Pearl: How to do proofs?

Practically proving properties about effectful programs’ results

Koen Jacobs
KU Leuven
Leuven, Belgium
koen.jacobs@cs.kuleuven.be

Andreas Nuyts
KU Leuven
Leuven, Belgium
andreas.nuyts@cs.kuleuven.be

Dominique Devriese
Vrije Universiteit Brussel
Brussels, Belgium
dominique.devriese@vub.be

Abstract
Dependently-typed languages are great for stating and proving properties of pure functions. We can reason about them modularly (state and prove their properties independently of other functions) and non-intrusively (without modifying their implementation). But what if we are interested in properties about the results of effectful computations? Ideally, we could keep on stating and proving them just as nicely.

This pearl shows we can. We formalise a way to lift a property about values to a property about effectful computations producing such values, and we demonstrate that we need not make any sacrifices when reasoning about them. In addition to this modular and non-intrusive reasoning, our approach offers independence of the underlying monad and allows for readable proofs whose structure follows that of the code.

CCS Concepts • Theory of computation → Type theory: Equational logic and rewriting; • Software and its engineering → Formal software verification.

Keywords Agda, dependently-typed programming, effectful, extrinsic proofs, monad, functor, applicative, strong specification, equational reasoning

ACM Reference Format:

1 Some pseudo-proofs about effects
Imagine that we are developing a Monopoly game where players frequently throw a pair of dice. A single die roll is at most six, and the game rules sometimes rely on the fact that a pair of dice can never be greater than twelve.

In a dependently-typed language, we can prove such facts. That is, if natural numbers \( x \) and \( y \) are not greater than 6, we can prove that \( x + y \) is not greater than 12. To do this,

we define a function, say \( \text{sumOfBound6IsBound12} \), of type \( \{ x : \mathbb{N} \} \rightarrow x \leq 6 \rightarrow \{ y : \mathbb{N} \} \rightarrow y \leq 6 \rightarrow x + y \leq 12 \), which takes proofs that \( x \leq 6 \) and \( y \leq 6 \), and returns a proof that \( x + y \leq 12 \).

However, in our Monopoly implementation, we are not interested in this property for individual rolls, but as a property over the results of the effectful operation \( \text{twoDice} \), which is implemented in terms of an underlying operation \( \text{die} \):

\[
\text{die} : \text{IO} \ \mathbb{N} \\
\text{die} = \ldots \\
\text{twoDice} : \text{IO} \ \mathbb{N} \\
\text{twoDice} = \text{do} \ x \leftarrow \text{die} \\
\quad y \leftarrow \text{die} \\
\quad \text{return} (x + y)
\]

That is, we are interested in proving that \( \text{twoDice} \) returns, upon execution, a natural number not greater than 12.

An intrusive solution We can of course reimplement \( \text{die} \) and make it return not just a natural number \( n \) but also a proof that \( n \) is bounded by 6. Likewise, we can reimplement \( \text{twoDice} \) – with the help of the \( \text{sumOfBound6IsBound12} \) function – so that it returns a natural number \( n \) and a proof that \( n \) is bounded by 12:

\[
\text{die} : \text{IO} (\Sigma [ n \in \mathbb{N} ] n \leq 6) \\
\text{die} = \ldots \\
\text{twoDice} : \text{IO} (\Sigma [ n \in \mathbb{N} ] n \leq 12) \\
\text{twoDice} = \text{do} (x : \mathbb{N}, px : \text{sumOfBound6IsBound12}) \leftarrow \text{die} \\
\quad (y : \mathbb{N}, py : \text{sumOfBound6IsBound12}) \leftarrow \text{die} \\
\quad \text{return} (x + y)
\]

1The type constructor \( \preceq \) maps natural numbers \( a \) and \( b \) to the type \( a \preceq b \) representing the proposition that \( a \) is at most \( b \). Following the Curry-Howard correspondence [12], the type \( a \preceq b \) is inhabited if this proposition is true, and its inhabitants represent proofs of the proposition.

2All code samples that appear here, are written in the dependently-typed functional programming language Agda [11]. The Agda files can be found at https://github.com/scala/scala-liftprop

3That is, upon execution, \( \text{die} \) will return a pair in which the first component is a natural number, and the second component a proof that the first component is not greater than 6. More concisely, it will return a pair of the form \( (n, \rho) \) where \( n : \mathbb{N} \) and \( \rho : n \preceq 6 \). Such pairs are exactly the inhabitants of the type \( \Sigma [ n \in \mathbb{N} ] n \leq 6 \).

4To aid the reader, we sometimes annotate functions and variables with their type \( \text{\#\#} \). These superscripts are not part of the code.
return \((x + y) \mod 12\)

, \((\mathrm{sumOfBounds} \circ \mathrm{listBound} 12 \, px \, py \, (x + y))\)

This approach is referred to as strong specification [13]; the type \(\mathrm{IO} (\Sigma \ n \in \mathbb{N} \mid n \leq 12)\) of this reimplemented \(\text{twoDice}\) captures the desired property about the function’s result by making it return a proof along with the result. The function itself needs to be modified to return this proof and so the proof of the property is baked into the new implementation.

However, modifying the original code to use strong specification is not always desirable. For one, the code becomes more verbose, unnecessarily so for readers who do not care about the property. Also, we run the risk of introducing new bugs, simply because we have to modify the original code to return the extra proof. Furthermore, proving several properties about a single function is only possible by including them all in the original definition.

Because of these downsides, we would prefer to avoid reimplementing \(\text{die}\) and \(\text{twoDice}\). Instead, we would like to leave their original versions of type \(\mathrm{IO} \n \) untouched and prove their properties extrinsically, in a separate definition. Let us imagine what such a solution could look like.

### Dreaming up a better solution

Of course, we cannot simply write \(\text{twoDice} \leq 12\) as \(\lambda \ a \rightarrow a \leq 12\) is a predicate\(^5\) on \(\mathbb{N}\), not \(\mathrm{IO} \n\). This suggests that what we need is an operator, say \(\text{Lift}\), which takes a predicate on \(\mathbb{N}\), say \(\lambda \ a \rightarrow a \leq 12\), and returns the desired, lifted predicate on \(\mathrm{IO} \n\). That is, for an \(\text{ioa} : \mathrm{IO} \ A\), the type \(\text{Lift} \ \text{ioa}\) encodes the proposition that \(\text{ioa}\) returns upon execution – an \(a : A\) that satisfies \(P\).

But even if we had such a Lift operator, how would we prove such a proposition? More concretely, given an inhabitant \(\text{dieBound}\) of type \(\text{Lift} \ (\lambda \ a \rightarrow a \leq 6) \ \text{die}\), how can we prove \(\text{Lift} \ (\lambda \ a \rightarrow a \leq 12) \ \text{twoDice}\)? One way to think about this is that intuitively, \(\text{Lift} \ (\lambda \ a \rightarrow a \leq 6) \ \text{die}\) is true because \(\text{die}\) could be reimplemented as a computation of type \(\mathrm{IO} (\Sigma \ n \in \mathbb{N} \mid n \leq 6)\). Analogously, \(\text{Lift} \ (\lambda \ a \rightarrow a \leq 12) \ \text{twoDice}\) is true intuitively because \(\text{twoDice}\) could be reimplemented at type \(\mathrm{IO} (\Sigma \ n \in \mathbb{N} \mid n \leq 12)\). Perhaps, even though Lift is obviously not a monad, it would be nice if we could write a proof of \(\text{Lift} \ (\lambda \ a \rightarrow a \leq 12) \ \text{twoDice}\) in a form of do-notation, where we essentially replicate this hypothetical reimplementation, only now in terms of \(\text{dieBound}\).

\(\text{dieBound}\) : \(\text{Lift} \ (\lambda \ a \rightarrow a \leq 6) \ \text{die}\)

\(\text{dieBound} \ = \ldots\)

\(\text{twoDiceBound} \ = \ \text{Lift} \ (\lambda \ a \rightarrow a \leq 12) \ \text{twoDice}\)

\(^3\)Completely analogous to the pure case, we defined \(\text{sumOfBounds} \circ \text{listBound} 12\) extrinsically instead some intrinsic specification of addition, which would have the type \(\Sigma \ n \in \mathbb{N} \mid n \leq 6 \to \Sigma \ n \in \mathbb{N} \mid n \leq 6 \to \Sigma \ n \in \mathbb{N} \mid n \leq 12\).

\(^4\)A predicate, say \(P\), on a type \(A\) is a function of type \(A \rightarrow \text{Set}\). That is, for each inhabitant of \(A\), it returns a type \(P\) \(a\). For example, the predicate \(\lambda \ a \rightarrow a \leq 12\) on \(\mathbb{N}\) takes a natural number \(n\), and maps it to the proposition \(n \leq 12\).

\(\text{twoDiceBound} 12 \ = \)

\(\begin{array}{c}
\text{do} \ (x, px) \leftarrow \text{dieBound} \ (\lambda \ a \rightarrow a \leq 6) \ \text{die} \\
\quad \ (y, py) \leftarrow \text{dieBound} \\
\quad \text{return} \ (x + y, \text{sumOfBounds} \circ \text{listBound} 12 \, px \, py)
\end{array}\)

Ideally, the proof \(\text{twoDiceBound} 12\) should not depend on the precise implementation of \(\text{die}\), nor on that of \(\text{dieBound}\). For example, we should also be able to write the following:

\(\text{twoTimes} : \mathrm{IO} \ \mathbb{N} \to \mathrm{IO} \ \mathbb{N}\)

\(\text{twoTimes} \ \text{die} \ = \ \text{do} \ x \leftarrow \text{die} \\
\quad \ y \leftarrow \text{die} \\
\quad \text{return} \ (x + y)\)

\(\text{dieBound} 6 \circ \text{twoTimesBound} 12\) :

\(\begin{array}{c}
\text{(die} : \mathrm{IO} \ \mathbb{N}) \to \text{Lift} \ (\lambda \ a \to a \leq 6) \ \text{die} \to \\
\quad \text{Lift} \ (\lambda \ a \to a \leq 12) \ (\text{twoTimes} \ \text{die}) \\
\text{dieBound} 6 \circ \text{twoTimesBound} 12 \ \text{die} \ \text{dieBound} 6 \ = \\
\quad \text{do} \ (x, px) \leftarrow \text{dieBound} \\
\quad \ (y, py) \leftarrow \text{dieBound} \\
\quad \text{return} \ (x + y, \text{sumOfBounds} \circ \text{listBound} 12 \, px \, py)
\end{array}\)

This modularity is important to accommodate situations where \(\text{die}\) and \(\text{dieBound}\) are implemented independently and abstractly by another party, in some other module; in such a scenario, changes to the internals of \(\text{die} : \mathrm{IO} \ \mathbb{N}\) or \(\text{dieBound} 6 : \text{Lift} \ (\lambda \ n \to n \leq 6) \ \text{die}\) should not affect the validity of the proof \(\text{twoDiceBound} 12\).

In principle, the above pseudo-proof also does not really depend on the fact that we are in the IO monad. For example, why shouldn’t we be able to use the same approach for computations in the List monad:

\(\text{twoTimesList} : \text{List} \ \mathbb{N} \to \text{List} \ \mathbb{N}\)

\(\text{twoTimesList} \ \text{dieList} \ = \ \text{do} \ x \leftarrow \text{dieList} \\
\quad \ y \leftarrow \text{dieList} \\
\quad \text{return} \ (x + y)\)

\(\text{dieBound} 6 \circ \text{twoTimesListBound} 12\) :

\(\begin{array}{c}
\text{(dieList} : \text{List} \ \mathbb{N}) \to \text{Lift} \ (\lambda \ a \to a \leq 6) \ \text{dieList} \to \\
\quad \text{Lift} \ (\lambda \ a \to a \leq 12) \ (\text{twoTimesList} \ \text{dieList}) \\
\text{dieBound} 6 \circ \text{twoTimesListBound} 12 \ \text{dieList} \ \text{dieListBound} 6 \ = \\
\quad \text{do} \ (x, px) \leftarrow \text{dieListBound} \\
\quad \ (y, py) \leftarrow \text{dieListBound} \\
\quad \text{return} \ (x + y, \text{sumOfBounds} \circ \text{listBound} 12 \, px \, py)
\end{array}\)

Although the meaning of Lift changes for this other monad, the intuitive reasoning does not change, so why should the proofs?

### Overview

It turns out that we can in fact implement the Lift operator sketched above, and in the next section, we explain how. Moreover, we can provide convenient abstractions to work with lifted properties, and we can even allow formal proofs that resemble the above pseudo-code quite closely. In §3, we will demonstrate this framework on some
more elaborate examples. In §4, we broaden our view to applicative and arbitrary functors, zoom in on a particular kind of functors classified by an important property related to Lift, and prove some properties about List functions that we introduced in §3.2. Afterwards, in §5, we will see that our framework provides not only an elegant way to prove lifted properties, but also an interesting way to make use of these properties. Finally, we conclude in §6, where we summarise the advantages and limitations of our approach, and lay out some related and future work.

Remark Although this paper’s subtitle is ‘Practically proving properties about effectful programs results’, we do not claim that our approach supports proving all such properties. Particularly, when a program’s result depends on the behavior of effectful operations, proving properties about this result will require other techniques for reasoning about the behavior of those effects. We encounter such an example in §3.1.

Note also that this paper is specifically about extrinsic or retroactive proofs. In other words, we want to keep proofs like dieBound6twoTimesBound12 separate from the implementation of twoTimes because of the advantages described before: twoTimes does not need to be modified, it remains readable to non-experts and we can easily formulate and prove many separate properties about it. The flip side of the choice for extrinsic proofs is a certain amount of repetition: dieBound6twoTimesBound12 repeats some of the structure of the underlying program twoTimes. However, this code duplication is not the same as that which is widely discouraged in software engineering courses, as there is no risk for inconsistencies between twoTimes and dieBound6twoTimesBound12. Any such inconsistency will be reliably detected and reported by the type-checker.

2 How does it work?

In this section, we formalise the notations from §1: the meaning of Lift (§2.1) and of the corresponding do-notation (§2.2).

2.1 Lifting a predicate

So how can we define this hypothetical Lift operator? Consider, for example, a list of natural numbers dieList = [1, 2, 3, 4, 5, 6]. How can we encode the fact that every element in dieList is not greater than 6? Notice, again, that dieList could just as well have been implemented to be of type List (Σ [n ∈ N] n ≤ 6).2

\[
\text{dieListWithProofs : List (Σ [n ∈ N] n ≤ 6)}
\]

\[
\text{dieListWithProofs} =
\]

3When the implementation of a term of a specific type is irrelevant and distracting, we give it a generic name together with its type in superscript like \([\text{List}]\).

4For clarity, we use a Haskell inspired pseudo syntax to denote lists.

\[
\begin{align*}
(1, p16 & \leq 1), (2, p26 \leq 2), (3, p36 \leq 3), (4, p46 \leq 4), (5, p56 \leq 5), (6, p66 \leq 6)
\end{align*}
\]

This dieListWithProofs : List (Σ [n ∈ N] n ≤ 6) corresponds to dieList in the sense that executing dieListWithProofs and then forgetting the returned proofs, is equivalent to the original dieList. More formally, we can show that fmap proj1 dieListWithProofs (i.e. executing dieListWithProofs and using proj1 : Σ [n ∈ N] n ≤ 6 → N to forget the proof) is equal to the original dieList.9

\[
\text{dieListWithProofsCorr : fmap proj1 dieListWithProofs ≡ dieList dieListWithProofsCorr = refl}
\]

We can prove this equality using refl because fmap proj1 dieListWithProofs simply reduces to dieList. Intuitively, we can think of dieListWithProofs as a witness to the fact that every result of dieList is indeed at most 6.

Generalising this example, we can define the proposition Lift P fa as follows, for an arbitrary functor, say F, a type A, a predicate P on A, and a functorial value fa : F A:

\[
\text{record Lift (P : Predicate A) (fa : F A) : Set where}
\]

\[
\text{field witness : F (Σ A P)}
\]

\[
\text{corresponds : fa ≡ fmap proj1 witness}
\]

Lift P fa is a record type with two fields: witness of type F (Σ A P) and corresponds: a proof of equality between fa and fmap proj1 witness.

Coming back to our example, we now have the following:

\[
\begin{align*}
\text{dieListBound6} & : \text{Lift (λ a → a ≤ 6)} \text{dieList dieListBound6} = \\
\text{record \{witness} & = \text{dieListWithProofs} \text{corresponds} = \text{dieListWithProofsCorr}\}
\end{align*}
\]

Intuitively, the meaning of Lift is slightly different for different functors. To get a better feel for the full generality of Lift, let us consider some more examples.

For an IO-operation choosePassword : IO String, a proof that Lift (λ s → length s ≥ 20) choosePassword expresses that choosePassword will only produce passwords of length ≥ 20. For a non-deterministic operation range : N → N → List N in the List monad, we can implement \(∀\{n \in \mathbb{N}\} \rightarrow \text{Lift (λ x → (n ≤ x)) (range n m)} \) and \(∀\{n \in \mathbb{N}\} \rightarrow \text{Lift (λ x → (x ≤ m)) (range n m)} \), to formalise that every element in range n m is between n and m. Considering a stateful implementation of Euclid’s algorithm, gcd : N → N → State N N, we could implement Lift (λ d → (Divisible d n)) × (Divisible d m) (gcd n m), encoding the fact that, for arbitrary s : N, we have Divisible (evalState (gcd n m) s) n and Divisible (evalState (gcd n m) s) m.

In general, if we think of a functorial values fa : F A as a container storing values of type A, then Lift P fa encodes...
the proposition that every value inside this container satisfies $P$. If we think of a monadic value $ma : M A$ as the encoding of an effectful computation that gives output in $A$, then Lift $P ma$ encodes the proposition that every output will satisfy $P$.

### 2.2 Binding proofs

But let us consider again the operation $\text{twoDice} : 1O \mathbb{N}$ from the introduction. Now that we can lift properties, let us attempt to prove $\text{twoDiceBound12}$. We can do this by manually implementing the witness and corresponds fields:

$$\text{twoDiceBound12} : \text{Lift} (\lambda a \rightarrow a \leq 12) \text{twoDice}$$

$$\text{twoDiceBound12} = \text{record} \{ \text{witness} = \text{aWitness}; \text{corresponds} = \text{aCorresponds} \}$$

where

$$\text{aWitness} = \text{do} \left( x, px \rightarrow (\text{witness} \ \text{dieBound6}) \right) \quad \left( y, py \rightarrow \text{witness} \ \text{dieBound6} \right) \quad \text{return} \left( x + y, \text{sumOfBound6sBound12} \right)$$

$$\text{aCorresponds} : \text{twoDice} \equiv \text{fmap proj1 witness}$$

$$\text{aCorresponds} = ???$$

While the candidate witness is easy, the corresponds field is a bit tricky. We have a good intuition for why the latter must be so, but formalising this intuition requires no less than 34 lines of code, that we show in appendix A. This manual proof consists of 7 equational reasoning steps, of which 5 tedious correspondences from $lp$ and $f lp$.

And of course we also have $\_ \_L$ as a special case of $\_ \_L$:

$$\_ \_L : \text{Lift} P ma \rightarrow \text{Lift} Q mb \rightarrow \text{Lift} Q (ma \_ \_ mb)$$

$$\text{lPma} \_ \_ \_ \text{lQmb} = \text{lPma} \_ \_ \_ \text{lQmb}$$

Now that we have defined these lifted operators, we can write down a concise proof for Lift $(\lambda a \rightarrow a \leq 12) \text{twoDice}$:

$$\text{twoDiceBound12} : \text{Lift} (\lambda a \rightarrow a \leq 12) \text{twoDice}$$

$$\text{twoDiceBound12} = \text{dieBound6}$$

$$\text{dieBound6} : \text{Lift} (\lambda (a, px) \rightarrow \text{dieBound6}) \_ \_ \_ \text{L} (\lambda (y, py) \rightarrow \text{returnL} (x + y, \text{sumOfBound6sBound12}))$$

The corresponds field is now completely taken care of by our lifted operators! Notice also that the outline of our full proof is identical to that of the witness field in our first attempt; a programmer can just use these lifted operators, and pretend that he/she is doing a retroactive proof by strong specification.

But can’t we make this a bit more readable still? Instead of writing out the $\_ \_L$ operator, can’t we just do it? The do-notation desugars recursively to expressions with $\_ \_L$ and $\_ \_$ as described in [2]. It was developed with the classical monadic $\_ \_L$ and $\_ \_ \_L$ operators in mind to restructure monadic compositions using these operators, making them more readable.

In Agda however, it is fully up to us which $\_ \_L$ and $\_ \_L$ we want to have in scope. By locally renaming $\_ \_L$ to $\_ \_L$, we can reuse the do-notation to structure our proof more easily. We have the following:

**open import Monads hiding (return; \_ \_L; \_ \_L)**

**open import LiftOperators renaming (returnL to return; \_ \_L to \_ \_L; \_ \_L to \_ \_L)**

$$\text{twoDiceBound12} : \text{Lift} (\lambda a \rightarrow a \leq 12) \text{twoDice}$$

$$\text{twoDiceBound12} = \text{dieBound6}$$

$$\text{dieBound6} : \text{Lift} (\lambda (a, px) \rightarrow \text{dieBound6}) \_ \_ \_ \text{L} (\lambda (y, py) \rightarrow \text{returnL} (x + y, \text{sumOfBound6sBound12}))$$

In other words, our pseudo-proofs from the introduction have been valid formal ones all along!

\[^{10}\text{For consistency, we rename our returnL operator to return as well here.}\]
3 Some more elaborate examples
So our framework can tackle the property $\text{Lift} \ (\lambda \ a \to a \leq 12) \ \text{twoDice}$. But does it also work for bigger, more realistic examples? To appreciate its generality, and to see how we could use it in practice, let us have a look at some more elaborate examples.

3.1 Tree relabelling
Our first example is the stateful tree relabelling function from Hutton and Fulger [7]. Consider a straightforward Tree data type:

```haskell
data Tree (A : Set) : Set where
  leaf : (a : A) → Tree A
  node : Tree A → Tree A → Tree A
```

Now consider the relabel function, which walks over the tree and replaces all node values with freshly-generated numbers:

```haskell
relabel : Tree A → State N (Tree N)
relabel (leaf a) = do n ← fresh
                   return (leaf n)
relabel (node l r) = do l' ← relabel l
                        r' ← relabel r
                        return (node l' r')
```

Here, we have defined fresh as follows:

```haskell
fresh : State N N
fresh = do n ← get
          modify suc
          return n
```

The aim of this function is to relabel a tree with unique labels while leaving its shape unchanged. To establish that it fulfils this objective, we prove the following two lifted propositions:

**Isomorphic** $\text{Lift} \ (\lambda \ t' \to t' \equiv t) \ (\text{relabel} \ t)$ That is, given some input tree $t : \text{Tree} A$, any resulting tree should be isomorphic to it, where isomorphism is implemented in the obvious way:

```haskell
data _≡_ : Tree A → Tree B → Set
leafISO : leaf a ≡ leaf b
nodesISO : tal ≡ tbl → tar ≡ tbr → node tal tar ≡ node tbl tbr
```

**No duplicates** $\text{Lift} \ \text{NoDups} \ (\text{relabel} \ t)$ where $\text{NoDups}$ is a predicate on Tree $\mathbb{N}$ such that $\text{NoDups} \ \text{tree}$ encodes the property that $\text{tree} : \text{Tree} \ \mathbb{N}$ contains no duplicate values. That is, any tree resulting from $\text{relabel} \ t$ does not contain duplicates.

Let us consider the isomorphism property. While it is often overlooked in the literature for being too trivial, formalising our intuition for it is not. In appendix B, we showcase an elementary but awkward proof to illustrate this. In our framework, however, it is a breeze:

```haskell
relabel≡ : (t : Tree A) → Lift (λ t' → t ≡ t') (relabel t)
relabel≡ (leaf a) = do (n , _) ← nothing2Prove fresh
                      return (leaf n , leafISO)
relabel≡ (node l r) =
  do (l' , pl≡l'ISO) ← relabel≡ l
     (r' , pr≡r'ISO) ← relabel≡ r
  return (node l' r' , nodesISO pl≡l' pr≡r')
```

The above uses a simple helper function not\_thing\_2\_\_prove of type $(fa : F A) \to \text{Lift} (\lambda a \to T) (fa)$, which proves a trivial predicate for the result of an arbitrary computation $fa : F A$. The predicate $(\lambda a \to T)$ is always satisfied as $T$ is the unit type with single inhabitant $tt$.

Now for the no-duplicates property... Although we can state this property using $\text{Lift}$, we cannot prove it with our lifted bind operators as our induction hypothesis is not strong enough. Indeed, given trees $l' : \text{Tree} \mathbb{N}$ and $r' : \text{Tree} \mathbb{N}$ that satisfy $\text{NoDups}$, it is generally not the case that $\text{node} \ l' \ r'$ satisfies $\text{NoDups}$.

Of course, we could strengthen our hypothesis by also proving that the resulting tree is appropriately bounded with respect to the initial and final state. However, such a strengthened hypothesis cannot be expressed as a lifted property, as it does not merely refer to the computational output, but also to the computation’s effect on the state. Since Lift and our lifted operators are defined over arbitrary functor/monad, this naturally falls outside the scope of our approach. In §6, we briefly come back to this problem statement, and discuss how we can solve it by explicitly supporting the State monad.

3.2 n-Queens
A second larger example that we look at is a simple solver for the $n$-queens problem. Given a natural number $n : \mathbb{N}$, the problem is to find all configurations of $n$ queens on a chessboard of size $n$ for which no two queens are attacking each other. As in standard chess, two queens attack each other if and only if they are on the same column, row, or diagonal.

We define a List computation $\text{queenConfs}$ of type $\mathbb{N} \to \mathbb{N} \to \text{List QConfig}$. Given a chessboard of size $n : \mathbb{N}$ and an amount of queens $k : \mathbb{N}$, $\text{queenConfs} \ n \ k : \text{List QConfig}$ returns a list of $k$-sized queen configurations. We represent queen configurations as lists of natural numbers, i.e. we write $\text{QConfig}$ for List $\mathbb{N}$. The encoding is depicted in Figure 1: queens are placed in the $k$ leftmost columns and the $i$th number in the list represents the row number for the queen in column $i-1$.

As can be seen in Figure 1, our encoding as List $\mathbb{N}$ is quite loose. That is, many terms of type List $\mathbb{N}$ represent

\[\text{From here on, we leave the renaming of our lifted operators implicit.}\]
These definitions are easily verified by glancing at Figure 2. Notice that the encoding already enforces that no two queens reside in the same column.

To find valid configurations, we can now simply recurse on the amount of queens we place leftmost on the board.

\[
\text{queenConfigs} : \mathbb{N} \to \mathbb{N} \to \text{List QConfig}.
\]

- \text{queenConfigs} n zero = return []
- \text{queenConfigs} n (suc k) =
  \begin{align*}
  \text{do} & \quad qs \leftarrow \text{queenConfigs} n k \quad \text{qs} \leftarrow \text{filter} \left( \lambda q \rightarrow q \text{ areNotAttacking} q \right) \\
  & \quad (\text{range} \text{ from 0 to } (n - 1)) \quad \text{return} \ (qs + [q])
  \end{align*}

Let us now prove that every obtained configuration solves the \(n\)-queens problem, i.e. that it is both fitting and peaceful:

**Fitting** A configuration is fitting if every element in it is actually smaller than \(n\), that is, each queen actually fits on the board. For example, the list \([0, 6, 3, 2]\) from Figure 1 is not fitting as the queen in the second column falls outside the board.

**Peaceful** A configuration is peaceful, if no two queens are in the same column, row or diagonal. For example, the list \([0, 6, 3, 2]\) from Figure 1 is not peaceful as the queens from the third and fourth column are attacking each other.

For a board of size \(n\), the fact that a configuration fits the board is formalised as a predicate \(\text{Fitting}(n)\) on \text{QConfig} which we denote as fitting \(n\). We can then prove that every obtained configuration in \text{queenConfigs} \(n\ k\) List \text{QConfig} fits, that is, we prove \(\text{Fitting}(n)\) (\text{queenConfigs} \(n\ k\)):

\[
\text{queenConfigsFit} : (n : \mathbb{N}) \to (k : \mathbb{N}) \to \text{List QConfig}.
\]

- \(\text{queenConfigsFit} n zero =\) \(\text{emptyConfigFits}[\text{Fitting} \ n]\)
- \(\text{queenConfigsFit} n (\text{suc} \ k) = \text{do} \quad (qs, \text{qsFit} \ n \ k) \leftarrow \text{queenConfigsFit} n k \quad \text{return} \ (qs \text{ of } k)
\]
The preserved property in this scenario is indeed the fact that every element in range 0 \( n - 1 \) is smaller than \( n \), which is encoded by the function \( rangeUpBound \). We finally have to prove Fitting (qs + [q]). Remember now, that we defined Fitting n as Lift (\( \lambda q \rightarrow q \leq n - 1 \)). So to prove Lift (\( \lambda q \rightarrow q \leq n - 1 \)) (qs + [q]), we used the operator \(- \#_L -\) of type Lift P xs \( \rightarrow \) Lift P ys \( \rightarrow \) Lift P (xs + ys) where xs is instantiated by qs and ys by [q], and the \([\_]_L\) operator of type P a \( \rightarrow \) Lift P [a] where a is instantiated by q.

The peacefulness of a configuration is formalised in the following predicate:

**Peaceful : Predicate QConfig**

Peaceful qs =

- NoDups (fmap upwardDiagonal coordinates) \( \times \)
- NoDups (fmap downwardDiagonal coordinates) \( \times \)
- NoDups (fmap row coordinates)

where coordinates = toCoordinates qs

We also implement an **addPeacefully** function of the following type:

\[(q : QConfig) \rightarrow (q : \mathbb{N}) \rightarrow \text{Peaceful } q \rightarrow (q \text{ areNotAttacking } q \equiv \text{true}) \rightarrow \text{Peaceful } (q + [q])\]

Its implementation is unimportant here, so we omit it.

A proof that every obtained configuration in **queenConfigs n k** satisfies Peaceful is now feasible:

**queenConfigsPeaceful : (n : \mathbb{N}) \rightarrow (k : \mathbb{N}) \rightarrow Lift Peaceful (queenConfigs n k)**

**queenConfigsPeaceful n zero =**

return ([], emptyConfigPeaceful[peaceful])

**queenConfigsPeaceful n (suc k) = do**

- (qs, qsP, q = queenConfigsPeaceful n k)
- filterNew (\( \lambda q \rightarrow q \text{ areNotAttacking } q \))

\( \text{return } ((q + [q]), \text{addPeacefully } q \text{ qsp } qsp)\)

Here, we have used the property **filterNew**, defined so that \( \text{filterNew } f \) as proves that \( \text{filter } f \) as satisfies Lift \( \lambda a \rightarrow f a \equiv \text{true} \).

**Gradual proving** Note that we have split up validity of a configuration into two separate predicates Fitting n and Peaceful. This was quite handy, as we could focus on proving weaker properties in isolation of each other. The contrast of our approach to the alternative in absence of Lift is stark; we would have to implement queenConfigs to be of type \( (n : \mathbb{N}) \rightarrow \mathbb{N} \rightarrow \text{List } \text{ValidQConfig} \) where \text{ValidQConfig} already fully specifies a valid configuration. In addition to the disadvantages mentioned before, we would have been forced to implement the specifications of ValidQConfig all at once.

In order for this to work, we have made the implicit assumption that we can easily combine both these properties afterwards to prove the validity of our algorithm:

\[
\text{Valid} : \mathbb{N} \rightarrow \text{Predicate QConfig}
\]

\[
\text{Valid } n \triangleq \text{Fitting } n \land \text{Peaceful}
\]

\[
\text{queenConfigsValid} : (n : \mathbb{N}) \rightarrow (k : \mathbb{N}) \rightarrow
\]

Lift (Valid n) (queenConfigs n k)

**queenConfigsValid n k =**

\[
(\text{queenConfigsFit } n k) \land (\text{queenConfigsPeaceful } n k)
\]

The above uses a predicate conjunction operator \(\land\), where \(\land\) represents the conjunction predicate \(\lambda a \rightarrow P_1 a \land P_2 a\). Interestingly, this \(\land\) is less trivial than one might expect. We come back to this in §4.3.

### 4 Completing the picture

Up until this point, we have only talked about properties of monadic computations\(^{12}\). In this section, we complete our story to cover more ground. In §4.1, we will broaden our point of view by illustrating that our framework fits just as nicely in the context of applicative functors. In §4.2, we generalise further to arbitrary functors. Afterwards, in §4.3, we illustrate the need to zoom in on a particular class of functors for which we can sensibly implement \(\land_\_\land\) as we have seen for List in §3.2. Lastly, in §4.4, we will focus in on the List functor, and some of the List-specific properties that we used in §3.2.

#### 4.1 Simplifying twoDice and Relabel - Applicative Functors

Throughout this pearl, we have confined ourselves to monadic computations. Sadly, this presentation is incomplete as it’s often a good idea to use applicative functors [10] to define effectful computations.

Indeed, **twoDice** and **relabel** can be nicely rephrased in this applicative style.

**twoDice : IO \mathbb{N}**

\[
twoDice = \{(\text{die }\uparrow \text{die})\}
\]

**relabel : Tree A \rightarrow \text{State } \mathbb{N} (\text{Tree } \mathbb{N})**

\[
\text{relabel } (\text{leaf } a) = \{(\text{leaf } \text{fresh})\}
\]

\[
\text{relabel } (\text{node } l r) = \{(\text{node } (\text{relabel } l) (\text{relabel } r))\}
\]

\(^{12}\)That is, computations that are composed using \(\cong\) and return.
Here – in order make code a bit more readable – we have used Agda’s built-in idiomatic bracket notation (proposed by McBride and Paterson [10]). Intuitively, the idiomatic brackets denote function application lifted to effectful computation. Formally, we have [13] that \([ e \ a_1 \ldots a_n \]\) desugars to \(\text{pure } e \otimes a_1 \otimes \ldots \otimes a_n\).

Ideally, we could now prove the lifted properties just as easily:

\[
\text{twoDiceBound12} : \text{Lift } (\lambda \ a \to a \leq 12) \text{twoDice}
\]

\[
\text{twoDiceBound12} = \langle \sum \text{Boundds12 dieBound6 dieBound6} \rangle
\]

\[
\text{relabel} = : (t : \text{Tree } A) \to \text{Lift } (\lambda t' \to t \equiv t') \text{(relabel } t)
\]

\[
\text{relabel} = (\text{leaf } a) = \langle \lambda \ _ \to \text{leafISO} \rangle \text{(nothing2Prove fresh)}
\]

\[
\text{relabel} = (\text{node } l r) = \langle \text{nodesISO } \text{(relabel } l) \text{(relabel } r) \rangle
\]

Luckily we can! To make the above proofs formal, we first lift the operators of the applicative functor class. The lifted operator for \(\text{pure}\) is almost identical to the one return; we have \(\text{pure}_t\) of type \(\forall \{x : X\} \to (p : P x) \to \text{Lift } P \text{ (pure } x)\). More interesting is the \(\otimes\) operator.

The \(\otimes\) operator, is easily explained by analogy with the pure case, as depicted in Figure 3. Consider some function \(f : X \to Y\), an \(x : X\), a predicate \(P\) on \(X\), and a predicate \(Q\) on \(Y\). Now suppose that \(x\) satisfies some predicate \(P\) on \(X\), and suppose that \(f\) satisfies \(P \Rightarrow Q\) where \(\_ \Rightarrow \_\) is defined as follows.

\[
\_ \Rightarrow \_ : \text{Predicate } X \to \text{Predicate } Y \to \text{Predicate } (X \to Y) \quad (P \Rightarrow Q) \ f = \forall \{x : X\} \to P x \Rightarrow Q (f x)
\]

That is, suppose that \(f\) maps inputs satisfying \(P\) to outputs satisfying \(Q\). It is trivial now to prove that the application of \(f\) to \(x\) satisfies \(Q\).

The operator \(\otimes\) gives us the same in the impure context of an applicative functor \(F\). There, we have a particular instance of \(\otimes\) to encode application of an effectful function \(af : F (X \to Y)\) to an effectful argument \(ax : F X\). Analogously now, if \(ax\) satisfies \(Lift \ P\) and \(af\) satisfies \(Lift \ (P \Rightarrow Q)\), we can now use \(\otimes\) to prove that \(af \otimes ax\) satisfies \(Lift \ Q\). This is summarised in Figure 3.

The actual implementation of \(\otimes\) is straightforward but tedious; the witness implementation is as expected and the proof of the \textit{corresponds} field is a long and tedious application of the applicative laws.

With \(\otimes\) and \(\text{pure}\) in scope as \(\_\) and \(\_\) respectively, we can recycle the bracket notation as demonstrated above.\(^{15}\)

---

\(^{15}\)Note that \(\langle \text{genericDie } + \text{genericDie} \rangle\) should be interpreted as \(\langle + \text{genericDie} \text{genericDie}\rangle\) for the purpose of this desugaring.

\(^{14}\)The slight difference being that we let the initial \(x\) be inferred for us automatically.

\(^{13}\)Again, we rely on the fact that the bracket notation – the implementation of it in Agda – is just syntax sugaring that gets desugared before type checking.

4.2 Simplifying relabel - General Functors

Consider again the definition of \(\text{relabel}\). In the first case (\(\text{leaf } a\)), we do not fully use the \(\_\) operator as indeed, we could have used \(\text{fmap}\) instead.

\[
\text{relabel} : \text{Tree } A \to \text{State } \mathbb{N} \text{ (Tree } \mathbb{N})
\]

\[
\text{relabel} = \lambda a \to \text{fmap leaf fresh}
\]

\[
\text{relabel} = (\text{node } l r) = \langle \text{nodesISO } \text{(relabel } l) \text{(relabel } r) \rangle
\]

Luckily, we also have a lifted version of \(\text{fmap}, \text{fmap}_L\) of type \((P \Rightarrow Q) \ f \to \text{Lift } P \ af \to \text{Lift } Q \ (\text{fmap } f \ af)\). So in the context of a functor \(F\); types \(A\) and \(B\); predicates \(P\) on \(A\) and \(Q\) on \(B\); a functorial value \(fa : F A\); and a function \(f : A \to B\), if we can prove \((P \Rightarrow Q) \ f\) and \(\text{Lift } P \ af\), we can conclude \(\text{Lift } Q \ (\text{fmap } f \ af)\). With this in mind, we have the following proof.

\[
\text{relabel} = : (t : \text{Tree } A) \to \text{Lift } (\lambda t' \to t \equiv t') \text{(relabel } t)
\]

\[
\text{relabel} = (\text{leaf } a) = \langle \\text{fmap}_L (\lambda \ _ \to \text{leafISO}) \text{(nothing2Prove fresh)} \rangle
\]

\[
\text{relabel} = (\text{node } l r) = \langle \text{nodesISO } \text{(relabel } l) \text{(relabel } r) \rangle
\]

4.3 Combining properties - Pullback preserving functors

Consider again the strategy that we used in §3.2. In order to prove that every obtained configuration in \(\text{queensConfigs}\) was valid, we separately proved them to be both Fitting and Peaceful. Remember how we have then used the operator \(\otimes\) to combine these two into a proof of the combined property \(\text{Valid } n = \text{Fitting } n \land \text{Peaceful}\):

\[
\text{Valid} : \mathbb{N} \to \text{QConfig } \to \text{Set}
\]

\[
\text{Valid } n = \text{Fitting } n \land \text{Peaceful}
\]

\[
\text{queenConfigsValid} = : (n : \mathbb{N}) \to (k : \mathbb{N}) \to \text{Lift } (\text{Valid } n) \text{ (queenConfigs } n \ k)
\]

\[
\text{queenConfigsValid } n \ k = \langle \text{queenConfigsFitting } n \ k \rangle \otimes \text{queenConfigsPeaceful } n \ k
\]

Crucial for this to work is the operator \(\otimes\) : \(\langle fa : F A\rangle \to \text{Lift } P \ fa \to \text{Lift } Q \ fa \to \text{Lift } (P \land Q) \ fa\). Ideally, we would hope that such an operator exists for an \textit{arbitrary} functor \(F\). Sadly however, it is far from obvious how we can implement the general case.

If we restrict ourselves to pullback-preserving functors, we have such a \(\otimes\) operator. Examples of such functors include List, Writer, Maybe, State and all other polynomial functors (also called container functors [1, 5]). Moreover, beside the existence of \(\otimes\), we have that pullback-preserving functors and only those have \(\otimes\) operators that behave universally. Universal behaviour of an operator \(\otimes\) characterises that

\[
\text{uncurry } \otimes : \text{Lift } P \ fa \times \text{Lift } Q \ fa \to \text{Lift } (P \land Q) \ fa
\]

is inverse to the canonical map.
Figure 3. The lifted applicative bind operator \((\odot_L)\) generalises pure function predicate application, just like the applicative bind \((\odot)\) generalises regular function application.

4.4 Proving our low-level properties about List

Up until this section, we have only proven functor-independent lifted properties. In §3.2 however, we have assumed a lot of properties about everyday List functions, whose validity actually relies upon the structure of List itself.

Ideally, the proofs of these assumptions should of course be just as concise and readable. In this section, we show that it is indeed the case.

We begin by assuming three operators that directly correspond to the constructors of the List data type. First of all, note that for the empty list \([\]\), it is trivial to prove \([\] \equiv \text{List P} \) where \(P\) an arbitrary predicate. Moreover, it is easy to implement \(\_\_L : (P a) \to \text{List P a} \times \text{List P a}\). And finally, we also have \(\text{invertP}\)-cons of type \(\text{List P}(x :: xs) \to P x \times (\text{List P} x s)\). However easy they are implemented, their proofs are a bit verbose, and we leave them out here. Given these primitive implementations specific to List, we can easily derive our interesting properties.

Consider a typical implementation of the \(\text{filter}\) function:

\[
\begin{align*}
\text{filter} : \{A : \text{Set}\} & \to \{(A \to \text{Bool}) \to \text{List A} \to \text{List A}\} \\
\text{filter f} [\] & = [\] \\
\text{filter f} (x :: xs) \text{ with } f x & = ? \text{ true} \\
\text{filter f} (x :: xs) & | \text{ yes } = x :: \text{filter f xs} \\
\text{filter f} (x :: xs) & | \text{ no } = \text{ filter f xs}
\end{align*}
\]

With the \([\_]_L\) and \(\_\_L\) operators, it is easy to prove, for instance, that every element in the resulting filtered list satisfies the filtered predicate:

\[
\begin{align*}
\text{filterNew} : (f : A \to \text{Bool}) & \to \{(as : \text{List} A) \to \text{lift} (\lambda a \to f a \equiv \text{true}) \to \text{filter f as}\} \\
\text{filterNew f} [\_L] & = [\_L] \\
\text{filterNew f} (x :: as) \text{ with } f x & = ? \text{ true} \\
\text{filterNew f} (x :: as) & | \text{ yes } p = p :: L \text{filterNew f as} \\
\text{filterNew f} (x :: as) & | \text{ no } u p = \text{filterNew f as}
\end{align*}
\]

Now consider a typical \(\text{range}\) function as defined below.

\[
\begin{align*}
\text{range} : \mathbb{N} & \to \mathbb{N} \to \text{List} \mathbb{N} \\
\text{range zero} & = [0] \\
\text{range succ n} & = [\_]_L \\
\text{range succ m} & = \text{range zero m} + [\text{suc m}] \\
\text{range succ n} (\text{suc m}) & = \text{fmap suc (range n m)}
\end{align*}
\]

Proving that the resulting list is bounded below by the first argument is just as easy.\(^\text{16}\)

\[
\begin{align*}
\text{rangeDownBound} : (d : \mathbb{N}) & \to (u : \mathbb{N}) \to \text{lift} (\lambda x \to d \leq x) \to (\text{range d u}) \\
\text{rangeDownBound zero} & = [\_L_0] \\
\text{rangeDownBound zero} & = [\_]_L \\
\text{rangeDownBound succ m} & = \text{range zero m} + \text{succ m} \\
\text{rangeDownBound} (\text{suc m}) & = \text{fmap succ (range n m)}
\end{align*}
\]

The above uses a lemma for combining a lifted property when appending lists:

\[
\begin{align*}
\_\_L_0 : & \text{lift} P x s \to \text{lift} P x s \to \text{lift} P x s \\
\_\_L_0 & \equiv \text{filter f as} \\
\_\_L_0 & | \text{succ m as} = \text{filter f as}
\end{align*}
\]

Finally, for Lists, we can also prove the \(\_\_L\) operator discussed earlier:

\[
\begin{align*}
\_\_L : & \text{lift} P a \to \text{lift} P Q a \to \text{lift} (P \land Q) a \\
\_\_L & \equiv \text{filter f as} \\
\_\_L & | \text{succ m as} = \text{xconsP asP}\_L
\end{align*}
\]

\(^\text{16}\)Here, we have the singleton operator of type \(P a \to \text{List P a}\). As \([\_]_L\) is easily implemented by \(\lambda a \to a \equiv [\_]\), we have \([\_]_L\) trivially implemented as \(\lambda a \to a :: [\_]_L\).
The above examples demonstrate how we can use TyDe 2019, August 2019, Berlin, Germany Koen Jacobs, Andreas Nuyts, and Dominique Devriese de/ine a restricted de/ine a restricted of type an arbitrary result, it would be better to rule out the case to something like the following:

\[ \text{lift } P \text{ xs } \rightarrow \text{lift } P (\text{xs } + \text{ ys}) \]

Unfortunately, such a rephrasing would require a generalisation of Agda’s pattern matching along the lines of Epigram’s induction by syntax [9].

5 Feeding proofs to programs

The above examples demonstrate how we can use Lift to prove lifted properties about existing programs. But what if we want to rely on such lifted properties when implementing other programs?

Imagine, for example, that we want to spic up our monopoly implementation with a new chance card. The card says the player is fined for speeding, that is, he/she has to pay an amount of \(1000 \div (13 - n)\), where \(n\) is the number of pips he/she throws. A naive implementation might look like this:

\[
\text{fine : IO } \mathbb{N} \\
\text{fine } = \text{fmap amount twoDice where} \\
\text{amount } : \mathbb{N} \rightarrow \mathbb{N} \\
\text{amount } n = \text{case } (n \leq? 12) \text{ of} \\
\quad \lambda \{(\text{yes } p : : \mathbb{N}) \rightarrow (1000 \div (13 - n, \text{ easy } [13 - n \neq 0])\}; \\
\quad (\text{no } p : : \mathbb{N}) \rightarrow ???\} \\
\text{where} \\
\quad \text{div} _{-} : \mathbb{N} \rightarrow (\Sigma [n \in \mathbb{N}] n \neq 0) \rightarrow \mathbb{N} \\
\quad n \text{ div } (d, p) = \ldots \\
\]

Here, we have defined an amount function from \(\mathbb{N}\) to \(\mathbb{N}\), taking the outcome of a throw and mapping it to a fine. To avoid a division by zero, we do a case split to decide whether the roll is greater than 12 or not. However, the case that the roll is greater than 12 is spurious. Rather than returning an arbitrary result, it would be better to rule out the case explicitly. This will also prevent us from forgetting about this assumption in the future.\(^{17}\)

So how can we use the proof twoDiceBound12 of type Lift (\(\lambda n \rightarrow n \leq 12\)) twoDice to rule out the spurious case above. Given this proof, it should in fact suffice to define amount of type \(\Sigma [n \in \mathbb{N}] n \leq 12 \rightarrow \mathbb{N}\). To do this, we define a restricted fmap operator, fmap\(_{R}\), formalising the intuition that, when applying fmap with a function \(f : A \rightarrow B\) and a value \(a : A\) for which we have a proof of \(P f a\), we can always assume that when defining \(a, a\) satisfies \(P\). That is, it is enough to define \(f\) as a function of type \(\Sigma A P \rightarrow B\):

\[
\text{fmap}_R : \{f : F A \rightarrow (\Sigma A P \rightarrow B) \rightarrow (\text{Lift } P \text{ fa}) \rightarrow F B\} \\
fmap_\text{R } f R = \text{fmap } f \text{R (witness lp)} \\
\]

Using fmap\(_R\), we now have the following:

\[
\text{fine } = \text{fmap}_R \text{amount}_R \text{twoDiceBounded12 where} \\
\text{amount}_R : \Sigma [n \in \mathbb{N}] n \leq 12 \rightarrow \mathbb{N} \\
\text{amount}_R (n, p) = 1000 \div (13 - n, \text{ easy } [13 - n \neq 0]) \\
\]

It is in fact easy to prove that this new implementation of fine is equal to the old one. Intuitively, this is because for \(d : \mathbb{N}\) and \(p : n \leq 12\), we have that amount \(d\) is equal to amount\(_R\) \((d, p)\). In general, it is easily proven formally that \(\text{fmap } f \text{R } f R = \text{fmap } f \text{R } f R\) if \(f\) agrees with \(f R\) on \(P\).\(^{18}\)

We have an analogous operator for \(_\text{R}_-\).

\[
\text{ax} : F X \rightarrow F (\Sigma X P \rightarrow Y) \rightarrow \text{Lift } P \text{ ax } \rightarrow \text{Lift } Y \\
f R = \text{axP } f R = \text{witness } axP \\
\]

So given an applicative value \(\text{ax} : F X\) for which we have a proof \(\text{axP}\) of Lift \(P\) \(\text{ax}\), it is enough to have \(f R\) of type \((\Sigma X P \rightarrow Y)\) instead of \((\text{F } X \rightarrow Y)\).

And finally, the analogous operator for \(_\text{R}_\rightarrow\).

\[
\text{ma } : M A \rightarrow \text{Lift } P \text{ ma } \rightarrow \text{Lift } M B \\
lp = \text{witness lp } f R \\
\]

That is, given a monadic value \(\text{ma} : M A\) and a proof of Lift \(\text{ma}\), when binding \(\text{ma}\) with a function \(f : A \rightarrow M B\), it is enough to define \(f\) given that a satisfies \(P\). That is, it is enough to define \(f\) of type \(\Sigma A P \rightarrow M B\).

6 Conclusion

In summary, this paper shows a nice way to express and prove lif/ing properties of effectful code. In general, we can express any property related to the results of an effectful com/utation, and prove it with our lif/ed operators provided that it holds independently of the specific function/applicative/monad in use.

The properties can be formulated extrinsically (no need to modify the original code). The proofs are readable and easy to understand, and can be composed modularly. No language modifications are needed and in fact, the core of our framework is very small; it consists only of Lift, \(_\text{R}_-\), return\(_L\), pure\(_L\), \(_\text{R}_-\) \(_\text{L}_-\), and fmap\(_L\).

Moreover, we can easily reuse existing notation to structure compositions with \(_\text{R}_-\) \(_\text{do}-\)notation, and \(_\text{R}_-\) together with \text{pure\(_L\)} (idiom brackets) due to the flexible nature\(^{18}\).

\(^{17}\)Imagine, for example, that we introduce a new rule that you can roll the dice again if you roll doubles the first time (same number on each die).

\(^{18}\)That is, if for all \((a, p) : \Sigma A P\) we have that \(f a\) equals \(f R (a, p)\).
of their implementation in Agda. That is, both do-notation and idiom brackets are desugared before type checking, and so, we can easily experiment with operators whose types do not adhere to the prior intent of the syntax. Furthermore, the examples in this pearl provide a clear case for the virtues of said flexibility.

As we have explained, our approach is limited to properties that can be phrased in terms of the results of effectful operations. Moreover – confining ourselves to the lifted operators – we can only prove properties independent of the specific functor in use. We expect that supporting more expressive properties is possible however, by focusing in on a specific (class of) underlying monads/functors. We already demonstrated the feasibility of this for the List functor; by merely implementing some basic primitive properties corresponding to the data constructors, we were able to obtain nice and intuitive proofs about your everyday List functions. More elaborately, we show in the git repository how one can take Swierstra’s Hoare State monad for writing intersections of lifted properties (over State) that are quantified over the initial and final state variable and prove the no-duplicates property extrinsically. In the future, it could be interesting to extend the approach to more specific properties. The idea would be to use strongly-specified witnesses that testify for these more expressive properties and require an appropriate correspondence to the underlying code.

Of course, not all properties regarding effectful computations concern themselves merely with the results of that computation; think interestingOperation : IO ⊤ for example. In such cases, the programmer should use a different approach, like equational reasoning [6, 7].

### 6.1 Related work

**Equational reasoning** The tree relabelling problem is often used in literature to showcase the use of equational reasoning to prove general properties about effectful computations [7]. So too is the n-queens problem [6]. We note however that the general objective in this setting is quite different from what we do here; one proves a desired property about a given effectful computation by arguing that it is contextually equivalent to a more naive computation, clearly satisfying said property. This is done by chaining together a link of equalities; hence the name ‘equational reasoning’. A narrow version of said practice can be found in the framework presented in this paper though. We prove that computations satisfy specifications with regard to their result, and we do this by implementing a strongly specified version. Arguing that forgetting about this specification gives us back the original computation, is now done completely under the hood, formally encapsulated in our lifted operators. Moreover, the program that will be run is still the original one, untouched by our extrinsic proofs, so that our technique has no runtime cost (other than the one involved in migrating to a dependently typed functional language).

**Ornaments** A key idea in the development of our framework is the way in which we define Lift; we demand an intrinsic, strongly specified version of our original computation together with a proof that forgetting about this specification, we obtain the original computation.

Of course, the practice of decorating structures is reminiscent of ornaments [8]. However, we believe that the theory of ornaments does not provide an alternative to our techniques, for two reasons. First, the goal of ornaments is different. We are ultimately interested in the ability to express and prove properties of effectful code (such as twoDice) extrinsically, as we did in `twoDiceBound12 : Lift (λ a → a ≤ 12) twoDice ℕ₀`. Ornamentation libraries, on the other hand, are often designed to combine an extrinsic proof like `twoDiceBound12` with the underlying implementation `twoDice` into an intrinsically correct implementation.

Secondly, the results in the ornament literature simply do not seem to be applicable in our setting. Our Lift operator is designed to reason about forgetful maps of the form `proj₁ : Σ A P → A`. We like to point out that, since it is possible in dependent type theory to define the inverse image of a function, any function `f : B → A` factors as `B ≅ Σ(x : A) g⁻¹(x) → A`. Thus, we essentially consider all functions. Ornaments, on the other hand, consider only a restricted class of functions which can be seen as forgetting ornaments\(^\dagger\). Alternatively, one might try to apply the theory of ornaments not to the result type but to the monad at hand, but then we would obtain results regarding effect specifications ignoring the result of a computation, which sounds interesting but is quite the opposite of the current paper’s subject.

### Acknowledgments

This work was funded in part by Internal Funds KU Leuven grant C14/18/064.

Andreas Nuyts holds a Ph.D. Fellowship from the Research Foundation - Flanders (FWO).

### References


\(^\dagger\)Dagand [4] characterizes them as functions between indexed inductive types (viewed as indexed W-types) that arise from cartesian natural transformations between their generating indexed polynomial functors.
A Manual Proof

cumbersomeProof : twoDice ≡ fmap proj1 aWitness

cumbersomeProof =
begin
  do x ← die
   y ← die
   return (x + y))
≡ ⟨ cong (flip _⇒ _) (corresponds dieBound6) ⟩
  (do x ← fmap proj1 (witness dieBound6)
   y ← die
   return (x + y))
≡ ⟨ fmap-bind _⇒ _ ⟩
  (do (x , px) ← witness dieBound6
   y ← px
   return (x + y))
≡ ⟨ cong (λ (x , px) → witness dieBound6) ⟩
  (funext λ _ → cong (flip _⇒ _)
   (corresponds dieBound6))
  (do (x , px) ← witness dieBound6
   y ← px
   return (x + y))
≡ ⟨ cong (λ (x , px) → witness dieBound6) ⟩
  (funext λ _ → fmap-bind _⇒ _)
  (do (x , px) ← witness dieBound6
   y ← px
   return (x + y))
≡ ⟨ cong (λ (x , px) → witness dieBound6) ⟩
  (funext λ a → cong (λ (x , px) →
   (funext λ _ → sym (fmap-return proj1 _))))
  (do (x , px) ← witness dieBound6
   (y , py) ← witness dieBound6
   fmap (proj1 (B = λ n → n ≤ 12))
   (return (x + y , sumOfBoundsIsBound12 px py)))
≡ ⟨ cong (λ (x , px) → witness dieBound6) ⟩
  (funext λ a → cong (λ (x , px) →
   (funext λ _ → sym (fmap-return proj1 _))))
  (do (x , px) ← witness dieBound6
   (y , py) ← witness dieBound6
   fmap (proj1 (B = λ n → n ≤ 12)))

d (y , py) ← witness dieBound6
  return (x + y , sumOfBoundsIsBound12 px py))
≡ ( sym (fmap-move-bind _⇒ _ _))
  fmap proj1 (do (x , px) ← witness dieBound6
  (y , py) ← witness dieBound6
  return (x + y , sumOfBoundsIsBound12 px py)) ■

Here, we have used the following helper functions.

\[
\text{fmap-bind} \ g \ f \ mx : (fmap \ f \ mx) \gg (g \gg mx) = (g \circ f)
\]

\[
\text{fmap-return} \ a : \Sigma (f \ a = a) \gg \Sigma (f) = (f \ a)
\]

\[
\text{fmap-move-bind} \ f \ ma \ g : (fmap \ g \ ma) \gg (ma \gg (f \circ g))
\]

B Manual proof relabel

\[
\begin{align*}
\text{relabel} &: (t : \text{Tree} \ A) \rightarrow (n : \text{Node} \ A) \rightarrow \text{evalState} (\text{relabel} \ t) \equiv t
\end{align*}
\]

\[
\begin{align*}
\text{relabel} \ (\text{leaf} \ a) &= \text{leafISO} \\
\text{relabel} \ (\text{node} \ l \ r) &= \text{nodesISO} (\text{relabel} \ l \ n) \rightarrow \text{relabel} \ r \text{ (execState (relabel) \ l \ n)}
\end{align*}
\]

However small, the above proof is quite awkward as it needs to take into account the particular details of State binding that are totally void in our intuitive understanding of the property.

C On Pullback Preservation

In this appendix, we show that a well-behaved operator \( \sim \) exists for a given functor \( F \) if and only if \( F \) preserves pullbacks.

Moreover, we show that the continuation monad \( M X = (X \rightarrow R) \rightarrow R \) does not preserve pullbacks.\(^{20}\)

C.1 Definitions

Because this paper is not about formalizing category theory in type theory, we use the following down-to-earth definition of a pullback:

**Definition C.1.** (propositionally) commutative diagram

\[
\begin{array}{ccc}
T & \xrightarrow{p_1} & A \\
\downarrow f & & \downarrow \ \\
B & \xrightarrow{g} & C
\end{array}
\]

is called a pullback square (and \( T \) is called the pullback of \( A \rightarrow C \rightarrow B \)) if \( T \) is isomorphic to the type

\[
\Sigma \{ a \in A \} \Sigma \{ b \in B \} \Sigma \{ c \in C \} (f \ a = c) \times (g \ b = c)
\]

with the maps \( p_1 : T \rightarrow A \) and \( p_2 : T \rightarrow B \) corresponding to the appropriate projections from this type of quintuples.\(^{20}\)

\(^{20}\)Throughout the section, we assume uniqueness of identity proofs.
Definition C.2. A functor $F$ preserves pullbacks if it maps any pullback square as in definition C.1 to a new diagram

\[
\begin{array}{c}
F T \xrightarrow{\text{fmap } f} F A \\
\downarrow \text{fmap } p_2 & \downarrow \text{fmap } f \\
F B \xrightarrow{\text{fmap } f} F C
\end{array}
\]

that is also a pullback square.

C.2 Combining properties requires pullback preservation

We seek to prove the following:

Proposition C.3. The function split$_L$ (§4.3) is an isomorphism if and only if $F$ preserves pullbacks.

Proof. If we define $P$ as the inverse image of $f$ and $Q$ as that of $g$, then $A \cong \Sigma \ C \ P$ and $B \cong \Sigma \ C \ Q$. Then $T$ will be the pullback of $f$ and $g$ if and only if $T \cong \Sigma \ C \ (P \land Q)$. If we apply to this diagram the functor $F$ and observe that $F (\Sigma \ X \ R) \cong \Sigma (F (X) (\text{Lift } R))$, then we can write the result up to isomorphism as:

\[
\Sigma (F C) (\text{Lift } (P \land Q)) \xrightarrow{\text{proj}} F C.
\]

Now this diagram is a pullback square if and only if $\Sigma (F C) (\text{Lift } (P \land Q))$ is isomorphic to $\Sigma (F C) (\text{Lift } P \land \text{Lift } Q)$ in a manner compatible with the canonical maps to $\Sigma (F C) (\text{Lift } P)$ and $\Sigma (F C) (\text{Lift } Q)$. In other words, we require that $\text{Lift } (P \land Q) \text{fc}$ be isomorphic to $\text{Lift } P \text{fc} \times \text{Lift } Q \text{fc}$ in a manner compatible with the projections to $\text{Lift } P \text{fc}$ and $\text{Lift } Q \text{fc}$. This compatibility criterion equivalently says that one side of the isomorphism is given by split$_L$. This proves the proposition.

C.3 The continuation monad does not preserve pullbacks

In this section, we consider the functor $M X = (X \rightarrow R) \rightarrow R$, and show via proposition C.3 that it does not preserve pullbacks. In other words, we will show that $\text{Lift } (P \land Q) ma \cong \text{Lift } Q ma$ and $\text{Lift } ma \cong \text{Lift } P ma$ as a warm-up, let us consider what Lift even means for the continuation monad.

A value $ma : M A$ is a computation that pretends to produce an output of type $A$ but in fact grabs the continuation of type $A \rightarrow R$ (a computation containing a hole of type $A$ and producing an overall result of type $R$) and manipulates it to produce some result of type $R$. A pure computation will simply feed a value of type $A$ to the continuation; in general, $ma$ may call the continuation zero or multiple times and combine the results.

If we have a value $ma : M A$ and a function $\mathord{f} : A \rightarrow B$, then $\text{fmap } f ma : M B$ will take a continuation $\mathord{k} : B \rightarrow R$, compose it with $f$ and feed the result to $ma$. A value $ma : M A$ satisfies Lift $P$ if it arises by applying $\text{fmap } \text{proj}_1 : M (\Sigma \ A \ P) \rightarrow M A$ to some computation of type $M (\Sigma \ A \ P)$. In other words, a proof of Lift $P ma$ indicates that, even though $ma$ takes a continuation of type $A \rightarrow R$, it will only invoke this computation on values $a : A$ for which it can prove $P a$.

A remarkable phenomenon arises when $P$ happens to be a proof-relevant predicate: a type family that for some values $a : A$ may contain more than a single element. In this case, Lift $P$ also becomes proof-relevant, but in a blown-up manner. Indeed, $ma : M A$ takes continuations of type $A \rightarrow R$, whereas a computation of type $M (\Sigma \ A \ P)$ takes continuations of type $\Sigma A P \rightarrow R$. The latter type of continuations is much bigger, as it contains continuations that distinguish between proofs of $P a$. Hence, a witness that $ma : M A$ satisfies Lift $P$ needs to respect the behaviour of $ma$ on continuations that ignore the proof of $P a$, but can behave arbitrarily on those that don’t. The result is that the number of witnesses corresponding to a single $ma$ can become enormous.

In fact, we can consider the dullest instance of a proof-relevant predicate and argue with a simple cardinality argument that $M$ cannot preserve pullbacks. We take $A = \top \land \bot$ (the unit type), $R = \text{Bool}$ and $P = Q = \lambda \mathord{x}. \top \rightarrow \text{Bool}$. Then we have $\Sigma (M \top) (\text{Lift } (P \land Q)) \cong M (\Sigma \top (P \land Q)) \cong M (\text{Bool} \times \text{Bool})$ and

\[
\Sigma (M \top) (\text{Lift } P \times \text{Lift } Q)
\]

\[
\cong (\Sigma (M \top) (\text{Lift } P)) \times (\Sigma (M \top) (\text{Lift } Q))
\]

\[
\cong M \text{Bool} \times M \text{Bool}
\]

where $\cong$ denotes an injection. Thus, if $M$ were to preserve pullbacks, then $M (\text{Bool} \times \text{Bool})$ should have lower cardinality than $M \text{Bool} \times M \text{Bool}$. However, the cardinality of the former type is $2^{2^2} \cdot 2^2 = 2^8$, whereas the latter type has cardinality $2^{2^2} \cdot 2^2 = 2^8$ and this is not even a conservative estimate.

\[\text{split}_L\]