e_2 : \tau_x \\
\text{T-Let} & \colon \Gamma \vdash \text{let rec } x = e \text{ of } D, \gamma \rightarrow e_1 : \tau
\end{align*}
\]

Figure 3. Typing of \(\lambda^R\)
As a proposition, for example, the application \( \text{fib} \) is required to equate the reflected functions in the type. This is a generalization of the “selfification” rules from [14, 21], and is required to equate the reflected functions with their definitions. For example, the application (\( \text{fib} \)) is typed as \( \{ v : \text{Int} \mid \text{fib}P v 1 \wedge v = \text{fib} 1 \} \) where the first conjunct comes from the (reflection-strengthened) output refinement of \( \text{fib} \) § 2, and the second conjunct comes from rule T-EXACT. Finally, rule T-FIX is used to type the intermediate \( \text{fix} \) expressions that appear, not in the surface language but as intermediate terms in the operational semantics.

**Soundness** Following \( \lambda^U \) [32], we can show that evaluation preserves typing and that typing implies denotational inclusion.

**Theorem 1.** \( \text{[Soundness of } \lambda^R \text{]} \)

- **Definitions** If \( \Gamma \vdash p : \tau \) then \( \forall \theta \in [\Gamma], \theta \cdot p \in [\theta \cdot \tau] \).
- **Preservation** If \( \forall \theta \mid \theta \vdash p : \tau \) and \( p \mapsto w \) then \( \theta \vdash w : \tau \).

**3.7 From Programs & Types to Propositions & Proofs**

The denotational soundness Theorem 1 lets us interpret well-typed programs as proofs of propositions.

**“Definitions”** A definition \( d \) is a sequence of reflected binders: 

\[
d ::= \bullet \mid \text{reflect } x : \tau = e \in d
\]

A definition’s environment \( \Gamma(d) \) comprises its binders and their reflected types:

\[
\Gamma(\bullet) = \emptyset
\]

\[
\Gamma(\text{reflect } f : \tau = e \in d) = (f, \text{Reflect}(\tau, e)), \Gamma(d)
\]

A definition’s substitution \( \theta(d) \) maps each binder to its definition:

\[
\theta(\bullet) = \emptyset
\]

\[
\theta(\text{reflect } f : \tau = e \in d) = [[f \mapsto \text{fix } f] e], \theta(d)
\]

**“Propositions”** A proposition is a type

\[
x_1 : \tau_1 \rightarrow \ldots \rightarrow x_n : \tau_n \rightarrow \{ v : \text{Unit} \mid \text{prop} \}
\]

For brevity, we abbreviate propositions like the above to \( \overline{\tau} : \tau \rightarrow \{ \text{prop} \} \) and we call \( \text{prop} \) the proposition’s refinement. For simplicity we assume that \( \forall v(\tau_v) = \emptyset \).

**“Validity”** A proposition \( \overline{\tau} : \overline{\tau} \rightarrow \{ \text{prop} \} \) is valid under \( d \) if

\[
\forall \overline{w} \in [\overline{\tau}], \theta(d) \cdot \text{prop}[\overline{\tau} \mapsto \overline{w}] \hookrightarrow^* \text{True}
\]

That is, the proposition is valid if its refinement evaluates to \( \text{True} \) for every (well typed) interpretation for its parameters \( \overline{\tau} \) under \( d \).

**“Proofs”** A binder \( b \) proves a proposition \( \tau \) under \( d \) if

\[
\theta(\text{reflect } f : \tau = e \in d) = [[f \mapsto \text{fix } f] e], \theta(d)
\]

That is, if the binder \( b \) has the proposition’s type \( \tau \) under the definition \( d \)’s environment.

**Theorem 2.** \( \text{[Proofs]} \) If \( b \) proves \( \tau \) under \( d \) then \( \tau \) is valid under \( d \).

**Proof.** As \( b \) proves \( \tau \) under \( d \), we have

\[
\theta(\text{reflect } f : \tau = e \in d) = [[f \mapsto \text{fix } f] e], \theta(d)
\]

\[
\theta(\text{reflect } f : \tau = e \in d) = [[f \mapsto \text{fix } f] e], \theta(d)
\]

\[
\theta(\text{reflect } f : \tau = e \in d) = [[f \mapsto \text{fix } f] e], \theta(d)
\]

\[
\theta(\text{reflect } f : \tau = e \in d) = [[f \mapsto \text{fix } f] e], \theta(d)
\]

\[
\theta(\text{reflect } f : \tau = e \in d) = [[f \mapsto \text{fix } f] e], \theta(d)
\]

\[
\theta(\text{reflect } f : \tau = e \in d) = [[f \mapsto \text{fix } f] e], \theta(d)
\]

\[
\theta(\text{reflect } f : \tau = e \in d) = [[f \mapsto \text{fix } f] e], \theta(d)
\]

\[
\theta(\text{reflect } f : \tau = e \in d) = [[f \mapsto \text{fix } f] e], \theta(d)
\]

Hence, the above set is not empty, and hence \( \tau \) is valid under \( d \).

**Example: Fibonacci is increasing** In § 2 we verified that under a definition \( d \) that includes \( \text{fib} \), the term \( \text{fibUp} \) proves

\[
\forall n.0 \leq n \hookrightarrow^* \text{True} \Rightarrow \text{fib} n \leq \text{fib} (n + 1)
\]

Thus, by Theorem 2 we get

\[
\forall n.0 \leq n \hookrightarrow^* \text{True} \Rightarrow \text{fib} n \leq \text{fib} (n + 1) \hookrightarrow^* \text{True}
\]

**4. Algorithmic Verification**

Next, we describe \( \lambda^S \), a conservative approximation of \( \lambda^R \) where the undecidable type subsumption rule is replaced with a decidable one, yielding an SMT-based algorithmic type system that enjoys the same soundness guarantees.

**4.1 The SMT logic \( \lambda^S \)**

**Syntax: Terms & Sorts** Figure 4 summarizes the syntax of \( \lambda^S \), the sorted (SMT-) decidable logic of quantifier-free equality, uninterpreted functions and linear arithmetic (QF-EUFLIA) [4, 19]. The terms of \( \lambda^S \), include integers \( n \), booleans \( \text{Bool} \), variables \( x \), data constructors \( D \) (encoded as constants), fully applied unary \( \oplus_2 \) and binary \( \oplus_2 \) operators, and application \( x \tau \) of an uninterpreted function \( x \). The sorts of \( \lambda^S \) include built-in integers \( \text{Int} \) and \( \text{Bool} \) for representing integers and booleans. The interpreted functions of \( \lambda^S \), e.g. the logical constants \( = \) and \(<\), have the function sort \( s \rightarrow s \). Other functional values in \( \lambda^S \), e.g. reflected \( \lambda \) functions and \( \lambda \)-expressions, are represented as first-order values with uninterpreted sort \( \text{Fun} s a \). The universal sort \( \text{Unit} \) represents all other values.

**Semantics: Satisfaction & Validity** An assignment \( \sigma \) is a mapping from variables to terms \( \sigma \models \{ x_1 \mapsto r_1, \ldots, x_n \mapsto r_n \} \). We write \( \sigma \models \tau \) if the assignment \( \sigma \) is a model of \( \tau \), intuitively if \( \sigma \models r \) “is true” [19]. A predicate \( r \) is satisfiable if there exists \( \sigma \models r \). A predicate \( r \) is valid if for all assignments \( \sigma \models r \).

---

**Figure 4. Syntax of \( \lambda^S \)**

By Theorem 1 on 1 we get

\[
\theta(d) \in [\Gamma(d)]
\]

Furthermore, by the typing rules 1 implies \( \Gamma(d) \vdash b : \tau \) and hence, via Theorem 1

\[
\forall \theta \in [\Gamma(d)]. \theta \cdot b \in [\theta \cdot \tau]
\]

Together, 2 and 3 imply

\[
\theta(d) \cdot b \in [\theta(d) \cdot \tau]
\]

By the definition of type denotations, we have

\[
[\theta(d) \cdot \tau] \models \{ f \mid \text{r is valid under } d \}
\]

By 4, the above set is not empty, and hence \( \tau \) is valid under \( d \).

---

7 2016/10/12
4.2 Transforming \( \lambda^R \) into \( \lambda^S \)

The judgment \( \Gamma \vdash e \rightsquigarrow r \) states that a \( \lambda^R \) term \( e \) is transformed, under an environment \( \Gamma \), into a \( \lambda^S \) term \( r \). The transformation rules are summarized in Figure 5.

**Embedding Types** We embed \( \lambda^R \) types into \( \lambda^S \) sorts as:

\[
\begin{align*}
\text{(Int)} & \quad \cong \quad \text{Int} \\
\text{(Bool)} & \quad \cong \quad \text{Bool} \\
\end{align*}
\]

**Embedding Constants** Elements shared on both \( \lambda^R \) and \( \lambda^S \) translate to themselves. These elements include booleans (T-BOOL), integers (T-INT), variables (T-VAR), binary (T-BIN) and unary (T-UN) operators. SMT solvers do not support currying, and so in \( \lambda^S \), all function symbols must be fully applied. Thus, we assume that all applications to primitive constants and data constructors are saturated, i.e., fully applied, e.g. by converting source level terms like \((+ 1)\) to \((\lambda x.x + 1)\).

**Embedding Functions** As \( \lambda^S \) is a first-order logic, we embed \( \lambda \)-abstraction and application using the uninterpreted functions \( \text{lam} \) and \( \text{app} \). We embed \( \lambda \)-abstractions using \( \text{lam} \) as shown in rule T-FUN. The term \( \text{lam} e \) of type \( \tau_0 \rightarrow \tau \) is transformed to \( \text{lam}_{\tau_0}^\lambda \ x \ r \) of sort \( \text{Fun} s_0 s \), where \( s_0 \) and \( s \) are respectively \( (\tau_0) \) and \( (\tau) \). \( \text{lam}_{\tau_0}^\lambda \) is a special uninterpreted function of sort \( \text{Fun} s_0 s \), and \( x \) of sort \( s_0 \) and \( r \) of sort \( s \) are the embedding of the binder and body, respectively. As \( \text{lam} \) is just an SMT-function, it does not create a binding for \( x \). Instead, the binder \( x \) is renamed to a fresh name pre-declared in the SMT environment.

**Embedding Applications** Dually, we embed applications via de-functionalization [23] using an uninterpreted \( \text{apply} \) function \( \text{app} \) as shown in rule T-APP. The term \( e \ e' \), where \( e \) and \( e' \) have types \( \tau_0 \rightarrow \tau \) and \( \tau_0 \), is transformed to \( \text{app}_{\tau_0}^\ast \ r \ r' \) of sort \( s \) where \( s \) and \( s_0 \) are respectively \( (\tau) \) and \( (\tau_0) \), the \( \text{app}_{\tau_0}^\ast \) is a special uninterpreted function of sort \( \text{Fun} s \), where \( s \rightarrow s \rightarrow s \) and \( r \) and \( r' \) are the respective translations of \( e \) and \( e' \).

**Embedding Data Types** Rule T-DC translates each data constructor to a predefined \( \lambda^S \) constant \( s_D \) of sort \( (\text{Ty}(D)) \). Let \( D \) be a non-boolean data constructor such that

\[ \text{Ty}(D) \cong \tau_{i_1} \rightarrow \cdots \rightarrow \tau_{i_n} \rightarrow \tau \]

Then the check function \( \text{is} \) has the sort \( \text{Fun} (\tau) \text{Bool} \) and the select function \( \text{select} \) has the sort \( \text{Fun} (\tau) (\tau_{i_1}) \). Rule T-Case translates case-expressions of \( \lambda^R \) into nested if terms in \( \lambda^S \), by using the check functions in the guards, and the select functions for the binders of each case. For example, following the above, the body of the list append function

\[
\begin{align*}
[] & \quad \text{++} \ x \ y = \ y s \n x & \quad \text{++} \ x = x : (x \text{++} \ y)
\end{align*}
\]

is reflected into the \( \lambda^S \) refinement:

\[
\text{isNil} \text{Nil} x s \text{then} \ y s \text{else} \text{select} \text{Nil} x s : (\text{select} \text{List} ++ s)
\]

We favor selectors to the axiomatic translation of HALO [35] and F* [30] to avoid universally quantified formulas and the resulting instantiation unpredictability.

4.3 Correctness of Translation

Informally, the translation relation \( \Gamma \vdash e \rightsquigarrow r \) is correct in the sense that if \( e \) is a terminating boolean expression then \( e \) reduces to \( \text{True} \) if \( r \) is SMT-satisfiable by a model that respects \( \beta \)-equivalence.

**Definition 1 (\( \beta \)-Model).** A \( \beta \)-model \( \sigma^0 \) is an extension of a model \( \sigma \) where \( \text{lam} \) and \( \text{app} \) satisfy the axioms of \( \beta \)-equivalence:

\[
\forall x y e. \text{lam} x e = \text{lam} y (e[x \mapsto y])
\]

\[
\forall x e x. (\text{app} (\text{lam} x e) e) = e[x \mapsto e]
\]

**Semantics Preservation** We define the translation of a \( \lambda^R \) term into \( \lambda^S \) under the empty environment as \( \text{[e]} \cong r \) if \( \emptyset \vdash e \rightsquigarrow r \). A lifted substitution \( \theta^+ \) is a set of models \( \sigma \) where each “bottom” of the substitution \( \theta \) is mapped to an arbitrary logical value of the respective sort [32]. We connect the semantics of \( \lambda^R \) and translated \( \lambda^S \) via the following theorems:

**Theorem 3.** If \( \Gamma \vdash e \rightsquigarrow r \), then for every \( \theta \in [\Gamma] \) and every \( \sigma \in \theta^+ \), if \( \theta^+ \cdot e \rightsquigarrow s \) then \( \sigma^0 \models r \models [e] \).

**Corollary 1.** If \( \Gamma \vdash e : \text{Bool} \), \( e \) reduces to a value and \( \Gamma \vdash e \rightsquigarrow r \), then for every \( \theta \in [\Gamma] \) and every \( \sigma \in \theta^+ \), \( \theta^+ \cdot e \rightsquigarrow^* \text{True} \) if \( \sigma^0 \models r \models [e] \).

4.4 Decidable Type Checking

Figure 6 summarizes the modifications required to obtain decidable type checking. Namely, basic types are extended with labels that track termination and subtyping is checked via an SMT solver.

**Termination** Under arbitrary beta-reduction semantics (which includes lazy evaluation), soundness of refinement type checking requires checking termination, for two reasons: (1) to ensure that refinements cannot diverge, and (2) to account for the environment during subtyping [32]. We use \( \parallel \) to mark provably terminating computations, and extend the rules to use refinements to ensure that if \( \Gamma \vdash s : e : \{v : B^0 | r\} \), then \( e \) terminates [32].

**Verification Conditions** The verification condition (VC) \( \langle [\Gamma] \Rightarrow \parallel r \rangle \) is valid only if the set of values described by \( \Gamma \), is subsumed by the set of values described by \( r \). \( \Gamma \) is embedded into logic by adjoining (the embeddings of) the refinements of provably
### Refined Types

\[ \tau ::= \{v : B^{[i]} \mid e\} \mid x : \tau \rightarrow \tau \]

### Well Formedness

\[ \Gamma \vdash_{S} \tau \]

\[ \frac{\Gamma, v : B \vdash_{S} e : \text{Bool}^{\emptyset}}{\Gamma \vdash_{S} \{v : B \mid e\}} \quad \text{WF-BASE} \]

### Subtyping

\[ \Gamma \vdash \tau \leq \tau' \]

\[ \frac{\Gamma' \equiv \Gamma, v : B^{[i]} \vdash e' \leadsto r'}{\Gamma \vdash \{v : B \mid e\} \leq \{v : B \mid e'\} \quad \text{-BASE}} \]

### Figure 6. Algorithmic Typing (other rules in Figs 1 and 3.)

terminating binders [32]:

\[ \langle \Gamma \rangle \equiv \bigwedge_{x \in \Gamma} \langle \Gamma, x \rangle \]

where we embed each binder as

\[ \langle \Gamma, x \rangle \equiv \begin{cases} r & \text{if } \Gamma(x) = \{v : B^{[i]} \mid e\}, \Gamma \vdash e[v \mapsto x] \leadsto r \in \text{reduced terms} \\ \text{True} & \text{otherwise} \end{cases} \]

### Subtyping via SMT Validity

We make subtyping, and hence, typing decidable, by replacing the denotational base subtyping rule \( \leq \text{-BASE} \) with a conservative, algorithmic version that uses an SMT solver to check the validity of the subtyping VC. We use Corollary 1 to prove soundness of subtyping.

**Lemma 2.** If \( \Gamma \vdash_{S} \{v : B \mid e_1\} \leq \{v : B \mid e_2\} \) then \( \Gamma \vdash \{v : B \mid e_1\} \leq \{v : B \mid e_2\} \).  

**Soundness of \( \lambda^8 \)** Lemma 2 directly implies the soundness of \( \lambda^8 \).

**Theorem 4 (Soundness of \( \lambda^8 \)).** If \( \Gamma \vdash_{S} e : \tau \) then \( \Gamma \vdash e : \tau \).

### 5. Reasoning About Lambdas

Though \( \lambda^8 \), as presented so far, is sound and decidable, it is imprecise: our encoding of \( \lambda \)-abstractions and applications via uninterpreted functions makes it impossible to prove theorems that require \( \alpha \)- and \( \beta \)-equivalence, or extensional equality. Next, we show how to address the former by strengthening the VCs with equalities \( \leq \text{-BASE} \), and the latter by introducing a combinator for safely asserting extensional equality \( \leq \text{-BASE} \). In the rest of this section, for clarity we omit \texttt{app} when it is clear from the context.

#### 5.1 Equivalence

As soundness relies on satisfiability under a \( \sigma^\emptyset \) (see Definition 1), we can safely instantiate the axioms of \( \alpha \)- and \( \beta \)-equivalence on any set of terms of our choosing and still preserve soundness (Theorem 4). That is, instead of checking the validity of a VC \( p \Rightarrow q \), we check the validity of a strengthened VC, \( a \Rightarrow p \Rightarrow q \), where \( a \) is a (finite) conjunction of equivalence instances derived from \( p \) and \( q \), as discussed below.

**Representation Invariant** The lambda binders, for each SMT sort, are drawn from a pool of names \( x_i \) where the index \( i = 1, 2, \ldots \). When representing \( \lambda \) terms we enforce a normalization invariant that for each lambda term \( \lambda m \ x \ e \), the index \( i \) is greater than any lambda argument appearing in \( e \).

**\( \alpha \)-instances** For each syntactic term \( \lambda m \ x \ e \), and \( \lambda \)-binder \( x_j \) such that \( i < j \) appearing in the VC, we generate an \( \alpha \)-equivalence instance predicate (or \( \alpha \)-instance):

\[ \lambda m \ x \ e = \lambda m \ x \ e[x_i \mapsto x_j] \]

The conjunction of \( \alpha \)-instances can be more precise than De Bruijn representation, as they let the SMT solver deduce more equalities via congruence. For example, consider the VC needed to prove the applicative laws for \texttt{Reader}:

\[ d = \lambda m \ x (x m) \Rightarrow \lambda m \ x \ (\lambda m \ (x m) (x m)) = \lambda m \ x \ d \]

The \( \alpha \) instance \( \lambda m \ x (d m) = \lambda m \ x \ (d m) \) derived from the VC’s hypothesis, combined with congruence immediately yields the VC’s consequence.

**\( \beta \)-instances** For each syntactic term \( \text{app} \ (\lambda m \ x \ e) \ e_{\emptyset} \), with \( e_{\emptyset} \) not containing any \( \lambda \)-abstractions, appearing in the VC, we generate an \( \beta \)-equivalence instance predicate (or \( \beta \)-instance):

\[ \text{app} \ (\lambda m \ x \ e) \ e_{\emptyset} = \text{e}[x_i \mapsto e_{\emptyset}] \quad \text{s.l. } e_{\emptyset} \text{ is } \lambda \text{-free} \]

We require the \( \lambda \)-free restriction as a simple way to enforce that the reduced term \( e[x_i \mapsto e_{\emptyset}] \) enjoys the representation invariant.

For example, consider the following VC needed to prove that the bind operator for lists satisfies the monadic associativity law:

\[ (f x \gg g) = \text{app} \ (\lambda m \ y (f y \gg g)) x \]

The right-hand side of the above VC generates a \( \beta \)-instance that corresponds directly to the equality, allowing the SMT solver to prove the (strengthened) VC.

**Normalization** The combination of \( \alpha \) - and \( \beta \)-instances is often required to discharge proof obligations. For example, when proving that the bind operator for the \texttt{Reader} monad is associative, we need to prove the VC:

\[ \lambda m \ x_2 (\lambda m \ x_1 w) = \lambda m \ x_3 (\text{app} \ (\lambda m \ x_2 (\lambda m \ x_1 w)) w) \]

The SMT solver proves the VC via the equalities corresponding to an \( \alpha \) and then \( \beta \)-instance:

\[ \lambda m \ x_2 (\lambda m \ x_1 w) = \alpha \lambda m \ x_2 (\lambda m \ x_1 w) = \beta \lambda m \ x_2 (\text{app} \ (\lambda m \ x_2 (\lambda m \ x_1 w))) w \]

### 5.2 Extensionality

Often, we need to prove that two functions are equal, given the definitions of reflected binders. For example, consider

\[ \textbf{reflect} \quad \text{id} \quad \text{id} \ x = x \]

Liquid Haskell accepts the proof that \texttt{id} \( x = x \) for all \( x \):

\[ \text{if} \ x \text{eq} \ x :: \text{a} \rightarrow \{\text{id} \ x = x\} \]

\[ \text{if} \ x \text{eq} \ x = \langle \text{x} \rightarrow \text{id} \ x \rangle = (\text{y} \rightarrow \text{y}) \]

Liquid Haskell rejects the proof:

\[ \text{fails} :: \text{Id} \text{eq} \text{id} \quad \text{fails} = (\langle \text{x} \rightarrow \text{id} \ x \rangle =. (\text{y} \rightarrow \text{y}) \quad \text{**} \text{QED} \]

The invocation of \texttt{if} \( x \text{eq} \ x \) unfolds its definition, completing the proof. However, consider this \( \eta \)-expanded variant of the above proposition:

\[ \textbf{type} \quad \text{Id} \text{eq} \text{id} = \{ \langle \text{x} \rightarrow \text{id} \ x \rangle = (\text{y} \rightarrow \text{y}) \} \]

Liquid Haskell rejects the proof:

\[ \text{fails} :: \text{Id} \text{eq} \text{id} \quad \text{fails} = (\langle \text{x} \rightarrow \text{id} \ x \rangle =. (\text{y} \rightarrow \text{y}) \quad \text{**} \text{QED} \]

The invocation of \texttt{if} \( x \text{eq} \ x \) unfolds the definition, but the resulting equality refinement \( \{\text{id} \ x = x\} \) is \textit{trapped} under the \( \lambda \)-abstraction. That is, the equality is absent from the typing environment at the top level, where the left-hand side term is compared to \( \text{y} \rightarrow \text{y} \). Note that the above equality requires the definition of \texttt{id} and hence is outside the scope of purely the \( \alpha \)- and \( \beta \)-instances.
An Extensionality Operator
To allow function equality via extensionality, we provide the user with a (family of) function comparison operator(s) that transform an explanation \( p \) which is a proof that \( f \ x = g \ x \) for every argument \( x \), into a proof that \( f = g \).

\[
\Rightarrow V : f : (a \rightarrow b) \rightarrow g: (a \rightarrow b) \\
\Rightarrow \text{exp} : (x:a \rightarrow \{f \ x = g \ x\}) \\
\Rightarrow \{f = g\}
\]

Of course, \( \Rightarrow V \) cannot be implemented; its type is assumed. We can use \( \Rightarrow V \) to prove \( \text{Id\_eq\_id} \) by providing a suitable explanation:

\[
\text{pf\_id\_id} = (\forall y \rightarrow y) \Rightarrow V (\forall x \rightarrow \text{id} \ x) \cdot : \text{exp} \cdot \quad ** \text{QED}
\]

where

\[
\text{exp1} = (\forall x \rightarrow \text{id} \ x = . \ x ** \text{QED})
\]

The explanation is the second argument to \( \cdot \) which has the following type that syntactically fires \( \beta \)-instances:

\[
x : a \rightarrow (\forall x \rightarrow \text{id} \ x) \ x = (\forall x \rightarrow \text{id} \ x) \ x
\]

6. Evaluation

We have implemented refinement reflection in Liquid Haskell. In this section, we evaluate our approach by using Liquid Haskell to verify a variety of deep specifications of Haskell functions drawn from the literature and categorized in Figure 7, totalling about 2500 lines of specifications and proofs. Next, we detail each of the four classes of specifications, illustrate how they were verified using refinement reflection, and discuss the strengths and weaknesses of our approach. All of these proofs require refinement reflection, i.e., are beyond the scope of shallow refinement typing.

Proof Strategies. Our proofs use three building blocks, that are seamlessly connected via refinement typing:

- **Unfolding** definitions of a function \( f \) at arguments \( e_1 \ldots e_n \), which due to refinement reflection, happens whenever the term \( f \ e_1 \ldots e_n \) appears in a proof. For exposition, we render the function whose unfolding is relevant as \( f \);

- **Lemma Application** which is carried out by using the “because” combinator (\( . \)) to instantiate some fact at some inputs;

- **SMT Reasoning** in particular, arithmetic, ordering and congruence closure which kicks in automatically (and predictably!), allowing us to simplify proofs by not having to specify, e.g. which subterms to rewrite.

6.1 Arithmetic Properties

The first category of theorems pertains to the textbook Fibonacci and Ackermann functions. The former were shown in § 2. The latter are summarized in Figure 8, which shows two alternative definitions for the Ackermann function. We proved equivalence of the definition (Prop 1) and various arithmetic relations between them (Prop 2 — 13), by mechanizing the proofs from [31].

Monotonicity Prop 3, shows that \( A_n(x) \) is increasing on \( x \). We derived Prop 4, by applying \( f\text{Mono} \) theorem from § 3 with input function the partially applied Ackermann Function \( A_n(*) \). Similarly, we derived the monotonicity Prop 9, by applying \( f\text{Mono} \) to the locally increasing Prop 8 and \( A_n(*) \). Prop 5, proves that \( A_n(x) \) is increasing on the first argument \( n \). As \( f\text{Mono} \) applies to the last argument of a function, we cannot directly use it to derive Prop 6. Instead, we define a variant \( f\text{Mono2} \) that works on the first argument of a binary function, and use it to derive Prop 6.

Constructive Proofs In [31] Prop 12, was proved by constructing an auxiliary ladder that counts the number of (recursive) invocations of the Ackermann function, and uses this count to bound \( A_n(x) \) and \( A_n(x) \). It turned out to be straightforward and natural to formalize the proof just by defining the ladder function in Haskell, reflecting it, and using it to formalize the algebra from [31].

6.2 Algebraic Data Properties

The second category of properties pertain to algebraic data types.

Fold Universality Next, we proved properties of list folding, such as the following, describing the universal property of right-folds [18]:

\[
f\text{dr\_univ} : f : (a \rightarrow b \rightarrow b) \\
\Rightarrow h : ([a] \rightarrow b) \\
\Rightarrow e : b \\
\Rightarrow y : [a] \\
\Rightarrow \text{base} : (h \ [ ] = e) \\
\Rightarrow \text{stp} : (x : a \rightarrow \text{Id} : [a] \rightarrow h(x:1) = f \ x \ (h \ l))) \\
\Rightarrow (h \ y : = f\text{dr} \ f \ e \ y)
\]
Our proof foldr_univ differs from the one in Agda, in two ways. First, we encode Agda’s universal quantification over x and l in the assumption stp using a function type. Second, unlike Agda, Liquid Haskell does not support implicit arguments, so at uses of foldr_univ the programmer must explicitly provide arguments for base and stp, as illustrated below.

**Fold Fusion** Let us define the usual composition operator:

```
reflect . :: (b → c) → (a → b) → a → c
f . g = \x → f (g x)
```

We can prove the following foldr_fusion theorem (that shows operations can be pushed inside a foldr), by applying foldr_univ to explicit base and stp proofs:

```
foldr_fusion :: h:(b → c) → f:(a → b → b) → g:(a → c → c) → e:b → z:a → x:a → y:b → fuse: {h x y = g x (h y))} → {(h . foldr f e) z = foldr g (h e) z}
```

```
foldr_fusion h f g e ys fuse = foldr_univ g (h . foldr f e) (h e) ys
  (fuse_base h f e)
  (fuse_step h f e g fuse)
```

where `fuse_base` and `fuse_step` prove the base and inductive cases, and for example `fuse_base` is a function with type

```
 fuse_base :: h:(b→c) → f:(a→b→b) → e:b → {(h . foldr f e) []} = h e
```

### 6.3 Typeclass Laws

We used Liquid Haskell to prove the Monoid, Functor, Applicative and Monad Laws, summarized in Figure 9, for various user-defined instances summarized in Figure 7.

**Monoid Laws** A Monoid is a datatype equipped with an associative binary operator \( \diamond \) and an identity element mempty. We use Liquid Haskell to prove that Peano (with add and 2), Maybe (with a suitable `mappend` and `Nothing`), and List (with `append` and `[]`) satisfy the monoid laws. For example, we prove that `++` (§ 3.5) is associative by reifying the textbook proof [12] into a Haskell function, where the induction corresponds to case-splitting and recurring on the first argument:

```
assoc :: xs:[a] → ys:[a] → zs:[a] →
  (xs ++ ys) ++ zs = xs ++ (ys ++ zs)
```

```
assoc [] ys zs = ([] ++ ys) ++ zs
=. [ ] ++ (ys ++ zs) ** QED
assoc (x:xs) ys zs = ((x:xs) ++ ys) ++ zs
=. ((x:xs) ++ ys) ++ zs
=. x:(x:xs) ++ zs
=. x: (xs ++ (ys ++ zs))
:: assoc xs ys zs
=. (x:xs) ++ (ys ++ zs) ** QED
```

**Functor Laws** A type is a functor if it has a function `fmap` that satisfies the *identity* and *distribution* (or fusion) laws in Figure 9. For example, consider the proof of the `fmap` distribution law for the lists, also known as “map-fusion”, which is the basis for important optimizations in GHC [36]. We reflect the definition of `fmap`:

```
reflect map :: (a → b) → [a] → [b]
map f [] = []
map f (x:xs) = f x : map f xs
```

and then specify fusion and verify it by an inductive proof:

```
map_fusion :: f:(b → c) → g:(a → b) → xs:[a] → (map f . g) xs = (map f . map g) xs
```

**Monad Laws** The monad laws, which relate the properties of the two operators `>>=` and `return` (Figure 9), refer to \( \eta \)-functions, thus their proof exercises our support for defunctionalization and \( \eta \) and \( \beta \) equivalence. For example, consider the proof of the associativity law for the list monad. First, we reflect the bind operator:

```
reflect (>>=) :: [a] → (a → [b]) → [b]
(x:xs) >>= f = f x ++ (xs >>= f)
[] >>= f = [ ]
```

Next, we define an abbreviation for the associativity property:

```
type AssocLaw m f g =
{ m >>= f >>= g = m >>= (\x → f x >>= g) }
```

Finally, we can prove that the list-bind is associative:

```
assoc :: m:[a] → f:(a → [b]) → g:(b → [c]) → AssocLaw m f g
assoc [] f g
= [ ] >>= f >>= g
=. [ ] >>= g
=. [ ]
=. [ ] >>= (\x → f x >>= g) ** QED
assoc (x:xs) f g
= (x:xs) >>= f >>= g
=. (f x ++ xs >>= f) >>= g
=. (f x >>= g) ++ (xs >>= f >>= g)
:: bind_append (f x) (xs >>= f) g
=. (f x >>= g) ++ (xs >>= (\y → f y >>= g))
:: assoc xs f g
=. ((\y → f y >>= g) x ++
(xs >>= (\y → f y >>= g))
:: \eq f g x
=. (x:xs) >>= (\y → f y >>= g) ** QED
```

Where the bind-append fusion lemma states that:
Notice that the last step requires β-equivalence on anonymous functions, which we get by explicitly inserting the redex in the logic, via the following lemma with trivial proof:

\[ βeq \colon f \rightarrow g \rightarrow x \rightarrow (bind (f \ x) \ g \ x) = (bind (f \ y) \ g \ y) \]

6.4 Functional Correctness

Finally, we proved correctness of two programs from the literature: a SAT solver and a Unification algorithm.

SAT Solver We implemented and verified the simple SAT solver used to illustrate and evaluate the features of the dependently typed language Zombie [7]. The solver takes as input a formula \( f \) and returns an assignment that satisfies \( f \) if one exists.

\[
\text{solve} :: f \colon \text{Formula} \rightarrow \text{Maybe} \, \{a \colon \text{Asgn} \mid \text{sat} \, a \, f\}
\]

Function assignments \( f \) returns all possible assignments of the formula \( f \) and \( \text{sat} \, a \, f \) returns True iff the assignment \( a \) satisfies the formula \( f \):

\[
\text{reflect} \, \text{sat} :: \text{Asgn} \rightarrow \text{Formula} \rightarrow \text{Bool}
\]

Verification of \( \text{solve} \) follows simply by reflecting \( \text{sat} \) into the refinement logic, and using (bounded) refinements to show that \( \text{find} \) returns only values on which its input predicate yields True [33].

\[
\text{find} :: p \colon (a \rightarrow \text{Bool}) \rightarrow \{a\} \rightarrow \text{Maybe} \, \{a \mid p \ a\}
\]

Unification As another example, we verified the unification of first order terms, as presented in [27]. First, we define a predicate alias for when two terms \( s \) and \( t \) are equal under a substitution \( su \):

\[
\text{eq}_{\text{sub}} \, su \, s \, t = \text{apply} \, su \, s = \text{apply} \, su \, t
\]

Now, we can define a Haskell function \( \text{unify} \) that can diverge, or return Nothing, or return a substitution \( su \) that makes the terms equal:

\[
\text{unify} :: s \colon \text{Term} \rightarrow t \colon \text{Term} \\
\rightarrow \text{Maybe} \, \{su \mid \text{eq}_{\text{sub}} \, su \, s \, t\}
\]

For the specification and verification we only needed to reflect apply and not unify; thus we only had to verify that the former terminates, and not the latter.

As before, we prove correctness by invoking separate helper lemmas. For example to prove the post-condition when unifying a variable \( \text{TVar} \, i \) with a term \( t \) in which \( i \) does not appear, we apply a lemma not-in:

\[
\text{unify} \, (\text{TVar} \, i) \, t2 \mid \text{not} \, (i \in \text{freeVars} \, t2) = \text{Just} \, (\text{const} \, ((i, t2)) \, : \, \text{not-in} \, i \, t2)
\]

i.e. if \( i \) is not free in \( t \), the singleton substitution yields \( t \):

\[
\text{not-in} :: i \colon \text{Int} \\
\rightarrow t \colon \text{Term} \mid \text{not} \, (i \in \text{freeVars} \, t) \\
\rightarrow \{\text{eq}_{\text{sub}} \, [(i, t)] \, (\text{TVar} \, i) \, t\}
\]

7. Related Work

SMT-Based Verification SMT-solvers have been extensively used to automate program verification via Floyd-Hoare logics [19]. Our work is inspired by Dafny’s Verified Calculations [17], a framework for proving theorems in Dafny [15], but differs in (1) our use of reflection instead of axiomatization, and (2) our use of refinements to compose proofs. Dafny, and the related F* [30] which like Liquid Haskell, uses types to compose proofs, offer more automation by translating recursive functions to SMT axioms. However, unlike reflectionm this axiomatic approach renders typechecking / verification undecidable (in theory) and leads to unpredictability and divergence (in practice) [16].

Dependent types Our work is inspired by dependent type systems like Coq [6] and Agda [20]. Reflection shows how deep specification and verification in the style of Coq and Agda can be retrofitted into existing languages via refinement typing. Furthermore, we can use SMT to significantly automate reasoning over important theories like arithmetic, equality and functions. It would be interesting to investigate how the tactics and sophisticated proof search of Coq etc. can be adapted to the refinement setting.

Dependent Types for Non-Terminating Programs Zombie [7, 27] integrates dependent types in non terminating programs and supports automatic reasoning for equality. Vazou et al. have previously [32] shown how Liquid Types can be used to check non-terminating programs. Reflection makes Liquid Haskell at least as expressive as Zombie, without having to axiomatize the theory of equality within the type system. Consequently, in contrast to Zombie, SMT based reflection lets Liquid Haskell verify higher-order specifications like foldr_fusion.

Dependent Types in Haskell Integration of dependent types into Haskell has been a long standing goal that dates back to Cayenne [3], a Haskell-like, fully dependent type language with undecidable type checking. In a recent line of work [10] Eisenberg et al. aim to allow fully dependent programming within Haskell, by making “type-level programming ... at least as expressive as term-level programming”. Our approach differs in two significant ways. First, reflection allows SMT-aided verification which drastically simplifies proofs over key theories like linear arithmetic and equality. Second, refinements are completely erased at run-time. That is, while both systems automatically lift Haskell code to either uninterpreted logical functions or type families, with refinements, the logical functions are not accessible at run-time, and promotion cannot affect the semantics of the program. As an advantage (resp. disadvantage) our proofs cannot degrade (resp. optimize) the performance of programs.

Proving Equational Properties Several authors have proposed tools for proving (equational) properties of (functional) programs. Systems [29] and [2] extend classical safety verification algorithms, respectively based on Floyd-Hoare logic and Refinement Types, to the setting of relational or k-safety properties that are assertions over k-traces of a program. Thus, these methods can automatically prove that certain functions are associative, commutative etc., but are restricted to first-order properties and are not programmer-extensible. Zeno [28] generates proofs by term rewriting and Halo [35] uses an axiomatic encoding to verify contracts. Both the above are automatic, but unpredictable and not programmer-extensible, hence, have been limited to far simpler properties than the ones checked here. Hermit [11] proves equivalences by rewriting GHC core guided by user specified scripts. In contrast, our proofs are simply Haskell programs, we can use SMT solvers to automate reasoning, and, most importantly, we can connect the validity of proofs with the semantics of the programs.
8. Conclusions & Future Directions

We have shown how refinement reflection – namely reflecting the definitions of functions in their output refinements – can be used to convert a language into a proof assistant, while ensuring (refinement) type checking stays decidable and predictable via careful design of the logic and proof combinators.

Our evaluation shows that refinement reflection lets us prove deep specifications of a variety of implementations, and identifies important avenues for research. First, while proofs are possible deep specifications of a variety of implementations, and identifies definitions of functions in their output refinements – can be used to convert a language into a proof assistant, while ensuring (refinement) type checking stays decidable and predictable via careful design of the logic and proof combinators.

We have shown how refinement reflection – namely reflecting the complete SMT axiomatization, thereby automating proofs predictably.

References


[34] Panagiotis Vekris, Benjamin Cosman, and Ranjit Jhala. Refinement types for typescript. In PLDI, 2016.

