

# *Transporting functions across ornaments*

PIERRE-ÉVARISTE DAGAND

*Inria Rocquencourt, Le Chesnay, France*  
(e-mail: pierre-evariste.dagand@inria.fr)

CONOR McBRIDE

*University of Strathclyde, Glasgow, UK*  
(e-mail: conor@cis.strath.ac.uk)

---

## Abstract

Programming with dependent types is a blessing and a curse. It is a blessing to be able to bake invariants into the definition of datatypes: We can finally write correct-by-construction software. However, this extreme accuracy is also a curse: A datatype is the combination of a structuring medium together with a special purpose logic. These domain-specific logics hamper any attempt to reuse code across similarly structured data. In this paper, we capitalise on the structural invariants of datatypes. To do so, we first adapt the notion of ornament to our universe of inductive families. We then show how code reuse can be achieved by ornamenting functions. Using these functional ornaments, we capture the relationship between functions such as the addition of natural numbers and the concatenation of lists. With this knowledge, we demonstrate how the implementation of the former informs the implementation of the latter: The users can ask the definition of addition to be lifted to lists and they will only be asked the details necessary to carry on adding lists rather than numbers. Our presentation is formalised in the type theory with a universe of datatypes and all our constructions have been implemented as generic programs, requiring no extension to the type theory.

---

## 1 Introduction

Imagine designing a library for a language of the ML family. For instance, we start with natural numbers and their operations, then we move to binary trees, then rose trees, *etc.* It is the garden of Eden: datatypes are *data-structures*, each coming with its unique and optimised set of operations. If we move to a language with richer datatypes, such as a dependently typed language, we enter the Augean stables. Where we used to have binary trees, now we have complete binary trees, red-black trees, AVL trees, and countless other variants. Worse, we have to duplicate code across these tree-like datatypes, because these are defined upon this common binarily branching structure, a lot of computationally identical operations will have to be duplicated for the type checker to be satisfied.

Since their first introduction in ML, datatypes have evolved: besides providing an organising *structure* for computation, these are now offering more *control* over what is a valid result. With richer datatypes, we can enforce invariants on top of the *data-structures*. In such a system, programmers strive to express the correctness of their programs in the types: a well-typed program is correct *by construction*.

A simple yet powerful recipe to obtain richer datatypes is to *index* the data-structure. These datatypes have originally been studied in the type theory under the name of *inductive families* (Dybjer, 1994; Morris *et al.*, 2009). Inductive families made it to mainstream functional programming with Generalised Algebraic Data-Types (GADTs) (Cheney & Hinze, 2003; Schrijvers *et al.*, 2009), a subset of inductive families for which the principal-types property is preserved, thus enabling modular (local) type inference. Refinement types (Freeman & Pfenning, 1991; Swamy *et al.*, 2011) are another technique to equip data-structures with rich invariants. In a dependently typed setting, refinement types are expressible in terms of  $\Sigma$ -types. As such, they offer a clear-cut separation between the data (what is predicated upon, i.e. the first projection of the  $\Sigma$ -type) and the logic (the predicate, i.e. the second projection of the  $\Sigma$ -type). This approach benefits from a straightforward compilation strategy, which simply erases the refining predicates. Atkey *et al.* (2012) have shown how refinement types relate to inductive families.

### 1.1 Ornaments?

However, these carefully crafted datatypes are a threat to any library design: the same data-*structure* is used for logically incompatible purposes. This explosion of specialised datatypes is overwhelming: these objects are too specialised to fit in a global library. Yet, because they share this common structure, many operations on them are extremely similar, if not exactly the same. To address this issue, McBride (to appear) developed *ornaments*, describing how one datatype can be enriched into another *with the same structure*. Such structure-preserving transformations take two forms. First, we can *extend* the initial type with more information.

*Example 1.1 (Ornament: extending the Booleans to the option type)*

We can extend the Booleans to the option type by attaching an  $a : A$  to the constructor `true`:

$$\begin{array}{ccc} \mathbf{data\ Bool\ :SET\ where} & \xrightarrow{\text{Maybe-Orn } A} & \mathbf{data\ Maybe\ [A\ :SET]\ :SET\ where} \\ \text{Bool } \ni \text{ true} & \Rightarrow & \text{Maybe } A \ni \text{ just } (a : A) \\ \quad | \text{ false} & & \quad | \text{ nothing} \end{array}$$

*Example 1.2 (Ornament: extending numbers to lists)*

Or we can extend natural numbers to lists by inserting an  $a : A$  at each successor node:

$$\begin{array}{ccc} \mathbf{data\ Nat\ :SET\ where} & \xrightarrow{\text{List-Orn } A} & \mathbf{data\ List\ [A\ :SET]\ :SET\ where} \\ \text{Nat } \ni 0 & \Rightarrow & \text{List } A \ni \text{ nil} \\ \quad | \text{ suc } (n : \text{Nat}) & & \quad | \text{ cons } (a : A)(as : \text{List } A) \end{array}$$

Second, we can *refine* the indexing of the initial type, following a finer discipline. By refining the indices of a datatype, we make it logically more discriminating.

*Example 1.3 (Ornament: refining numbers to finite sets)*

We refine natural numbers to finite sets by indexing the number with an upper bound:

$$\begin{array}{ccc} \mathbf{data\ Nat} : \mathbf{SET\ where} & \xrightarrow{\text{Fin-Orn}} & \mathbf{data\ Fin} (n : \mathbf{Nat}) : \mathbf{SET\ where} \\ \mathbf{Nat} \ni 0 & & \mathbf{Fin} (n = \mathbf{suc\ } n') \ni \mathbf{f0} (n' : \mathbf{Nat}) \\ \quad | \mathbf{suc} (n : \mathbf{Nat}) & & \quad | \mathbf{fsuc} (n' : \mathbf{Nat})(k : \mathbf{Fin\ } n') \end{array}$$

Put otherwise, the datatype  $\mathbf{Fin\ } n$  is a type of cardinality  $n$ .

We can also do both at the same time, as illustrated by the following example.

*Example 1.4 (Ornament: extending and refining numbers to vectors)*

We extend natural numbers to lists while refining the index to represent the length of the list thus constructed:

$$\begin{array}{ccc} \mathbf{data\ Nat} : \mathbf{SET\ where} & \xrightarrow{\text{VecO } A} & \mathbf{data\ Vec} [A : \mathbf{SET}](n : \mathbf{Nat}) : \mathbf{SET\ where} \\ \mathbf{Nat} \ni 0 & & \mathbf{Vec\ } A \ (n = 0) \ni \mathbf{nil} \\ \quad | \mathbf{suc} (n : \mathbf{Nat}) & & \mathbf{Vec\ } A \ (n = \mathbf{suc\ } n') \ni \mathbf{cons} (n' : \mathbf{Nat})(a : A)(vs : \mathbf{Vec\ } A\ n') \end{array}$$

Note that we declare datatype parameters in brackets – e.g.  $[A : \mathbf{SET}]$  – and datatype indices in parentheses – e.g.  $(n : \mathbf{Nat})$ . We make equational constraints on the latter only when needed, and explicitly – e.g.  $(n = \mathbf{suc\ } n')$ . We come back to the notation for inductive definitions in Section 3.3.

Because of their constructive nature, ornaments are not merely identifying similar structures: They give an effective recipe to build new datatypes from old, guaranteeing by construction that the structure is preserved. Hence, we can obtain a plethora of new datatypes with minimal effort.

## 1.2 Functional ornaments!

While we have a good handle on the transformation of individual datatypes, we are still facing a major reusability issue: a datatype often comes equipped with a set of operations. Ornamenting this datatype, we have to entirely reimplement many similar operations. For example, the datatype  $\mathbf{Nat}$  comes with operations such as addition and subtraction. When defining lists as an ornament of natural numbers, it seems natural to transport the structure-preserving functions of  $\mathbf{Nat}$  to  $\mathbf{List\ } A$ , such as moving from addition of natural numbers to concatenation of lists:

$$\begin{array}{ccc} (m : \mathbf{Nat}) + (n : \mathbf{Nat}) : \mathbf{Nat} & & (xs : \mathbf{List\ } A) ++ (ys : \mathbf{List\ } A) : \mathbf{List\ } A \\ 0 + n \mapsto n & \Rightarrow & \mathbf{nil} ++ ys \mapsto ys \\ (\mathbf{suc\ } m) + n \mapsto \mathbf{suc} (m + n) & & (\mathbf{cons\ } a\ xs) ++ ys \mapsto \mathbf{cons\ } a\ (xs ++ ys) \end{array}$$

or from subtraction of natural numbers to dropping a prefix:

$$\begin{array}{ccc} (m : \mathbf{Nat}) - (n : \mathbf{Nat}) : \mathbf{Nat} & & \mathbf{drop} (xs : \mathbf{List\ } A) (n : \mathbf{Nat}) : \mathbf{List\ } A \\ 0 - n \mapsto 0 & \Rightarrow & \mathbf{drop\ } \mathbf{nil} \ n \mapsto \mathbf{nil} \\ m - 0 \mapsto m & & \mathbf{drop} \ xs \ 0 \mapsto xs \\ (\mathbf{suc\ } m) - (\mathbf{suc\ } n) \mapsto m - n & & \mathbf{drop} (\mathbf{cons\ } a\ xs) (\mathbf{suc\ } n) \mapsto \mathbf{drop\ } xs \ n \end{array}$$

More interestingly, the function we start with may involve several datatypes, each of which may be ornamented differently. In this paper, we develop the notion of *functional ornament* as a generalisation of ornaments to functions:

- We manually transport the comparison of numbers to the list lookup function in Section 2. This example provides the impetus for the rest of this paper: we aim at explaining the structure behind it, generalise, and automate it.
- For this paper to be self-contained, we recall the type theoretic foundations (Chapman *et al.*, 2010) upon which this paper builds in Section 3. We strive to provide an intuition for our universe-based presentation of datatypes, and describe a convenient notation for inductive definitions.
- We adapt ornaments to our universe of datatypes in Section 4. This presentation benefits greatly from our ability to inspect indices when defining datatypes. This allows us to consider ornaments that *delete* information, yielding a key simplification in the construction of algebraic ornament from ornamental algebra.
- We describe how functions can be transported through functional ornaments. We formalise the concept of functional ornament by a universe construction in Section 5. Based on this universe, we establish the connection between a base function (such as addition and subtraction) and its ornamented version (such as, respectively,  $- ++ -$  and  $\text{drop}$ ). Within this framework, we redevelop the example of Section 2 with all the automation offered by our framework.
- In Section 6, we provide further support to drive the computer into lifting functions. As we can see from our examples above, the lifted functions often follow the same recursion pattern and return similar constructors: with a few smart constructors, we shall remove further clutter from our libraries.

This paper is an exercise in constructive mathematics: upon identifying an isomorphism, we shall look at it with our constructive glasses and obtain an effective procedure to cross it. It is crucial to note that this paper is built entirely *within* the type theory. No change or adaptation to the meta-theory is required. In particular, the validity of our constructions is justified by mere type checking.

*Remark 1.5 (Notations)*

We shall write our code in a syntax inspired by the Epigram programming language (McBride & McKinna, 2004). For an optimal experience, we recommend reading the colour version of this paper, available on Dagand's webpage. Colours are used to classify the terms of the type theory. We also make use of the *by* ( $\Leftarrow$ ) and *return* ( $\mapsto$ ) programming gadgets, further extending them to account for the automatic lifting of functions. For brevity, we write pattern-matching definitions when the recursion pattern is evident and unremarkable.

As in ML, unbound variables in type signatures are universally quantified, further abating syntactic noise. For higher-order functions, we indicate the implicit arguments with the quantifier  $\forall x.(\dots)$  – or its annotated variant  $\forall x:T.(\dots)$  – as follows:

example  $(op : \forall n. \text{Vec } A n \rightarrow \mathbb{1}) (xs : \text{Vec } A k) (ys : \text{Vec } A l) : op\ xs = op\ ys$

...

Since we implicitly quantify over unbound type variables, these variables are not explicitly bound in the definition. We rely on the convention that these implicit arguments are automatically in scope of the definition, using the same variable name. For example, in the following definition,  $n$  is universally quantified in the type declaration and is in scope in the definition of `lengthVec`:

$$\begin{array}{l} \text{lengthVec } (vs : \text{Vec } A \ n) \ : \ \text{Nat} \\ \text{lengthVec} \quad \quad \quad vs \quad \quad \quad \mapsto \ n \end{array}$$

The syntax of datatype definitions draws upon the ML tradition as well: its novelty will be presented by way of examples in Section 3. Following mathematical usage, we shall extensively use mixfix operators, i.e. operators in prefix, infix, postfix, or closed form.

All the constructions presented in this paper have been modelled in Agda, using only standard inductive definitions and two levels of universes. Rather than commenting the machine-checked code, we have chosen to use a high-level notation. This notation relies on the reader's ability to cope with ambiguity. We shall therefore indulge in many abuse of language, as is common in mathematics. This allows us to focus on conveying ideas to the reader, rather than on satisfying a type checker. Throughout this paper, we relate the high-level definitions to their Agda counterparts using a MODEL footnote indicating their location. For an absolutely formal treatment, we therefore refer the reader to the companion formalisation. The formalisation is available on Dagand's website.

A shorter version of this paper has appeared in the proceedings of the 17th ACM SIGPLAN International Conference on Functional Programming (ICFP 2012) (Dagand & McBride, 2012). This version benefits from several presentational modifications to include significantly more examples (in particular, in Sections 3 and 4). The running example – lifting the comparison function of natural numbers – is also complemented by another example, lifting the addition of natural numbers. Worked out examples, throughout the paper, shall help the reader build a strong intuition of the generic constructions at play. We have also extended the original paper with new material. In Section 4.2, we cast the forcing and detagging transformations of Brady *et al.* (2003) in our universe of datatypes. Using these intuitions, we have streamlined the definition of reornaments and discuss the limits of iterating reornaments (Section 4.5). We have extended the lifting of recursion patterns to handle induction and case analysis (Section 6). Our treatment of the lifting of constructors (Section 6) has been also treated in more details and its underlying mechanisms has been thoroughly illustrated.

## 2 From comparison to lookup, manually

There is an astonishing resemblance between the comparison function `– < –` on numbers and the list lookup function (Figure 1). Interestingly, the similarity is not merely at the level of types. It is also in their implementation: their definition follows the same pattern of recursion (first, case analysis on the second argument; then induction on the first argument) and they both return a failure value (respectively,

$$\begin{array}{lcl}
 (m : \text{Nat}) < (n : \text{Nat}) : \text{Bool} & \text{lookup } (m : \text{Nat}) (xs : \text{List } A) : \text{Maybe } A & \\
 m < 0 \mapsto \text{false} & \text{lookup } m \text{ nil} \mapsto \text{nothing} & \\
 0 < (\text{succ } n) \mapsto \text{true} & \xrightarrow{?} \text{lookup } 0 (\text{cons } a \text{ xs}) \mapsto \text{just } a & \\
 (\text{succ } m) < (\text{succ } n) \mapsto m < n & \text{lookup } (\text{succ } n) (\text{cons } a \text{ xs}) \mapsto \text{lookup } n \text{ xs} & 
 \end{array}$$

Fig. 1. Implementation of  $- < -$  and lookup.

false and nothing) in the first case analysis and a success value (respectively, true and just) in the base case of the induction.

This raises the question: What *exactly* is the relation between  $- < -$  and lookup? Also, could we use the implementation of  $- < -$  to guide the construction of lookup? First, let us work out the relation at the type level. To this end, we use ornaments to explain how each individual datatype has been promoted when going from  $- < -$  to lookup:

$$\begin{array}{ccccc}
 - < - & : & \text{Nat} & \rightarrow & \text{Nat} & \rightarrow & \text{Bool} \\
 & & \downarrow \text{idO Nat-func} & & \downarrow \text{List-Orn } A & & \downarrow \text{Maybe-Orn } A \\
 \text{lookup} & : & \text{Nat} & \rightarrow & \text{List } A & \rightarrow & \text{Maybe } A
 \end{array}$$

Note that the first argument is ornamented to itself, or put differently, it has been ornamented by the identity ornament *idO* (Example 4.9).

Each of these ornaments come with a forgetful map:

$$\begin{array}{lcl}
 \text{length } (as : \text{List } A) : \text{Nat} & & \text{isJust } (m : \text{Maybe } A) : \text{Bool} \\
 \text{length nil} \mapsto 0 & & \text{isJust nothing} \mapsto \text{false} \\
 \text{length } (\text{cons } a \text{ as}) \mapsto \text{succ } (\text{length } as) & & \text{isJust } (\text{just } a) \mapsto \text{true}
 \end{array}$$

As we shall see in Section 4.3, the forgetful maps can be automatically derived from the ornament definition.

Using these forgetful maps we deduce a relation, at the operational level, between  $- < -$  and lookup. This relation is uniquely determined by the ornamentation of the individual datatypes. This *coherence property* is expressed as follows:

$$(n : \text{Nat})(xs : \text{List } A) \rightarrow \text{isJust } (\text{lookup } n \text{ xs}) = n < \text{length } xs$$

or, equivalently, using a commuting diagram:

$$\begin{array}{ccc}
 \text{Nat} \times \text{List } A & \xrightarrow{\text{lookup}} & \text{Maybe } A \\
 \text{id} \times \text{length} \downarrow & & \downarrow \text{isJust} \\
 \text{Nat} \times \text{Nat} & \xrightarrow{- < -} & \text{Bool}
 \end{array}$$

*Remark 2.1 (Vocabulary)*

We call the function we start with the *base function* (here,  $- < -$ ), its type being the *base type* (here,  $\text{Nat} \rightarrow \text{Nat} \rightarrow \text{Bool}$ ). The richer function type built by ornamenting

the individual pieces is called the *functional ornament*<sup>1</sup> of the base type (here,  $\text{Nat} \rightarrow \text{List } A \rightarrow \text{Maybe } A$ ). A function inhabiting this type is called a *lifting* (here, `lookup`). A lifting is said to be *coherent* if it satisfies the coherence property.

*Remark 2.2 (Coherence and functional ornament)*

It is crucial to understand that the coherence of a lifting is relative to a given functional ornament: the same base function ornamented differently would give rise to a different coherence property.

For example, the base type  $\text{Nat} \rightarrow \text{Nat} \rightarrow \text{Nat}$  can be functionally ornamented to

$$\text{Nat} \rightarrow \text{List } A \rightarrow \text{List } A$$

for which `drop` is a coherent solution with respect to  $--$ . However, it can also be functionally ornamented to

$$\text{List } A \rightarrow \text{List } A \rightarrow \text{List } A$$

for which  $-++-$  is a coherent solution with respect to  $-+-$ . Nonetheless, the two solutions are exclusive: `drop` is not coherent with respect to  $-+-$ , nor is  $-++-$  coherent with respect to  $--$ .

We now have a better grasp of the relation between the base function and its lifting. However, `lookup` remains to be implemented while making sure that it satisfies the coherence property. Traditionally, one would stop here: we would implement `lookup` and prove the coherence as a theorem. This works rather well in a system such as Coq since it offers a powerful theorem-proving environment. It does not work so well in a system such as Agda that does not offer tactics to its users, forcing them to write explicit proof terms. It would not work at all in an ML language with GADTs, which has no notion of proof.

Historically, Coq has been designed for the verification of (simply typed) programs through (dependently typed) propositions (Paulin-Mohring, 1989). This paradigm started shifting with languages such as Epigram, Cayenne, or Agda: these systems offer an environment for *dependently typed programming*. In this setting, the approach that consists in writing a simply typed programming to prove it correct *after the fact* feels utterly laborious. If we have dependent types, why should we use them only for *proofs*, as an afterthought? A dependently typed programming environment lets us write a `lookup` function *correct by construction*: by implementing a more finely indexed version of `lookup`, the user drives the type checker into verifying the necessary invariants. This paper is an exploration of this paradigm, in which we develop techniques to relieve the dependently typed programmer from the burden of proofs.

<sup>1</sup> Note that a functional ornament is entirely determined by the ornamentation of its individual components, which we shall (unambiguously) call ‘a functional ornament’ in Section 5.2. This follows the common usage of saying that ‘lists are an ornament of natural numbers’, when in fact lists are the *result* of interpreting an ornament of natural numbers.

To get the computer to work for us, we would rather implement the function `ilookup`

```
ilookup (m : Nat) (vs : Vec A n) : IMaybe A (m < n)
ilookup  m      nil      ↦ nothing
ilookup  0     (cons a vs) ↦ just a
ilookup (suc m) (cons a vs) ↦ ilookup m vs
```

where `IMaybe A` is the option type indexed by the truth value computed by `isJust`. It is defined as follows:

```
data IMaybe [A : SET](b : Bool) : SET where
  IMaybe A (b = true)  ∋ just (a : A)
  IMaybe A (b = false) ∋ nothing
```

and it comes with a forgetful map:

```
forgetIMaybe (ima : IMaybe A b) : (ma : Maybe A) × isJust ma = b
forgetIMaybe (just a)      ↦ (just a, refl)
forgetIMaybe nothing      ↦ (nothing, refl)
```

*Remark 2.3*

We overload the constructors of `Maybe` and `IMaybe`: For a bi-directional type checker, there is no ambiguity as constructors are checked against their type.

The rationale behind `ilookup` is to *index* the types of lookup by their unornamented version. In effect, we index the types of its arguments by the (respective) arguments  $m : \text{Nat}$  and  $n : \text{Nat}$  of  $- < -$  and we index the type of its result by  $m < n$ . By doing so, we can make sure that the result computed by `ilookup` respects the output of  $- < -$  on the unornamented indices: the result is necessarily correct, *by indexing!* The type of `ilookup` is naturally derived from the ornamentation of  $- < -$  into `lookup` and is uniquely determined by the functional ornament we start with. We shall automate its construction in Section 5.3 with the notion of *patch* (Definition 5.15).

*Remark 2.4 (Vocabulary)*

Expanding further our vocabulary, such a finely indexed function that is coherent by construction is called a *coherent liftings*.

We had separately introduced the notion of *lifting* and *coherence* in Remark 2.1, with the idea that a lifting is not necessarily coherent. Here we are defining the *coherent lifting* as those liftings that are coherent by construction. In fact, we shall establish in Theorem 5.19 that a lifting satisfying the coherence condition is isomorphic to a coherent lifting. There is therefore no ambiguity in identifying notions of both ‘coherent lifting’ and ‘lifting satisfying the coherence condition’.

Ko and Gibbons (2011) use ornaments to specify the coherence requirements of functional liftings, but we work the other way around. From `ilookup`, we extract the `lookup` function

```
lookup (m : Nat) (xs : List A) : Maybe A
lookup  m      xs      ↦ π₀(forgetIMaybe (ilookup m (makeVec xs)))
```



and its proof of correctness

$$\begin{aligned} \text{cohLookup } (n : \text{Nat}) (xs : \text{List } A) & : \text{isJust } (\text{lookup } n \text{ } xs) = n < \text{length } xs \\ \text{cohLookup } m \quad xs & \mapsto \pi_1(\text{forgetIMaybe } (\text{ilookup } m (\text{makeVec } xs))) \end{aligned}$$

where  $\text{makeVec} : (xs : \text{List } A) \rightarrow \text{Vec } A (\text{length } xs)$  turns a list into a vector of the corresponding length. Operationally, it is an identity. In Section 4.4, we show that it can be automatically derived from the ornament of lists.

The construction of  $\text{lookup}$  and  $\text{cohLookup}$  feels automatic: We shall see in Section 5.4, how  $\text{lookup}$  can automatically be obtained by *patching* (Definition 5.22), while  $\text{cohLookup}$  is merely an instance of a generic *coherence* result (Definition 5.23).

*Remark 2.5 (ilookup vs. vlookup)*

The function  $\text{ilookup}$  is very similar to the more familiar  $\text{vlookup}$  function:

$$\begin{aligned} \text{vlookup } (m : \text{Fin } n) (vs : \text{Vec } A \ n) & : A \\ \text{vlookup } f_0 \quad (\text{cons } a \ xs) & \mapsto a \\ \text{vlookup } (\text{fsuc } n) \quad (\text{cons } a \ xs) & \mapsto \text{vlookup } n \ xs \end{aligned}$$

These two definitions are actually equivalent, thanks to the isomorphism

$$(m : \text{Nat}) \rightarrow \text{IMaybe } A (m < n) \cong \text{Fin } n \rightarrow A$$

where we silently lift the boolean predicate  $m < n$  at the type level, as is a common practice in SSREFLECT (Gonthier *et al.*, 2008), for instance.

Intuitively, we can move the constraint ‘ $m < n$ ’ from the result – where we return an object of type  $\text{IMaybe } A (m < n)$  – to the premise – where we expect an object of type  $\text{Fin } n$ . Indeed, we can think of the type  $\text{Fin } n$  as the combination of a number  $m : \text{Nat}$  together with a proof that  $m < n$ .

With this example, we have manually unfolded the key steps of the construction of a lifting of  $- < -$ . Let us recapitulate each step:

- Start with a *base function*, here  $- < - : \text{Nat} \rightarrow \text{Nat} \rightarrow \text{Bool}$ ;
- Ornament its inductive components as desired, here  $\text{Nat}$  to  $\text{List } A$  and  $\text{Bool}$  to  $\text{Maybe } A$  in order to describe the lifting of interest, here  $\text{lookup} : \text{Nat} \rightarrow \text{List } A \rightarrow \text{Maybe } A$  satisfying

$$(n : \text{Nat})(xs : \text{List } A) \rightarrow \text{isJust } (\text{lookup } n \text{ } xs) = n < \text{length } xs$$

- Implement a carefully indexed version of the lifting, here

$$\text{ilookup} : (m : \text{Nat})(vs : \text{Vec } A \ n) \rightarrow \text{IMaybe } A (m < n)$$

- Derive the lifting, here  $\text{lookup}$ , and its coherence proof, without *writing* a proof!

Besides,  $\text{ilookup}$  is a useful addition to our library: It corresponds to the familiar vector lookup function, a function that one would have implemented anyway. Thus,  $\text{ilookup}$  is not just some scaffolding necessary to define  $\text{lookup}$ , it is a purposeful operation on its own.

This manual unfolding of the lifting is instructive: it involves many constructions on datatypes (here the datatypes  $\text{List } A$  and  $\text{Maybe } A$ ) as well as on functions (here

the type of `ilookup`, the definition of `lookup`, and its coherence proof). Yet, it feels like a lot of these constructions could be automated. In Section 5, we shall build the machinery to describe these transformations and obtain them *within* the type theory itself.

### 3 A Universe of datatypes

In dependently typed systems such as Coq or Agda, datatypes are an external entity: each datatype definition extends the type theory with new introduction and elimination forms. The validity of a datatype definition is guaranteed by a positivity checker that is a part of the meta-theory of the proof system. A consequence is that, from within the type theory, it is not possible to create or manipulate inductive definitions, since they belong to the meta-theory.

In a previous work (Chapman *et al.*, 2010), we have shown how to internalise inductive families into the type theory. The practical outcome of this approach is that we can manipulate datatype declarations as first-class objects. We can program over the grammar of datatypes and, in particular, we can compute new datatypes from old. This is particularly useful to formalise the notion of ornament entirely within the type theory. This also has a theoretical outcome: We do not need to prove meta-theoretical properties of our constructions, we can work in our type theory and use its logic as a formal system.

*Remark 3.1 (Theory vs. meta-theory)*

The constructions described in this paper are *also* applicable in a setting where datatype definitions are *not* internalised: All our constructions could be justified at the meta-level and then be syntactically presented in a language such as, say, Agda, Coq, or an ML with GADTs. Working with an internalised presentation, we can simply avoid these two levels of logic and work in the logic provided by the type theory.

Our requirements on the ambient type theory are boxed in a `TYPE THEORY` frame (e.g. Figure 2, while constructions within that type theory are boxed in a `DEFINITION` frame (e.g. Figure 3). Since our work is grounded in an intensional reading of extensional isomorphisms, we box the original, extensional results in `META-THEOREM` frames (e.g. Equation 4.20). The proof of these results are absent from our (intensional) Agda model. Examples illustrating the various concepts are left unboxed.

#### 3.1 The type theory

Following our previous work, our requirements on the type theory are minimal: We will need  $\Sigma$ -types,  $\Pi$ -types, the unit set  $\mathbb{1}$ , and at least two universes, `SET` and `SET1`.  $\Sigma$ -types are denoted as  $(a : A) \times B$ , introduced by pairs  $(x, y)$ , and eliminated by first and second projections, respectively,  $\pi_0$  and  $\pi_1$ .  $\Pi$ -types are denoted as  $(a : A) \rightarrow B$ , introduced by  $\lambda x. b$ , and eliminated by function application. The unit set is (uniquely) inhabited by  $*$ . For convenience, we require the  $\eta$ -laws for the unit set,

TYPE THEORY	
<b>data</b> $\mathbf{IDesc} [I : \mathbf{SET}] : \mathbf{SET}_1$ <b>where</b> $\mathbf{IDesc} I \ni \mathbf{var} (i : I)$ $\quad   1$ $\quad   \Pi (S : \mathbf{SET}) (T : S \rightarrow \mathbf{IDesc} I)$ $\quad   \Sigma (S : \mathbf{SET}) (T : S \rightarrow \mathbf{IDesc} I)$	$\llbracket (D : \mathbf{IDesc} I) \rrbracket (X : I \rightarrow \mathbf{SET}) : \mathbf{SET}$ $\llbracket \mathbf{var} i \rrbracket X \mapsto X i$ $\llbracket 1 \rrbracket X \mapsto \mathbb{1}$ $\llbracket \Pi ST \rrbracket X \mapsto (s : S) \rightarrow \llbracket T s \rrbracket X$ $\llbracket \Sigma ST \rrbracket X \mapsto (s : S) \times \llbracket T s \rrbracket X$

Fig. 2. Universe of inductive families.

$\Sigma$ -types (i.e. surjective pairing), and  $\Pi$ -types to hold definitionally. When  $x$  is not free in  $B$ , we use the following abbreviations:

$$(x : A) \rightarrow B \triangleq A \rightarrow B$$

$$(x : A) \times B \triangleq A \times B$$

hence obtaining the (non-dependent) implication and conjunction from the dependent quantifiers.

For convenience, we ask for our type theory to support *enumerations* of tags. We shall not dwell on their type theoretic definition, which can be found elsewhere (Dagand, 2013). We declare a (finite) enumeration of tags 'a, 'b, and 'c by writing  $\{ 'a 'b 'c \}$ . Similarly, we define functions from such a collection by exhaustively enumerating the returned values, using the notation

$$\{ 'a \mapsto e_a, 'b \mapsto e_b, 'c \mapsto e_c \}$$

When the cases are vertically aligned, we shall skip the separating commas.

We also need a pre-existing notion of propositional equality, denoted  $- = -$ . We shall assume that it is reflexive, as witnessed by `refl`, and substitutive. Since we perform numerous pattern-matches on indexed datatypes, we also require our equality to satisfy the K rule (McBride, 1999), i.e. `refl` is a unique inhabitant of a propositional equality.

### 3.2 Universe of descriptions

We internalise inductive families by a universe construction. The role of this universe is to *describe* signature functors over  $\mathbf{SET}$  indexed by  $I$ , i.e. functors from  $\mathbf{SET}^I$  to  $\mathbf{SET}^I$ . However, up to some currying–uncurrying, this type is subjected to the isomorphism

$$\mathbf{SET}^I \rightarrow \mathbf{SET}^I \triangleq (I \rightarrow \mathbf{SET}) \rightarrow (I \rightarrow \mathbf{SET})$$

$$\cong I \rightarrow (I \rightarrow \mathbf{SET}) \rightarrow \mathbf{SET}$$

that lets us focus on describing functors from  $\mathbf{SET}^I \rightarrow \mathbf{SET}$ , with the  $I$ -indexing being pulled away in the exponential. Following this remark, we focus first on describing signature functors of type  $\mathbf{SET}^I \rightarrow \mathbf{SET}$  (Definition 3.2). Then, to capture signature functors between slices of  $\mathbf{SET}$ , we simply introduce an exponential (Definition 3.3), a construction akin to the Reader monad.

*Definition 3.2 (Universe of descriptions<sup>2</sup>)*

The universe of descriptions is defined in Figure 2. The meaning of codes – the inhabitants of `IDesc` – is given by their interpretation in `SET`:

- $\Sigma$  codes  $\Sigma$ -types – to build sums-of-products;
- $\Pi$  codes  $\Pi$ -types – to capture higher-order arguments;
- `1` codes the unit type – to terminate codes;
- `var` codes the recursive arguments of inductive definitions, taken at an index  $i$ .

*Definition 3.3 (Descriptions<sup>3</sup>)*

We obtain the universe of descriptions `func` by simply pulling the  $I$ -index to the front. The interpretation  $\llbracket - \rrbracket$  extends pointwise to `func`:

TYPE THEORY	
$\text{func } (I : \text{SET}) : \text{SET}_1$ $\text{func } I \mapsto I \rightarrow \text{IDesc } I$	$\llbracket (D : \text{func } I) \rrbracket (X : I \rightarrow \text{SET}) : I \rightarrow \text{SET}$ $\llbracket D \rrbracket X \mapsto \lambda i. \llbracket D \ i \rrbracket X$

Because it describes functors, this universe offers a generic map operator:

TYPE THEORY
$\llbracket (D : \text{func } I) \rrbracket^{\rightarrow} : (f : \forall i. X \ i \rightarrow Y \ i)(xs : \llbracket D \rrbracket X \ i) \rightarrow \llbracket D \rrbracket Y \ i$

Inhabitants of the `func` type are called *descriptions*.

*Remark 3.4 (Overloaded notation)*

We overload the symbol  $\llbracket - \rrbracket$  to denote both the interpretation of a description code to a functor from `SETI` to `SET` (Definition 3.2), and the interpretation of a description to an endofunctor from `SETI` to `SETI` (Definition 3.3). Indeed, the latter is merely of pointwise lifting of the former.

Descriptions, by interpreting to strictly positive functors on slices of `SET`, admit a least fixpoint<sup>4</sup> construction:

TYPE THEORY
$\mathbf{data} \ \mu \ [D : \text{func } I](i : I) : \text{SET} \ \mathbf{where}$ $\mu \ D \ i \ni \text{ in } (xs : \llbracket D \rrbracket (\mu \ D) \ i)$

<sup>2</sup> MODEL: `IDesc.IDesc`

<sup>3</sup> MODEL: `IDesc.IDesc`

<sup>4</sup> MODEL: `IDesc.IDesc.InitialAlgebra`

The inductive types thus formed are eliminated by a generic elimination principle<sup>5</sup>:

TYPE THEORY
$\text{induction} : \forall P : \forall i : I. \mu D i \rightarrow \text{SET}.$ $(\alpha : (i : I)(xs : \llbracket D \rrbracket (\mu D) i) \rightarrow \square_D P xs \rightarrow P \text{ (in } xs))$ $(x : \mu D i) \rightarrow P x$

that corresponds to transfinite induction over tree-like structures. A formal description of induction can be found elsewhere (Dagand, 2013). Intuitively,  $\square_D P xs$  asserts that all sub-trees of  $xs$  satisfy  $P$ : this captures precisely the inductive hypothesis. The argument  $\alpha$  therefore corresponds to the inductive step: given that the induction hypothesis holds for sub-elements of  $xs$ , we must prove that  $P$  holds for the whole. In the categorical literature (Hermida & Jacobs, 1998; Fumex, 2012),  $\square_D$  is called the canonical lifting<sup>6</sup> of  $D$ .

Well-founded recursive definitions by pattern-matching can be expressed in terms of the induction principle (McBride, 2002). For conciseness, we adopt a pattern-matching style when the recursive pattern is unsurprising, with the confidence that it can be expressed in terms of to induction.

### 3.3 Inductive definitions

While we could *code* our inductive families directly in this universe, let us introduce an *informal notation* to declare datatypes. Our purpose here is to relate the reader's intuition for inductive definitions with our encodings. By relying on a more intuitive notation, we wish to make our examples more palatable. Our notation is strongly inspired by Agda's datatype declarations.

As witnessed by the Agda model, all the inductive definitions given in this paper can be translated into descriptions. For a datatype  $T$ , we write  $T$ -func the code it elaborates to. Similarly, we call  $T$ -elim the elimination principle of  $T$ , and  $T$ -case the case analysis over  $T$ . These operations can be reduced generically derived from induction (McBride *et al.*, 2004; Dagand & McBride, 2013b).

We also write datatype constructors (in expressions) and constructor patterns (in pattern-matching clauses) using a high-level notation. In fact, they correspond to (low-level) terms built from the generic in constructor and a tuple of arguments. This elaboration mechanism is described elsewhere (Dagand, 2013).

#### Example 3.5

For Peano numbers (i.e. natural numbers  $\text{Nat}$ ), these induction principles amount to – after suitable currying and simplification – the propositions:

$$\text{Nat-elim} : \forall P : \text{Nat} \rightarrow \text{SET}. P 0 \rightarrow ((m : \text{Nat}) \rightarrow P m \rightarrow P (\text{suc } m)) \rightarrow (n : \text{Nat}) \rightarrow P n$$

$$\text{Nat-case} : \forall P : \text{Nat} \rightarrow \text{SET}. P 0 \rightarrow ((m : \text{Nat}) \rightarrow P (\text{suc } m)) \rightarrow (n : \text{Nat}) \rightarrow P n$$

<sup>5</sup> MODEL: IDesc.IDesc.Induction

<sup>6</sup> MODEL: IDesc.IDesc.Lifting

A formal presentation of the elaboration of inductive definitions to code will be found elsewhere (Dagand & McBride, 2013b). However, it is intuitive enough to be understood with a few examples. Three key ideas are at play:

- Constructors are presented as sums of products, *à la* ML (Example 3.6).
- Indices can be constrained by equality, *à la* Agda (Example 3.7).
- Indices can be matched upon (Examples 3.8).

*Example 3.6 (Sums of products, following the ML tradition)*

We name the datatype and then comes a choice of constructors. Each constructor is then defined by a  $\Sigma$ -telescope of arguments. For example, the list datatype<sup>7</sup> is defined by

```

data List [A : SET] : SET where
  List A  $\ni$  nil
      | cons (a : A)(as : List A)
       $\vdots$ 
List-func (A : SET) : func  $\mathbb{1}$ 
List-func A  $\mapsto \lambda^*. \Sigma \left\{ \begin{array}{l} \text{'nil} \\ \text{'cons} \end{array} \right\} \left\{ \begin{array}{l} \text{'nil} \mapsto 1 \\ \text{'cons} \mapsto \Sigma A \lambda - . \text{var } * \end{array} \right\}$ 

```

Ordinals<sup>8</sup> also follow this pattern:

```

data Ord : SET where
  Ord  $\ni$  0
      | suc (o : Ord)
      | lim (l : Nat  $\rightarrow$  Ord)
       $\vdots$ 
Ord-func : func  $\mathbb{1}$ 
Ord-func  $\mapsto \lambda^*. \Sigma \left\{ \begin{array}{l} \text{'0} \\ \text{'suc} \\ \text{'lim} \end{array} \right\} \left\{ \begin{array}{l} \text{'0} \mapsto 1 \\ \text{'suc} \mapsto \text{var } * \\ \text{'lim} \mapsto \Pi \text{Nat } \lambda - . \text{var } * \end{array} \right\}$ 

```

Note the use of the higher-order  $\Pi$  code to express the limit ordinal.

The datatypes **Bool** – the Booleans<sup>9</sup> – and **Nat** – the natural numbers<sup>10</sup> – fall in this category too. They elaborate to descriptions indexed by  $\mathbb{1}$ , respectively **Bool-func** and **Nat-func**, following a similar sums-of-products pattern. We leave it as an exercise to compute their code, guided by the following remarks:

- **Nat-func** is a degenerate case of **List-func**: it is a list taking no *A*-argument.
- **Bool-func** is a degenerate case of **Nat-func**: it offers two constructors, but no recursive argument.

<sup>7</sup> MODEL: IDesc.Examples.List

<sup>8</sup> MODEL: IDesc.Examples.Ordinal

<sup>9</sup> MODEL: IDesc.Examples.Bool

<sup>10</sup> MODEL: IDesc.Examples.Nat

*Example 3.7 (Indexing, following the Agda convention)*

Indices can be *constrained* to some particular value. For example, vectors can be defined by constraining the index to be 0 in the nil case and  $\text{suc } n'$  for some  $n' : \text{Nat}$  in the cons case<sup>11</sup>:

```

data Vec [A : SET](n : Nat) : SET where
  Vec A (n = 0)   ∋ nil
  Vec A (n = suc n') ∋ cons (n' : Nat)(a : A)(vs : Vec A n')

```

⋮

```

Vec-func (A : SET) : func Nat
Vec-func A ↦ λn. Σ { 'nil } { 'cons ↦ Σ Nat λn'. Σ (n = suc n') λ - . Σ A λ - . var n' }

```

The constraint notation  $(n = t)$  reads ‘for any index  $n$ , as long as  $n$  equals  $t$ ’, following the Henry Ford principle (McBride, 1999). In particular, it must *not* be confused with a definition pattern-matching on the index.

In the same vein, finite sets<sup>12</sup> can be defined by constraining the upper-bound  $n$  to always be strictly positive, and indexing the argument of  $\text{fsuc}$  by the predecessor:

```

data Fin (n : Nat) : SET where
  Fin (n = suc n') ∋ f0 (n' : Nat)
                    | fsuc (n' : Nat)(k : Fin n')

```

⋮

```

Fin-func : func Nat
Fin-func ↦ λn. Σ { 'f0 } { 'fsuc ↦ Σ Nat λn'. Σ (n = suc n') λ - . var n' }

```

Note that elaboration captures the constraints on indices by using propositional equality. In the case of `Vec`, we first abstract over the index  $n$ , introduce the choice of constructors with the first  $\Sigma$  and then, once the constructors have been chosen, we restrict  $n$  to its possible value(s): 0 in the first case and  $\text{suc } n'$  for some  $n'$  in the second case. Hence, the placement of equality constraints in the elaborated code: After the constructor is chosen, we first introduce a fresh variable and then constrain the index with it. If no fresh variable needs to be introduced, we directly constrain the index.

*Example 3.8 (Computing over indices)*

We can also use the crucial property that a datatype definition is, in effect, a *function* from its indices to a choice of datatype constructors. Our notation should reflect this ability. For instance, inspired by Brady *et al.* (2003), we give an alternative presentation of vectors that matches on the index to determine the constructor to

<sup>11</sup> MODEL: IDesc.Examples.Vec

<sup>12</sup> MODEL: IDesc.Examples.Fin

be presented,<sup>13</sup> hence removing the need for constraints:

```

data Vec [A : SET](n : Nat) : SET where
  Vec A    n    <= Nat-case n
  Vec A    0    &sup3; nil
  Vec A (suc n) &sup3; cons (a : A)(vs : Vec A n)

  ~~~~~

Vec-func (A : SET) : func Nat
Vec-func A    n    <= Nat-case n
Vec-func A    0    &mapsto &Sigma { 'nil } &lambda - . 1
Vec-func A (suc n) &mapsto &Sigma { 'cons } &lambda - . &Sigma A &lambda - . var n
    
```

In order to be fully explicit about computations, we use the ‘by’ ( $\Leftarrow$ ) gadget, which lets us appeal to any elimination principle. For simplicity, we shall use a pattern-matching style when the recursion pattern is unremarkable.

Using pattern-matching, we define the computational counterpart of finite sets by matching on  $n$ ,<sup>14</sup> offering no constructor in the 0 case, and the two expected constructors in the  $\text{suc } n$  case:

```

data Fin (n : Nat) : SET where
  Fin 0    &sup3;
  Fin (suc n) &sup3; f0
                  | fsuc (k : Fin n)

  ~~~~~

Fin-func : func Nat
Fin-func 0    &mapsto &Sigma 0 0-elim
Fin-func (suc n) &mapsto &Sigma { 'f0 } { 'fsuc &mapsto var n }
    
```

Note the pattern used here to provide *no* constructor when the index is 0: we ask for a witness of the empty set, effectively preventing any constructor to be introduced.

*Remark 3.9 (Forcing and detagging (Brady et al., 2003))*

This technique of extracting information by case analysis on the indices applies to descriptions exactly where Brady’s *forcing* and *detagging* optimisations apply in compilation. They eliminate just those constructors, indices, and constraints that are redundant even in *open* computation.

Detagging amounts to restricting the choice of constructors by matching on the index. For detagging to apply, constructors must be in injective correspondence with the indices. Our presentation of vectors above is obtained by detagging. By noticing whether the index is 0 or  $\text{suc}$ , we deduce the vector’s constructor.

<sup>13</sup> MODEL: IDesc.Examples.Vec

<sup>14</sup> MODEL: IDesc.Examples.Fin



Forcing amounts to computing the argument  $x : X$  of a constructor from its index  $i : I$ . Hence, for forcing to apply, we must have a function  $f$  – ideally, the identity – from  $I$  to  $X$  such that  $f i \mapsto x$ . Our alternative presentation of `Fin` above is obtained by forcing: instead of storing an index  $n'$ , we pattern-match on the index  $n$  and directly use its predecessor in the recursive argument.

This last definition style departs radically from the one adopted by Coq, Agda, or GADTs. While it is possible to *encode* these definitions in Coq and Agda (through a large elimination), we have to step outside the realm of inductive definitions. Doing so, we lose access to the system's machinery for handling inductive reasoning. For instance, one would have to manually provide an elimination principle for the resulting object.

It is crucial to understand that this notation is reflecting the actual semantics of inductive families as functors of type  $I \rightarrow (I \rightarrow \text{SET}) \rightarrow \text{SET}$ . By using the function space  $I \rightarrow -$  to its full potential, we can *compute* over indices, not merely constrain them. With our syntax, we give the user the ability to write these *functions*: the reader should now understand a datatype definition as a special kind of function definition, taking indices as arguments, potentially computing over them, and eventually emitting a choice of constructors.

The original definition of ornaments was based on a universe following the Agda convention, which could only capture the indexing disciplines through equality constraints. Our ability to compute over indices has far-reaching consequences on ornaments. First, it enables the definition of a novel *deletion* ornament (Section 4), which uses the indexing information to delete redundant arguments in an ornamented datatype. Second, it enables a better structured and, consequently, more space-efficient definition of the algebraic ornament by the ornamental algebra (Section 4.5).

### Example 3.10

We can sensibly mix these definition styles. An example that benefits from this approach is the presentation of minimal logic<sup>15</sup> – i.e. from the other side of the Curry–Howard, the simply typed lambda calculus (Benton *et al.*, 2012) – given as an inductively defined inference system. We express the judgement  $\Gamma \vdash T$  through an inductive family indexed by a context  $\Gamma$  of typed variables and a type  $T$ :

```

data ( $\Gamma$  : Context)  $\vdash$  ( $T$  : Type) : SET where
   $\Gamma \vdash T \ni \text{var } (v : T \in \Gamma)$ 
    | app ( $S$  : Type) ( $f : \Gamma \vdash S \Rightarrow T$ ) ( $s : \Gamma \vdash S$ )
   $\Gamma \vdash \text{unit} \ni *$ 
   $\Gamma \vdash S \Rightarrow T \ni \text{lam } (b : \Gamma ; S \vdash T)$ 

```

where, for simplicity, we have restricted the language of types to the unit and the exponential:

```

data Type : SET where
  Type  $\ni$  unit
    | ( $S$  : Type)  $\Rightarrow$  ( $T$  : Type)

data Context : SET where
  Context  $\ni$   $\epsilon$ 
    | ( $\Gamma$  : Context) ; ( $T$  : Type)

```

<sup>15</sup> MODEL: IDesc.Examples.STLC

and for which we can define (inductively, in fact) a predicate  $T \in \Gamma$  that indexes a variable of type  $T$  in context  $\Gamma$ .

Crucially, the variable and application rules take the index *as is*, without constraint or computation. The remaining rules depend on the index: if it is an exponential, we give the abstraction rule; if it is the unit type, we give the (only) inhabitant of that type.

*Remark 3.11 (Constraints and equality)*

We have been careful in using equality to *introduce* constraints here: Our definition of datatypes is absolutely agnostic in the notion of propositional equality offered by the underlying type theory. For instance, our universe of inductive families cannot be used to *define* equality through the identity type: the identity type would only *expose* the underlying notion of equality to the user.

This is unlike systems such as Coq or Agda, where propositional equality is introduced by the identity type

$$\mathbf{data} \text{ Id } [a_1 : A](a_2 : A) : \mathbf{SET} \mathbf{where}$$

$$\text{Id } a_1 (a_2 = a_1) \ni \text{refl}$$

whose elimination principle gives the J-rule (Hofmann & Streicher, 1994).

In our system, this definition<sup>16</sup> would elaborate to a description *packaging* the propositional equality:

$$\text{Id-func } (a_1 : A) : \text{func } A$$

$$\text{Id-func } a_1 \mapsto \lambda a_2. \Sigma \{ \text{refl} \} \{ \Sigma (a_2 = a_1) \lambda - . 1 \}$$

#### 4 A Universe of ornaments

Originally, McBride (to appear) presented the notion of ornament for a universe where the indexing discipline could *only* be enforced by equality constraints. As a result, the deletion ornament was not expressible in that setting. We shall now adapt the original definition to our system.

*Definition 4.1 (Universe of ornaments<sup>17</sup>)*

The grammar of ornaments (Figure 3) is similar to the original one. It is defined over a base datatype  $D$  indexed by  $K$ , and ornaments it to a datatype indexed by  $I$ . The (forgetful) function  $u : I \rightarrow K$  specifies a refinement of  $K$ -indices into  $I$ -indices. We can *copy* the base datatype (with the codes  $1$ ,  $\Pi$ , and  $\Sigma$ ), *extend* it by inserting sets (with the code *insert*), and *refine* the indexing subject to the relation imposed by  $u$  (with the code *var*). Also, following Brady *et al.*'s (2003) insight that *inductive families need not store their indices*, we can *delete* parts of the datatype definition as long as we can provide a witness. This witness will typically be provided by the index, here in the context.

The extension of ornaments computes the description of the extended datatype. This amounts to traversing the ornament code, packing the freshly insert-ed data

<sup>16</sup> MODEL: IDesc.Examples.Id

<sup>17</sup> MODEL: Orn.Ornament

DEFINITION

<p><b>data</b> Orn (<math>D : \text{IDesc } K</math>) [<math>u : I \rightarrow K</math>] : SET<sub>1</sub> <b>where</b></p> <p>– Extend with <math>S</math>:</p> <p>Orn <math>D \ u \ \ni \ \text{insert } (S : \text{SET})</math>  <math>(D^+ : S \rightarrow \text{Orn } Du)</math></p> <p>– Refine index:</p> <p>Orn (<math>\text{var } k</math>) <math>u \ \ni \ \text{var } (i : u^{-1} k)</math></p> <p>– Copy the original:</p> <p>Orn <math>1 \ u \ \ni \ 1</math></p> <p>Orn (<math>\Pi ST</math>) <math>u \ \ni \ \Pi (T^+ : (s : S) \rightarrow \text{Orn } (T s) u)</math></p> <p>Orn (<math>\Sigma ST</math>) <math>u \ \ni \ \Sigma (T^+ : (s : S) \rightarrow \text{Orn } (T s) u)</math></p> <p>– Delete <math>S</math>:</p> <p style="margin-left: 40px;">  <b>delete</b> (<math>s : S</math>)  <math>(T^+ : \text{Orn } (T s) u)</math></p>	<p><math>\llbracket (O : \text{Orn } Du) \rrbracket_{\text{orn}} : \text{IDesc } I</math></p> <p><math>\llbracket \text{insert } S D^+ \rrbracket_{\text{orn}} \mapsto \Sigma S \lambda s. \llbracket D^+ s \rrbracket_{\text{orn}}</math></p> <p><math>\llbracket \text{var } (\text{inv } i) \rrbracket_{\text{orn}} \mapsto \text{var } i</math></p> <p><math>\llbracket 1 \rrbracket_{\text{orn}} \mapsto 1</math></p> <p><math>\llbracket \Pi T^+ \rrbracket_{\text{orn}} \mapsto \Pi S \lambda s. \llbracket T^+ s \rrbracket_{\text{orn}}</math></p> <p><math>\llbracket \Sigma T^+ \rrbracket_{\text{orn}} \mapsto \Sigma S \lambda s. \llbracket T^+ s \rrbracket_{\text{orn}}</math></p> <p><math>\llbracket \text{delete } s T^+ \rrbracket_{\text{orn}} \mapsto \llbracket T^+ \rrbracket_{\text{orn}}</math></p>
---	---

Fig. 3. Universe of ornaments.

into  $\Sigma$  codes. In the delete case, no  $\Sigma$  code is generated: we use the witness to compute the extension of the rest of the ornament. The  $\Pi$  and  $\Sigma$  ornament codes simply duplicate the underlying datatype definition: we retrieve the set  $S$  from the index ornament  $D$  (which is equal to  $\Sigma S T$  for a  $\Sigma$  ornament, and to  $\Pi S T$  for a  $\Pi$  ornament).

*Remark 4.2 (Inverse image)<sup>18</sup>*

The inverse of a function  $f$  is defined by the following inductive type

DEFINITION

**data** [ $f : A \rightarrow B$ ]<sup>-1</sup> ( $b : B$ ) : SET **where**  
 $f^{-1} (b = f a) \ni \text{inv } (a : A)$

Equivalently, it can be defined with a  $\Sigma$ -type:

$$(f : A \rightarrow B)^{-1} (b : B) : \text{SET}$$

$$f^{-1} b \quad \mapsto (a : A) \times f a = b$$

*Definition 4.3 (Ornament)<sup>19</sup>*

An ornament is defined upon a base datatype – specified by a description  $D : \text{func } K$  – and a refined set of indices – specified by a function  $u : I \rightarrow K$ . The ornament of

<sup>18</sup> MODEL: Logic.Logic

<sup>19</sup> MODEL: Orn.Ornament

$D$  is an  $I$ -family of ornament codes for each  $D(u\ i)$ , with  $i:I$ :

DEFINITION	
$\text{orn}(D : \text{func } K)(u : I \rightarrow K) : \text{SET}_1$	$\llbracket (o : \text{orn } D\ u) \rrbracket_{\text{orn}} : \text{func } I$
$\text{orn } D\ u \mapsto (i : I) \rightarrow \text{Orn}(D(u\ i))\ u$	$\llbracket o \rrbracket_{\text{orn}} \mapsto \lambda i. \llbracket o\ i \rrbracket_{\text{orn}}$

In effect, ornamenting a description `func` consists merely in *lifting* the ornamentation of `IDesc` codes to a family indexed by  $I$ .

*Remark 4.4 (Overloaded notation)*

We overload the symbol  $\llbracket - \rrbracket_{\text{orn}}$  to denote both the interpretation of an ornament code to a description code (Definition 4.1) and the interpretation of an ornament to a description (Definition 4.3). As for descriptions (Remark 3.4), the latter is merely a pointwise lifting of the former.

### 4.1 Notation

As for inductive definitions, we adopt an *informal notation* to succinctly define ornaments. The idea is to simply mirror our **data** definition, adding **from** which datatype the ornament builds upon. When specifying a constructor, we can then extend it with new information – using  $[x : S]$  – or delete an argument originally named  $x$  by providing a witness – using  $[x \triangleq s]$ . We require the order of constructors to be preserved across ornamentation, as their name might change from the original to the ornamented version.

This high-level notation enables us to succinctly specify ornaments. It provides an abstraction over the code of ornament, in the same manner that inductive definitions let us abstract over the code of description (Section 3.3). From the definition of an ornamented type  $T$ , we conventionally call  $T$ -Orn its ornament code. A formal description of the translation is beyond the scope of this paper. Nonetheless, a few examples are enough to illustrate our notation and shall help us build some intuition for ornaments.

In an effort to reduce the syntactic noise, our notation for ornaments does not specify the forgetful function relating the indices of the ornamented type to its base type. For the examples given in this paper, these functions can be inferred from the context. If in doubt, the reader should consult the corresponding definitions in the Agda model. In an actual implementation, the user would have to provide this information.

*Example 4.5 (Ornament: from Booleans to the option type<sup>20</sup>)*

We obtain the option type from the Booleans by inserting an extra  $a : A$  in the true case:

<sup>20</sup> MODEL: Orn.Ornament.Examples.Maybe

```

data Maybe [A : SET] from Bool where
  Maybe A  $\ni$  just [a : A]
           | nothing

```

⋮

Maybe-Orn (A : SET) : orn Bool-func id

Maybe-Orn A  $\mapsto$   $\lambda^*. \text{insert} \left\{ \begin{array}{l} \text{'just} \\ \text{'nothing} \end{array} \right\} \left\{ \begin{array}{l} \text{'just} \mapsto \text{delete 'true (insert A } \lambda - . 1) \\ \text{'nothing} \mapsto \text{delete 'false 1} \end{array} \right\}$

We leave it to the reader to verify that the interpretation of this ornament (by  $\llbracket - \rrbracket_{\text{orn}}$ ) followed by the interpretation of the resulting description (by  $\llbracket - \rrbracket$ ) yields the signature functor of the option type  $X \mapsto 1 + A$ :

$$\llbracket \llbracket \text{Maybe-Orn } A \rrbracket_{\text{orn}} \rrbracket X \cong 1 + A$$

*Remark 4.6 (Notation)*

To reduce the notational burden, we overload the interpretation of ornaments  $\llbracket - \rrbracket_{\text{orn}}$  to denote both the description and the interpretation of that description. For instance, we write the above isomorphism as follows:

$$\llbracket \llbracket \text{Maybe-Orn } A \rrbracket_{\text{orn}} \rrbracket X \cong 1 + A$$

*Example 4.7 (Ornamenting natural numbers to lists<sup>21</sup>)*

We obtain lists from natural numbers with the following ornament:

```

data List [A : SET] from Nat where
  List A  $\ni$  nil
          | cons [a : A](as : List A)

```

⋮

List-Orn (A : SET) : orn Nat-func id

List-Orn A  $\mapsto$   $\lambda^*. \text{insert} \left\{ \begin{array}{l} \text{'nil} \\ \text{'cons} \end{array} \right\} \left\{ \begin{array}{l} \text{'nil} \mapsto \text{delete '0 1} \\ \text{'cons} \mapsto \text{delete 'suc (insert A } \lambda - . \text{var (inv *)} \end{array} \right\}$

Unfolding the interpretations, we check that we obtain the signature functor of lists  $X \mapsto 1 + A \times X$ :

$$\llbracket \llbracket \text{List-Orn } A \rrbracket_{\text{orn}} \rrbracket X \cong 1 + A \times X$$

*Example 4.8 (Ornamenting natural numbers to finite sets<sup>22</sup>)*

We obtain finite sets by inserting a number  $n' : \text{Nat}$ , constraining the index  $n$  to  $\text{suc } n'$ , and  $-$  in the recursive case  $-$  indexing at  $n'$ :

<sup>21</sup> MODEL: Orn.Ornament.Examples.List

<sup>22</sup> MODEL: Orn.Ornament.Examples.Fin

```

data Fin (n : Nat) from Nat where
  Fin n  $\ni$  f0 [n' : Nat][q : n = suc n']
        | fsuc [n' : Nat][q : n = suc n'](k : Fin n')
    
```



```

Fin-Orn : orn Nat-func (λn. *)
Fin-Orn  $\mapsto$  λn. insert { f0 } { fsuc }  $\left\{ \begin{array}{l} \text{f0} \mapsto \text{delete } '0 \\ \quad (\text{insert Nat } \lambda n'. \text{insert } (n = \text{suc } n') \lambda - . 1) \\ \text{fsuc} \mapsto \text{delete } ' \text{suc} \\ \quad (\text{insert Nat } \lambda n'. \text{insert } (n = \text{suc } n') \lambda - . \\ \quad \text{var } (\text{inv } n')) \end{array} \right\}$ 
```

Again, we leave it as an exercise to unfold the interpretations of this ornament and verify that it is indeed describing the signature of finite sets.

*Example 4.9 (Identity ornament<sup>23</sup>)*

In Section 2, we have introduced the *identity ornament* idO as the (trivial) ornament that merely duplicates the definition of its base type. This construction is a straightforward generic program over description codes:

```

idO (D : IDesc I) : Orn D id
idO (var i)  $\mapsto$  var (inv i)
idO 1  $\mapsto$  1
idO (Π S T)  $\mapsto$  Π λs. idO (T s)
idO (Σ S T)  $\mapsto$  Σ λs. idO (T s)
    
```

which then lifts pointwise to ornaments:

idO : (D : func I)  $\rightarrow$  orn D id

In Section 3.3, we had to adapt the original presentation of ornaments to our universe. In the process, we discovered a new ornamental operation, namely the ‘deletion ornament’. In Section 4.2, we explore some of the possibilities offered by having such a code in our system. However, we shall also verify that the ornamental constructions presented in the original framework still apply: this shall be a topic of Section 4.3 – where we recast the *ornamental algebra* in our setting – and Section 4.4 – where we recast the *algebraic ornament* construction. Finally, we revisit the *algebraic ornament by the ornamental algebra* in Section 4.5, making crucial use of both the deletion ornament and the optimisations discussed in the following section.

### 4.2 Brady optimisations, internalised

In Example 3.8, we have seen an example of Brady’s forcing and detagging optimisations respectively on finite sets and vectors. We have explained how, thanks to our definition of descriptions as functions, we could (manually) craft datatypes in this form. Instead of a presentation based on constraints, we gave an equivalent

<sup>23</sup> MODEL: Orn.Ornament.Identity

but less redundant definition. Seen as a datatype transformation, this operation is (obviously) structure-preserving. In fact, these transformations are an instance of ornamentation. The key ingredient is the delete code that lets us delete parts of a definition, using a witness extracted from the index. We can therefore craft our own Brady-optimised datatypes by ornamentation and benefit from this optimisation as early as at type checking.

To illustrate this approach, we give an example of detagging (Example 4.10) and forcing (Example 4.11). To focus solely on the Brady optimisations, we define these ornaments on the naive indexed family that we wish to optimise. In practice, we would *compose* (Dagand & McBride, 2013a) the ornament of natural numbers (Example 1.4 for vectors, and Example 4.8 for finite sets) with these optimisations. The composition would directly give the optimised version of vectors and finite sets respectively, thus avoiding an unnecessary duplication of isomorphic datatypes.

*Example 4.10 (Detagging, by ornamentation<sup>24</sup>)*

The definition of vectors in Example 3.7 mirrors the Agda convention of constraining indices with equality. Our definition of ornaments lets us define a version of `Vec` that does not store its indices. Indeed, we can describe `Vec` by an ornament that matches the index  $n$  to determine which constructor to offer:

```

data Vec' [A : SET](n : Nat) from Vec A n where
  Vec' A 0   ⊃ nil
  Vec' A (suc n) ⊃ cons [n' ≐ n](a : A)(vs : Vec' A n)
  ⋮
Vec'-Orn (A : SET)      : orn Vec-func id
Vec'-Orn A      0   ↦ insert {'nil} λ - .delete 'nil (delete refl 1)
Vec'-Orn A      (suc n) ↦ insert {'cons} λ - .
                           delete 'cons (delete n (delete refl (Σ λ - .var (inv n))))

```

Such a definition was unavailable in the original presentation of ornaments (McBride, to appear). We have internalised detagging: the constructors of the datatype are determined by the index.

*Example 4.11 (Forcing, by ornamentation<sup>25</sup>)*

The definition of finite sets given in Example 3.7 is also subject to an optimisation: by matching the index, we can avoid the duplication of  $n$  by deleting  $n'$  with the matched predecessor and trivialising the proofs. Hence, `Fin` can be further ornamented to the

<sup>24</sup> MODEL: Orn.Ornament.Examples.Vec

<sup>25</sup> MODEL: Orn.Ornament.Examples.Fin

optimised  $\text{Fin}'$ , which makes crucial use of deletion:

```

data Fin' (n : Nat) from Fin n where
  Fin' 0     $\ni [b : 0]$ 
  Fin' (suc n)  $\ni f0 [n' \triangleq n]$ 
                | fsuc [n' \triangleq n](k : Fin' n')
                 $\vdots$ 
  Fin'-Orn      : orn Fin-func id
  Fin'-Orn 0     $\mapsto$  insert 0 0-elim
  Fin'-Orn (suc n)  $\mapsto$   $\Sigma$  {
    f0  $\mapsto$  delete n (delete refl 1)
    fsuc  $\mapsto$  delete n (delete refl (var (inv n)))
  }
    
```

Note that when  $n$  is 0, there is in fact no constructor: we insert the empty set  $\emptyset$  to account for the absence of constructor in this index.

Again, this definition was previously unavailable to us. We have internalised forcing: the content of the constructors – here  $n'$  – are retrieved from the index, instead of being needlessly duplicated.

*Remark 4.12 (Non-generic transformations)*

The above transformations are *ad-hoc*: We have to manually give the ornament that performs the detagging and/or forcing. Because of the higher-order nature of our universe of descriptions, we cannot analyse the link between the indices, and between the constructor choice and the constructor’s contents. To achieve this from within the type theory, we would need a first-order language for describing (a sufficiently expressive fragment of) the function space  $I \rightarrow \text{IDesc } I$ . This is left for the future work.

### 4.3 Ornamental algebra

Every ornament induces an *ornamental algebra* (McBride, to appear): An algebra that forgets the extra information introduced by the extensions, mapping the ornamented datatype back to its original form.

*Definition 4.13 (Cartesian morphism<sup>26</sup>)*

For an ornament  $O : \text{Orn } D u$ , there is a function – actually, a natural transformation (Dagand & McBride, 2013a) – projecting the ornamented functor down to the non-ornamented one (Figure 4). This function then lifts pointwise to ornaments:

DEFINITION

$$\text{forgetNT} : (o : \text{orn } D u) \rightarrow \llbracket o \rrbracket_{\text{orn}} (X \circ u) i \rightarrow \llbracket D \rrbracket X (u i)$$

<sup>26</sup> MODEL: Orn.Ornament.CartesianMorphism



DEFINITION		
$\text{forgetNT } (O : \text{Orn } D u)$	$(xs : \llbracket O \rrbracket_{\text{orn}} (X \circ u))$	$: \llbracket D \rrbracket X$
$\text{forgetNT } (\text{insert } S D^+)$	$(s, xs)$	$\mapsto \text{forgetNT } (D^+ s) xs$
$\text{forgetNT } (\text{var } (\text{inv } i))$	$xs$	$\mapsto xs$
$\text{forgetNT } 1$	$*$	$\mapsto *$
$\text{forgetNT } (\Pi T^+)$	$f$	$\mapsto \lambda s. \text{forgetNT } (T^+ s) (f s)$
$\text{forgetNT } (\Sigma T^+)$	$(s, xs)$	$\mapsto (s, \text{forgetNT } (T^+ s) xs)$
$\text{forgetNT } (\text{delete } s T^+)$	$xs$	$\mapsto (s, \text{forgetNT } T^+ xs)$

Fig. 4. Cartesian morphism.

*Definition 4.14 (Ornamental algebra<sup>27</sup>)*

Applied with  $\mu D$  for  $X$  and post-composed with the initial algebra  $\text{in}$ , this Cartesian morphism induces the ornamental algebra:

DEFINITION		
$\text{forgetAlg } (o : \text{orn } D u)$	$: \llbracket o \rrbracket_{\text{orn}} (\mu D \circ u) i$	$\mapsto \mu D (u i)$
$\text{forgetAlg } o$		$\mapsto \text{in } \circ (\text{forgetNT } o)$

*Definition 4.15 (Forgetful map<sup>27</sup>)*

In turn, this algebra induces a forgetful map from the ornamented type to its original form:

DEFINITION		
$\text{forget } (o : \text{orn } D u)$	$: \mu \llbracket o \rrbracket_{\text{orn}} i$	$\mapsto \mu D (u i)$
$\text{forget } o$		$\mapsto (\text{forgetAlg } o)$

where  $(\lambda (\alpha : \forall i. \llbracket D \rrbracket X i \rightarrow X i)) : \forall i. \mu D i \rightarrow X i$  denotes the catamorphism, which can be implemented in terms of induction (Chapman *et al.*, 2010).

*Example 4.16 (From lists back to natural numbers<sup>28</sup>)*

Applied to the ornament `List-Orn`, the Cartesian morphism removes the extra information added through `insert`, i.e. the inhabitant of  $A$ . The resulting algebra thus takes `nil` to `0`, and `cons a` to `suc`. In turn, the forgetful map computes the length of the list. We have (automatically) constructed the length function from Section 2.

*Example 4.17 (From the option type back to Booleans<sup>29</sup>)*

Applied to `Maybe-Orn`, the Cartesian morphism removes the  $a : A$  we attached to the constructor `true`. The forgetful map corresponds exactly to the function `isJust` (Section 2).

<sup>27</sup> MODEL: Orn.Ornament.Algebra

<sup>28</sup> MODEL: Orn.Ornament.Examples.List

<sup>29</sup> MODEL: Orn.Ornament.Examples.Maybe

Example 4.18 (From finite sets back to natural numbers<sup>30</sup>)

Applied to the ornament Fin-Orn, the Cartesian morphism removes the equations introduced by insert and forgets the indexing discipline enforced by the var code. The resulting forgetful map computes the cardinality – a natural number – of a finite set. It corresponds to the following function:

$$\begin{aligned} \text{forget Fin-Orn } (k : \text{Fin } n) & : \text{Nat} \\ \text{forget Fin-Orn } \text{f0} & \mapsto 0 \\ \text{forget Fin-Orn } (\text{fsuc } k) & \mapsto \text{suc } (\text{forget Fin-Orn } k) \end{aligned}$$

Example 4.19 (From optimised finite sets to naïve finite sets<sup>30</sup>)

When an ornament relies on a delete operation, the *forgetful* map has the – perhaps counter-intuitive – task to reintroduce the deleted information into the base datatype. To do so, it simply uses the information obtained from the index to fill-in the deleted arguments. For example, the forgetful map obtained from Fin'-Orn corresponds to the following function:

$$\begin{aligned} \text{forget Fin'-Orn } (n : \text{Nat}) (k : \text{Fin}' n) & : \text{Fin } n \\ \text{forget Fin'-Orn } (\text{suc } n) \text{ f0} & \mapsto \text{f0 } n \text{ refl} \\ \text{forget Fin'-Orn } (\text{suc } n) (\text{fsuc } k) & \mapsto \text{fsuc } n \text{ refl } (\text{forget Fin'-Orn } n k) \end{aligned}$$

where to be explicit about the origin of the recovered data, we pass the index *n* as an explicit argument.

#### 4.4 Algebraic ornaments

An important class of datatypes is constructed by *algebraic ornamentation* of a datatype. An algebraic ornament<sup>31</sup> indexes an inductive type by the result of a catamorphism over its elements. From the code  $D : \text{func } K$  and an algebra  $\alpha : \forall k. \llbracket D \rrbracket X k \rightarrow X k$ , we define the algebraic ornament, denoted  $D^\alpha$ , as the signature indexed by  $(k : K) \times X k$  that satisfies the following coherence property:

META-THEOREM

For all  $k : K$  and  $x : X k$ , we have:

$$\mu \llbracket D^\alpha \rrbracket_{\text{orn}} (k, x) \cong (t : \mu D k) \times \llbracket \alpha \rrbracket t = x \tag{4.20}$$

Seen as a refinement type, this states that  $\mu \llbracket D^\alpha \rrbracket_{\text{orn}} (k, x)$  is an inductive definition equivalent to the refinement type<sup>32</sup>  $\{t \in \mu D k \mid \llbracket \alpha \rrbracket t = x\}$ . A categorical presentation is given by Atkey *et al.* (2012), who explore the connection between refinement types and inductive families.

<sup>30</sup> MODEL: Orn.Ornament.Examples.Fin

<sup>31</sup> MODEL: Orn.AlgebraicOrnament

<sup>32</sup> Keeping with standard notations, we denote refinement types with a set comprehension. In the type theory, this amounts to a  $\Sigma$ -type.

The type-theoretic construction of  $D^\alpha$  was originally given by McBride (to appear). We shall not reiterate it here, the implementation being essentially the same. The idea is to define – by ornamentation of  $D$  – a description whose fixpoint will satisfy the above coherence property.

*Remark 4.21 (Computational interpretation)*

Constructively, the coherence property (4.20) gives us two (mutually inverse) functions, `coherentOrn` and `make  $D^\alpha$` .

The direction  $\mu \llbracket D^\alpha \rrbracket_{\text{orn}}(k, x) \rightarrow (t : \mu D k) \times (\alpha) t = x$  relies on the generic forgetful map `forget  $D^\alpha$`  to compute the first component of the pair and gives us the following theorem<sup>33</sup>:

DEFINITION

$$\text{coherentOrn} : (t^+ : \mu \llbracket D^\alpha \rrbracket_{\text{orn}}(k, x)) \rightarrow (\alpha) (\text{forget } D^\alpha t^+) = x$$

This corresponds to the `Recomputation` theorem of McBride (to appear). We shall not reprove it here, the construction being similar.

In the other direction, the isomorphism (4.20) gives us a function of type

$$(t : \mu D k) \times (\alpha) t = x \rightarrow \mu \llbracket D^\alpha \rrbracket_{\text{orn}}(k, x)$$

which, after simplifying the equation, gives a function that lifts a datatype to its algebraic version,<sup>34</sup> at the index computed by the predicate:

DEFINITION

$$\text{make } (D : \text{func } I)^{(\alpha) i. \llbracket D \rrbracket X i \rightarrow X i} : (t : \mu D k) \rightarrow \mu \llbracket D^\alpha \rrbracket_{\text{orn}}(k, (\alpha) t)$$

This corresponds to the `remember` function of McBride (to appear). Again, we will assume this construction here.

*Example 4.22 (Algebraic ornament: vectors)*

Ornamenting natural numbers to lists, we obtain an ornamental algebra: the algebra computing the length of a list. We can therefore build the algebraic ornament of lists by the length algebra.<sup>35</sup> This corresponds *exactly* to the datatype of vectors (Example 3.7): the resulting signatures are isomorphic, and both rely on constraints to enforce the indexing discipline.

Note that this operation generalises to all ornaments: any ornament induces an ornamental algebra. Therefore, we can always build the algebraic ornament by the ornamental algebra. We shall study this operation in more details in Section 4.5.

<sup>33</sup> MODEL: `Orn.AlgebraicOrnament.Coherence`

<sup>34</sup> MODEL: `Orn.AlgebraicOrnament.Make`

<sup>35</sup> MODEL: `Orn.AlgebraicOrnament.Examples.Vec`

Example 4.23 (Algebraic ornament: less-than-or-equal relation<sup>36</sup>)

For a given natural number  $m : \text{Nat}$ , the addition  $m + - : \text{Nat} \rightarrow \text{Nat}$  is obtained by folding the algebra

$$\begin{array}{lll} \text{plusAlg } (m : \text{Nat}) \text{ } (xs : \llbracket \text{Nat-func} \rrbracket \text{ Nat } *) & : & \text{Nat} \\ \text{plusAlg } m & (\text{'0, *}) & \mapsto m \\ \text{plusAlg } m & (\text{'suc, n}) & \mapsto \text{suc } n \end{array}$$

By ornamenting  $\text{Nat}$  by this algebra, we obtain the relation  $m \leq - : \text{Nat} \rightarrow \text{SET}$  that is characterised by the isomorphism

$$m \leq n \cong (k : \text{Nat}) \times m + k = n$$

Put explicitly, the datatype computed by the algebraic ornament corresponds to

$$\begin{array}{ll} \text{data } [m : \text{Nat}] \leq (n : \text{Nat}) : \text{SET} \text{ where} & \\ m \leq (n = m) & \ni 0 \\ m \leq (n = \text{suc } n') & \ni \text{suc } (k : m \leq n') \end{array}$$

Example 4.24 (Algebraic ornament: indexing by semantics<sup>37</sup>)

A typical use-case of algebraic ornaments is the implementation of semantic-preserving operations (McBride, to appear). For example, let us consider arithmetic expressions whose semantics is given by interpretation to  $\text{Nat}$ :

$$\begin{array}{lll} \text{data Expr} : \text{SET} \text{ where} & \text{evalAlg } (es : \llbracket \text{Expr-func} \rrbracket \text{ Nat } *) & : \text{Nat} \\ \text{Expr } \ni \text{const } (n : \text{Nat}) & \text{evalAlg } (\text{'const, } n) & \mapsto n \\ \quad | \text{add } (d : \text{Expr})(e : \text{Expr}) & \text{evalAlg } (\text{'add, } (m, n)) & \mapsto m + n \end{array}$$

Using the algebra  $\text{evalAlg}$ , we construct the algebraic ornament of  $\text{Expr}$  and obtain expressions indexed by their semantics:

$$\begin{array}{ll} \text{data Expr}^{\text{evalAlg}} (k : \text{Nat}) : \text{SET} \text{ where} & \\ \text{Expr}^{\text{evalAlg}} (k = n) & \ni \text{const } (n : \text{Nat}) \\ \text{Expr}^{\text{evalAlg}} (k = m + n) & \ni \text{add } (m n : \text{Nat})(d : \text{Expr}^{\text{evalAlg}} m)(e : \text{Expr}^{\text{evalAlg}} n) \end{array}$$

We can now enforce the preservation of semantics by typing. For example, let us optimise away all additions of the form  $'0 + e$ :

$$\begin{array}{lll} \text{optimise-0+ } (e : \text{Expr}^{\text{evalAlg}} n) & : & \text{Expr}^{\text{evalAlg}} n \\ \text{optimise-0+ } (\text{const } n) & \mapsto & \text{const } n \\ \text{optimise-0+ } (\text{add } 0 n d e) & \mapsto & \text{optimise-0+ } e \\ \text{optimise-0+ } (\text{add } (\text{suc } m) n d e) & \mapsto & \text{add } (\text{suc } m) n d e \end{array}$$

Since the type checker accepts our definition, we have that, by construction, this operation preserves the semantics. We can then prune the semantics from the types using the forgetful map and retrieve the transformation on raw syntax trees. The `make` function (Remark 4.21) lets us lift raw syntax trees to semantically indexed ones, while the `coherentOrn` theorem (Remark 4.21) certifies that the pruned tree satisfies the invariant we enforced by indexing.

<sup>36</sup> MODEL: Orn.AlgebraicOrnament.Examples.Leq

<sup>37</sup> MODEL: Orn.AlgebraicOrnament.Examples.Expr

### 4.5 Reornaments

In this paper, we are particularly interested in a subclass of algebraic ornaments. In Definition 4.14, we have constructed, for an ornament  $o$ , its ornamental algebra  $\text{forgetAlg } o$  that forgets the extra information introduced by the ornament. As hinted at in Example 4.22, given an ornament  $o$ , we can always algebraically ornament  $\llbracket o \rrbracket_{\text{orn}}$  using the ornamental algebra  $\text{forgetAlg } o$ . McBride (to appear) calls this construction the *algebraic ornament by the ornamental algebra*.

*Remark 4.25 (Notation)*

We write  $\lceil o \rceil$  to denote the algebraic ornament of  $o$  by the ornamental algebra. For brevity, we call it the *reornament* of  $o$ .

*Example 4.26 (Reornament: vectors)*

Paraphrasing Example 4.22, we have that vectors are a reornament of List-Orn. Explicitly, a vector is the algebraic ornament of List by the algebra computing its length, i.e. the ornamental algebra from List to Nat.

*Example 4.27 (Reornament: indexed option type)*

In Example 4.5, we have ornamented the Booleans to the option type. We can thus reornament the option type with its Boolean status. Unfolding the definition of the reornament, we obtain the  $\text{IMaybe } A$  datatype that was introduced in Section 2. The function  $\text{forgetIMaybe}$  corresponds to the left-to-right reading of the isomorphism (4.20) specialised to the Maybe ornament.

Reornaments are thus straightforwardly obtained through a two-step process: first, compute the ornamental algebra, and second, construct the algebraic ornament by this algebra. However, such a simplistic construction introduces a lot of spurious equality constraints and duplication of information. For instance, using this naive definition of reornaments, a vector indexed by  $n$  is constructed as *any list as long as it is of length  $n$* .

*Example 4.28 (Reornamenting vectors, efficiently)*

Let us consider the ornament List-Orn, taking natural numbers to lists. We gave its code in Example 4.7. Here, for simplicity, we shall work on the following variant

$$\begin{array}{l} \text{List-Orn } (A : \text{SET}) : \text{orn Nat-func id} \\ \text{List-Orn } A \quad \mapsto \lambda*. \Sigma \left\{ \begin{array}{l} '0 \mapsto 1 \\ 'suc \mapsto \text{insert } A \lambda - . \text{var } (\text{inv } *) \end{array} \right\} \end{array}$$

which does not update the constructor names, allowing us to focus on essential steps.

We can adopt a more fine-grained approach yielding an isomorphic but better structured datatype. In our setting, where we can compute over the index, a finer construction of the reornament of List-Orn is as follows:

- We retrieve the index, hence obtaining a number  $n : \text{Nat}$ .
- By inspecting the ornament List-Orn, we obtain the *exact* relationship between the index  $n$  and its ornament describing lists.

DEFINITION

$\llbracket (O : \text{Orn } Du) \rrbracket (xs : \llbracket D \rrbracket (\mu E))$	$: \text{Orn } \llbracket O \rrbracket_{\text{orn}} (\pi_0 : (i : I) \times \mu E (ui) \rightarrow I)$
$\llbracket \text{insert } S D^+ \rrbracket$	$xs \mapsto \Sigma \lambda s. \llbracket D^+ s \rrbracket xs$
$\llbracket \text{var (inv } i) \rrbracket$	$xs \mapsto \text{var (inv (} i, xs))$
$\llbracket 1 \rrbracket$	$* \mapsto 1$
$\llbracket \Pi T^+ \rrbracket$	$f \mapsto \Pi \lambda s. \llbracket T^+ s \rrbracket (f s)$
$\llbracket \Sigma T^+ \rrbracket$	$(s, xs) \mapsto \text{delete } s (\llbracket T^+ s \rrbracket xs)$
$\llbracket \text{delete } s T^+ \rrbracket$	$(s', xs) \mapsto \text{insert (} s = s') \lambda -. \llbracket T^+ \rrbracket xs$

Fig. 5. Reornament.

- If  $n = 0$ , we are in the first branch of the  $\Sigma$  code, and the ornamentation of  $n$  is necessarily the empty list. The corresponding reornament can therefore delete the choice of constructor (since it is entirely determined by the index), set it to  $\text{'}0$ , and terminate immediately:

$$\llbracket \text{List-Orn } A * \rrbracket (\text{'}0, *) \rightsquigarrow \text{delete '}0 1$$

- If  $n = \text{suc } n'$ , we are in the second branch of the  $\Sigma$  code, and the ornament of  $\text{suc } n'$  is necessarily a non-empty list. Again, the corresponding reornament deletes the choice of constructor by deducing from the index that it must be  $\text{'}cons$ . Since the list ornament extends natural numbers with an argument of type  $A$  (through the  $\text{insert}$  code), we must preserve this information in the reornament (through a  $\Sigma$  code). Finally, we index the recursive argument of the reornamented datatype by  $n'$ :

$$\llbracket \text{List-Orn } A * \rrbracket (\text{'suc } n') \rightsquigarrow \text{delete 'suc } (\Sigma \lambda a. \text{var (inv (*, } n')))$$

Altogether, we have ornamented lists by their length: When the index is  $0$ , the ornamented list is empty; when the index is  $\text{suc } n'$ , the ornamented list is non-empty and takes an argument indexed by  $n'$ . We have effectively described the datatype of vectors.

*Definition 4.29 (Reornament)<sup>38</sup>*

A reornament (Figure 5) is thus defined over an ornament code  $O : \text{Orn } Du$  (for some description  $D : \text{IDesc } I$ ) and an index belonging to the base datatype  $xs : \llbracket D \rrbracket (\mu D)$ . On  $1$  and  $\Pi$  codes, the reornament simply mirrors the underlying ornament while peeling off the index: the *structure* of the three datatypes is identical. On a  $\text{var}$  code, the reornament also duplicates the underlying structure by pairing the index of the ornament (provided by the index  $i$ ) with the recursive argument of the base datatype (provided by the argument  $xs$ ). On an  $\text{insert}$  code, the reornament preserves the extra information introduced by the ornament since it is absent from the index. However, on a  $\Sigma$  code, the ornament is merely duplicating information already

<sup>38</sup> MODEL: `Orn.Reornament`

provided by  $xs$ : in this case, we delete the argument, filling in the gap with the data provided by the index  $xs$ . On a `delete` code, we make sure – through an equality constraint – that the index  $xs$  is in sync with the data deleted by the ornament.

This definition over codes then lifts pointwise to ornaments:

DEFINITION

$$\begin{aligned} \llbracket (o : \text{orn } D u) \rrbracket & : \text{orn } \llbracket o \rrbracket_{\text{orn}} (\pi_0 : (i : I) \times \mu D (u i) \rightarrow I) \\ \llbracket o \rrbracket & \mapsto \lambda(i, \text{in } xs). \llbracket o i \rrbracket xs \end{aligned}$$

*Example 4.30 (Reornament: vectors<sup>39</sup>)*

Applied to the ornament `List-Orn` (Example 4.7), this construction gives the fully Brady-optimised – detagged and forced – version of `vectors` (Example 3.8). That is, we determine which constructor of `Vec` is available by pattern-matching on the index. This is unlike the naive reornament (Example 4.26), which relies on constraints to enforce the indexing discipline.

*Example 4.31 (Reornament: indexed option type<sup>40</sup>)*

Under this definition, the reornament of `Maybe-Orn` (Example 4.5) describes the datatype

```
data IMaybe [A : SET](b : Bool) : SET where
  IMaybe A true  ⊃ just (a : A)
  IMaybe A false ⊃ nothing
```

where, similarly, constraints are offloaded by pattern-matching on the indices (Example 3.8). Again, this must be compared with the definition obtained through the naive construction (Example 4.27), where we relied on constraints.

Note that our ability to *compute* over indices is crucial for this construction to work. Also, the datatypes that we obtain are isomorphic to the datatypes one would have obtained by the algebraic ornament of the ornamental algebra, i.e.:

META-THEOREM

For all ornament  $o : \text{orn } D u$ , we have

$$\llbracket \llbracket o \rrbracket \rrbracket_{\text{orn}} \cong \llbracket \llbracket o \rrbracket_{\text{orn}}^{\text{forgetAlg } o} \rrbracket_{\text{orn}}$$

*Remark 4.32 (Computational interpretation)*

Consequently, the coherence property of algebraic ornaments (Equation 4.20) is still valid. Constructively, this isomorphism gives the `coherentOrn` theorem<sup>41</sup> in one direction and the `make` function<sup>42</sup> in the other.

<sup>39</sup> MODEL: Orn.Reornament.Examples.List

<sup>40</sup> MODEL: Orn.Reornament.Examples.Maybe

<sup>41</sup> MODEL: Orn.Reornament.Coherence

<sup>42</sup> MODEL: Orn.Reornament.Make

*Remark 4.33 (Iterating reornamentation<sup>43</sup>)*

Every ornament induces a reornament. A reornament is itself an ornament: it therefore induces yet another reornament. We are naturally led to wonder if this process ever stops, and if so, then when. For example, the ornament of natural numbers into lists reornaments to vectors. Reornamenting vectors, we obtain an inductive predicate representing the length function  $\text{Length} : \text{Nat} \rightarrow \text{List } A \rightarrow \text{SET}$ . Reornamenting  $\text{Length}$  leads to an object with no computational content: all its information has been erased and is provided by the indices.

The same pattern arises in general: every chain of reornaments is bound to end with a computationally trivial object. We deduce this from our massaged definition of reornaments (Definition 4.29). To illustrate our reasoning, we simultaneously iterate the reornamentation of the following (artificial) ornament indexed by  $n : \text{Nat}$

$$\begin{aligned} o & : \text{orn } D (\lambda n. *) \\ o & \mapsto \lambda n. \Sigma \lambda a. \text{insert } C \lambda c. \Pi \lambda b. \text{delete true (var (suc } n)) \end{aligned}$$

which ornaments the description

$$\begin{aligned} D & : \text{func } \mathbb{1} \\ D & \mapsto \lambda *. \Sigma A \lambda a. \Pi B \lambda b. \Sigma \text{Bool } \lambda x. \text{var } * \end{aligned}$$

where  $A$ ,  $B$ , and  $C$  are sets.

We proceed by case analysis on the ornament. On a  $\mathbb{1}$ ,  $\Pi$ , and  $\text{var}$  code, the reornamentation proceeds purely structurally, merely duplicating the ornament's code and introducing no information (Definition 4.29, the first three cases). The reornamentation *deletes*  $\Sigma$  codes, using the indexing information (Definition 4.29, the fourth case). On a  $\text{delete}$  code, the reornament inserts an equality constraint (Definition 4.29, the sixth case), which contains no information *per se*: it is only enforcing the indexing discipline. Only on an  $\text{insert}$  code does the reornament introduce new information through a  $\Sigma$  code (Definition 4.29, the fifth case). In our example, the first reornament is defined by

$$\begin{aligned} o^+ & : \text{orn } (\llbracket o \rrbracket_{\text{orn}} : \text{func Nat}) \pi_0 \\ o^+ & \mapsto [o] \end{aligned}$$

and unfolds to

$$\begin{aligned} o^+ & \rightsquigarrow \lambda(n, \text{in } (a, f)). \\ & \text{delete } a (\Sigma C \lambda c. \Pi \lambda b. \text{insert (true = } \pi_0 (f b)) \lambda - . \text{var (inv (suc } n, \pi_1 (f b)))) \end{aligned}$$

In the subsequent iteration, these  $\Sigma$  codes in the reornament are in turn deleted by the re-reornament. In our example, the second reornamentation is defined by

$$\begin{aligned} o^{++} & : \text{orn } (\llbracket o^+ \rrbracket_{\text{orn}} : \text{Nat} \times \mu D *) \pi_0 \\ o^{++} & \mapsto [o^+] \end{aligned}$$

<sup>43</sup> MODEL: Orn.Reornament.Examples.Iterative



and unfolds to

$$o^{++} \rightsquigarrow \lambda((n, \text{in } (a, f)), \text{in } (a', (c, f^+))).$$

$$\text{insert } (a' = a) \lambda - . \text{delete } c (\Pi \lambda b. \Sigma \lambda q.$$

$$\text{var } (\text{inv } ((\text{suc } n, \pi_1 (f b)), f^+ b))$$

where the  $\Sigma$  code duplicates the (computationally trivial) equation on  $x$ , i.e.  $\text{true} = x$ .

In the third iteration, there is nothing left in the code but equations and structural scaffoldings (in the form of  $\text{var}$ ,  $1$ , and  $\Pi$  codes): the resulting datatype is computationally trivial and is entirely determined by its indices. On our example, the third reornamentation is defined by

$$o^{+++} : \text{orn } ([o^{++}]_{\text{orn}} : \text{func } (n : \text{Nat}) \times \mu D * \times \mu [o]_{\text{orn}} n) \pi_0$$

$$o^{+++} \mapsto [o^{+++}]$$

and unfolds to

$$o^{+++} \rightsquigarrow \lambda(((n, \text{in } (a, f)), \text{in } (a, (c, f^+))), \text{in } (c', f^{++})).$$

$$\Sigma \lambda q_1. \text{insert } (c' = c) \lambda q_2. \Pi \lambda b. \text{delete refl}$$

$$(\text{var } (\text{inv } (((\text{suc } n, \pi_1 (f b)), f^+ b), \pi_1 (f^{++} b))))$$

where the  $\Sigma$  code duplicates the (computationally trivial) equation on  $a$ , i.e.  $a' = a$ .

Formally, we have that any two inhabitants of a triple reornament are provably equal:

META-THEOREM

Let  $o : \text{orn } D u$  be an ornament.

Let

1.  $i : I$
2.  $ds : \mu D (u i)$
3.  $os : \mu [o]_{\text{orn}} i$
4.  $os^+ : \mu [[o]]_{\text{orn}} (i, ds)$

be some indices.

For any pair

1.  $xs : \mu [[[[[o]]]]]_{\text{orn}} (((i, ds), os), os^+)$
2.  $ys : \mu [[[[[o]]]]]_{\text{orn}} (((i, ds), os), os^+)$

We have:

$$xs \cong ys$$

In this section, we have adapted ornaments to our universe of datatypes. In doing so, we have introduced deletion ornaments, which rely on indexing to remove duplicated information from the datatypes. We shall see in Section 6, how this more careful definition can be turned to our advantage when we transport functions across ornaments.

## 5 A Universe of function types and their ornaments

Ornaments provide us with a calculus of data-structures: from a given inductive family, we can ornament it to as many similarly structured datatypes. The universe of ornaments is essentially an intensional characterisation of such structure-preserving transformation of datatype. Functional ornaments *build upon* ornaments (but not exclusively, as discussed in Remark 5.2), relying on them to capture the structural ties between the types of two functions, a base function and its lifting.

In that sense, the functional ornaments presented in this paper are a generalisation of ornaments to function types. To describe them, we first need to be able to, intensionally and in the type theory, manipulate function types. We thus define a universe of function types (Section 5.1). With it, we will be able to write generic programs over the class of functions captured by this universe. We define a functional ornament as a decoration over this universe (Section 5.2). The liftings implementing the functional ornament are related to the base function by a coherence property. To minimise the theorem-proving burden induced by coherence proofs, we expand our system with patches (Section 5.3): A patch is the type of the functions that satisfy the coherence property *by construction*. Finally, we show how we can project the lifting and its coherence certificate out of a patch (Section 5.4).

### 5.1 A universe of function types

*Definition 5.1 (Universe of types<sup>44</sup>)*

For clarity of exposition, we restrict our language of types to the bare minimum: A type can either be an exponential whose domain is an inductive type, or a product whose first component is an inductive type, or the unit type – used as a termination marker:

DEFINITION

**data** Type : SET<sub>1</sub> **where**

$$\begin{aligned} \text{Type} \ni & \mu_k^l(D : \text{func } K) \cdot (k : K) \} \rightarrow (T : \text{Type}) \\ & | \mu_k^l(D : \text{func } K) \cdot (k : K) \} \times (T : \text{Type}) \\ & | 1 \end{aligned}$$

This universe codes the function space from some (maybe none) inductive types to some (maybe none) inductive types. Concretely, the codes are interpreted as follows:

<sup>44</sup> MODEL: FunOrn.Functions

## DEFINITION

$$\begin{aligned}
\llbracket (T : \text{Type}) \rrbracket_{\text{Type}} & : \text{SET} \\
\llbracket \mu\{D \cdot k\} \rightarrow T \rrbracket_{\text{Type}} & \mapsto \mu D k \rightarrow \llbracket T \rrbracket_{\text{Type}} \\
\llbracket \mu\{D \cdot k\} \times T \rrbracket_{\text{Type}} & \mapsto \mu D k \times \llbracket T \rrbracket_{\text{Type}} \\
\llbracket \mathbb{1} \rrbracket_{\text{Type}} & \mapsto \mathbb{1}
\end{aligned}$$

*Remark 5.2 (Extensions)*

The constructions we develop next could be adapted to a more powerful universe – such as the one supporting higher-order functions, non-inductive parameters, or including dependent quantifiers. However, this would needlessly complicate our exposition.

For instance, the treatment of non-inductive parameters would lead to further, but orthogonal, extensions of the functional ornaments, namely, inserting or deleting these quantifiers during functional ornamentation. To support higher-order functions, we have to distinguish the variance of ornamentations, a technicality that we can simply overlook in the first-order system.

*Example 5.3 (Coding  $- < -$ <sup>45</sup>)*

Written in the universe of function types, the type of the comparison function is

$$\begin{aligned}
\text{type} < & : \text{Type} \\
\text{type} < & \mapsto \mu\{\text{Nat-func} \cdot *\} \rightarrow \mu\{\text{Nat-func} \cdot *\} \rightarrow \mu\{\text{Bool-func} \cdot *\} \times \mathbb{1}
\end{aligned}$$

The implementation of  $- < -$  is essentially the same as earlier excepted that it ought to return a pair of a Boolean and the inhabitant of the unit type. To reduce the syntactic noise introduced by this trivial multiplication by the unit, we assume that the type isomorphisms  $A \times \mathbb{1} \cong \mathbb{1} \times A \cong A$  are definitionally true: we spare ourselves from writing pairs with unit, and projections out of such pairs. Again, we refer our reader to the companion Agda code for the non-simplified terms.

To be explicit about the recursion pattern of this function, we make use of Epigram's *by* ( $\Leftarrow$ ) gadget:

$$\begin{aligned}
- & < - & : \llbracket \text{type} < \rrbracket_{\text{Type}} \\
m & < n & \Leftarrow \text{Nat-elim } n \\
m & < 0 & \mapsto \text{false} \\
m & < (\text{suc } n) & \Leftarrow \text{Nat-case } m \\
0 & < (\text{suc } n) & \mapsto \text{true} \\
(\text{suc } m) & < (\text{suc } n) & \mapsto m < n
\end{aligned}$$

That is, we first do induction on  $n$  and then, in the successor case, we proceed by case analysis over  $m$ .

<sup>45</sup> MODEL: FunOrn.Functions.Examples.Le

Example 5.4 (Coding  $- + -$ <sup>46</sup>)

In the universe of function types, the type of addition is given by

```
type+ : Type
type+ ↦ μ{Nat-func · *} ↦ μ{Nat-func · *} ↦ μ{Nat-func · *} × 1
```

Again, up to a trivial multiplication by  $\mathbb{1}$ , the implementation of  $- + -$  is left unchanged:

```

-      + - : [[type+]]_Type
m      + n ← Nat-elim m
0      + n ↦ n
(suc m) + n ↦ suc (m + n)

```

That is, it is defined by induction over  $m$ .

### 5.2 Functional ornament

It is now straightforward to define functional ornaments: We traverse the function type and ornament the inductive types as we go. Note that it is always possible to leave an object non-ornamented: we ornament by the identity (Example 4.9), which simply copies the original description.

Definition 5.5 (Universe of functional ornaments<sup>47</sup>)

Following this intuition, we define functional ornaments by the following grammar:

DEFINITION

```

data FunOrn (T : Type) : SET1 where
  FunOrn (μ{D · k} → T) ⊃ ∀ u : I → K. μ+{(o : orn D u) · (i : u-1 k)} → (T+ : FunOrn T)
  FunOrn (μ{D · k} × T) ⊃ ∀ u : I → K. μ+{(o : orn D u) · (i : u-1 k)} × (T+ : FunOrn T)
  FunOrn 1 ⊃ 1

```

Definition 5.6 (Lifting type<sup>47</sup>)

We get the type of the liftings by interpreting the ornaments as we traverse the functional ornament:

DEFINITION

```

[[ (T+ : FunOrn T) ]]_FunOrn : SET
[[ μ+{o · inv i} → T+ ]]_FunOrn ↦ μ [[o]]_orn i → [[T+]]_FunOrn
[[ μ+{o · inv i} × T+ ]]_FunOrn ↦ μ [[o]]_orn i × [[T+]]_FunOrn
[[ 1 ]]_FunOrn ↦ 1

```

<sup>46</sup> MODEL: FunOrn.Functions.Examples.Plus

<sup>47</sup> MODEL: FunOrn.FunOrnament

We want the ornamented function to be *coherent* with respect to the base function we started from: For a function  $f : \mu D k \rightarrow \mu E l$ , the ornamented function  $f^+$  of type  $\mu \llbracket o_D \rrbracket_{\text{orn}} i \rightarrow \mu \llbracket o_E \rrbracket_{\text{orn}} j$  is said to be coherent with  $f$  if the following diagram commutes:

$$\begin{array}{ccc}
 \mu \llbracket o_D \rrbracket_{\text{orn}} i & \xrightarrow{f^+} & \mu \llbracket o_E \rrbracket_{\text{orn}} j \\
 \text{forget } o_D \downarrow & & \downarrow \text{forget } o_E \\
 \mu D (u_i) & \xrightarrow{f} & \mu E (v_j)
 \end{array}$$

or, equivalently in type theory:

$$(x^+ : \mu \llbracket o_D \rrbracket_{\text{orn}} i) \rightarrow f (\text{forget } o_D x^+) = \text{forget } o_E (f^+ x^+)$$

This captures our intuition that the lifted function  $f^+$  behaves like the base function  $f$ , only that it also carries the extra-information introduced by the ornament  $o_D$  over to the ornament  $o_E$ . Coherence states that this extra step does not interfere with its core operational behaviour, which is specified by  $f$ .

*Definition 5.7 (Coherence<sup>48</sup>)*

This definition of coherence generalises to any arity. We define it by induction over the code of functional ornaments:

DEFINITION

$\text{Coherence } (T^+ : \text{FunOrn } T) (f : \llbracket T \rrbracket_{\text{Type}}) (f^+ : \llbracket T^+ \rrbracket_{\text{FunOrn}}) : \text{SET}$   
 $\text{Coherence } (\mu^+\{o \cdot \text{inv } i\} \rightarrow T^+) \quad f \quad f^+ \quad \mapsto$   
 $(x^+ : \mu \llbracket o \rrbracket_{\text{orn}} i) \rightarrow \text{Coherence } T^+ (f (\text{forget } o x^+)) (f^+ x^+)$   
 $\text{Coherence } (\mu^+\{o \cdot \text{inv } i\} \times T^+) (x, xs) (x^+, xs^+) \mapsto$   
 $\text{forget } o x^+ = x \times \text{Coherence } T^+ xs xs^+$   
 $\text{Coherence } \quad 1 \quad * \quad * \quad \mapsto \mathbb{1}$

*Example 5.8 (Ornamenting type< to describe lookup<sup>49</sup>)*

In Section 2, we have identified the ornaments taking the type of  $-<-$  to the type of lookup. We ornament  $\text{Nat}$  to  $\text{List } A$  (Example 4.7), and  $\text{Bool}$  to  $\text{Maybe } A$  (Example 4.5). From there the functional ornament describing the type of the lookup function is as follows:

$$\begin{aligned}
 \text{typeLookup} & : \text{FunOrn type} < \\
 \text{typeLookup} & \mapsto \mu^+\{\text{idO Nat-func} \cdot \text{inv } * \} \rightarrow \\
 & \mu^+\{\text{List-Orn } A \cdot \text{inv } * \} \rightarrow \mu^+\{\text{Maybe-Orn } A \cdot \text{inv } * \} \times 1
 \end{aligned}$$

<sup>48</sup> MODEL: FunOrn.FunOrnament

<sup>49</sup> MODEL: FunOrn.FunOrnament.Examples.Lookup

We leave it to the reader to verify that  $\llbracket \text{typeLookup} \rrbracket_{\text{FunOrn}}$  unfolds to the type of the lookup function up to a multiplication by  $\mathbb{1}$ . Also, unfolding the coherence condition gives the desired property:

$$\begin{aligned} \text{Coherence typeLookup } (- < -) &\rightsquigarrow \lambda f^+ : \llbracket \text{typeLookup} \rrbracket_{\text{FunOrn}}. \\ (n : \text{Nat})(xs : \text{List } A) &\rightarrow \text{isJust } (f^+ n xs) = n < \text{length } xs \end{aligned}$$

*Remark 5.9*

This equation is not *specifying* the lookup function: it is only establishing a computational relation between  $- < -$  and a candidate lifting  $f^+$ , for which lookup is a valid choice. However, one could be interested in other functions satisfying this coherence property and they would be handled by our system just as well: the notion of functional ornament (Definition 5.5), and its coherence property (Definition 5.7) still apply. For example, assuming that  $A$  is a monoid, a function that sums the elements of  $\text{List } A$  from 0 to the index  $n$ , or returns nothing if the index is out of bound is coherent with  $- < -$ .

*Example 5.10 (Ornamenting type+ to describe - ++ -<sup>50</sup>)*

The functional ornament of  $\text{type}+$  relies solely on the ornamentation of  $\text{Nat}$  into  $\text{List } A$ :

$$\begin{aligned} \text{type}++ & : \text{FunOrn type}+ \\ \text{type}++ & \mapsto \mu^+\{\text{List-Orn } A \cdot \text{inv } *\} \rightarrow \mu^+\{\text{List-Orn } A \cdot \text{inv } *\} \rightarrow \mu^+\{\text{List-Orn } A \cdot \text{inv } *\} \times 1 \end{aligned}$$

Again, we check that unfolding  $\llbracket \text{type}++ \rrbracket_{\text{FunOrn}}$  gives the type of  $- ++ -$  while the coherence condition  $\text{Coherence type}++ (- + -)$  correctly captures our requirement that appending lists preserve their lengths. As before, the list-append function is not the only valid lifting: one could, for example, consider a function that reverses the first list and appends it to the second one.

### 5.3 Patches

The coherence of the lifting  $f^+ : \llbracket T^+ \rrbracket_{\text{FunOrn}}$  of a base function  $f : \llbracket T \rrbracket_{\text{Type}}$  is therefore captured by the coherence predicate  $\text{Coherence } T^+ f$ . To implement a lifting that is coherent, we might ask the user to first implement the lifting  $f^+$  and then prove its coherence. However, we find this process unsatisfactory: We fail to harness the power of dependent types when implementing  $f^+$ , this weakness being then paid off by tedious proof obligations. To overcome this limitation, we define the notion of  $\text{Patch}$  as the type of *all* the functions that are coherent by construction.

*Remark 5.11*

We are looking for an isomorphism here: We will define patches in such a way that they are in bijection with the liftings satisfying a coherence property. Put otherwise, we want that:

$$\text{Patch } T T^+ f \cong (f^+ : \llbracket T^+ \rrbracket_{\text{FunOrn}}) \times \text{Coherence } T^+ f f^+$$

<sup>50</sup> MODEL: FunOrn.FunOrnament.Examples.Append

In this paper, we constructively exploit this bijection in the left-to-right direction: having implemented a patch  $f^{++}$  of type  $\text{Patch } T \ T^+ \ f$ , we show how we can ‘apply’ it, and extract a lifting together with its coherence proof.

*Example 5.12 (Patching  $- < -$ )*

Before giving the general construction of a  $\text{Patch}$ , let us first work through our running example. After having functionally ornamented  $- < -$  with  $\text{typeLookup}$ , the lifting function  $f^+$  and coherence property can be represented by the following commuting diagram:

$$\begin{array}{ccccc}
 \text{Nat} & \times & \text{List } A & \xrightarrow{f^+} & \text{Maybe } A \\
 \text{id} \parallel & & \text{length} \downarrow & & \downarrow \text{isJust} \\
 \text{Nat} & \times & \text{Nat} & \xrightarrow{- < -} & \text{Bool}
 \end{array} \tag{5.13}$$

In the type theory, this is written as

$$(f^+ : \text{Nat} \times \text{List } A \rightarrow \text{Maybe } A) \times \\
 (m : \text{Nat})(as : \text{List } A) \rightarrow \text{isJust } (f^+ \ m \ as) = m < \text{length } as$$

Applying intensional choice, this is isomorphic to

$$\cong (m : \text{Nat}) \times (n : \text{Nat}) \times (as : \text{List } A) \times \text{length } as = n \rightarrow \\
 (ma : \text{Maybe } A) \times \text{isJust } ma = m < n$$

Now, by the characterisation of reornaments (Equation 4.20), we have that:

$$\begin{aligned}
 (as : \text{List } A) \times \text{length } as = n &\cong \text{Vec } A \ n && \text{and} \\
 (ma : \text{Maybe } A) \times \text{isJust } ma = b &\cong \text{IMaybe } A \ b
 \end{aligned}$$

Applying these isomorphisms, we obtain the following type, which we call the  $\text{Patch}$  of the functional ornament  $\text{typeLookup}$ :

$$\cong (m : \text{Nat}) \rightarrow (n : \text{Nat}) \times (vs : \text{Vec } A \ n) \rightarrow \text{IMaybe } A \ (m < n)$$

This last type is thus isomorphic to the pair of a lifting and its coherence proof.

Intuitively, the  $\text{Patch}$  construction amounts to turning the vertical arrows of the commuting diagram (5.13) into equivalent reornaments. In type-theoretic terms, it turns the pairs of datatypes and their algebraically defined constraints into the equivalent reornaments. The coherence property of reornaments (Equation 4.20) tells us that projecting the ornamented function down to its non-ornamented components gives back the base function. By turning the projection functions into inductive datatypes, we enforce the coherence property directly by the index: We introduce a fresh index for the arguments (in Example 5.12, introducing  $m$  and  $n$ ) and index

the return types by the result of the non-ornamented function (in Example 5.12, indexing  $\text{IMaybe } A$  by the result  $m < n$ ).

*Remark 5.14 (Terminology)*

The name of ‘patch’ comes from the idea that the Patch type  $\text{Patch } T T^+ f$  captures all those (coherent) functions that *extends* the base function  $f$ . In Section 5.4, we shall see how such a patch can be *applied* (Definition 5.22), i.e. we describe how a base function is patched by an inhabitant of a Patch type to build its coherent lifting.

*Definition 5.15 (Patch type<sup>51</sup>)*

We define the Patch type generically by induction over the functional ornament. Upon an argument (i.e. a code  $\mu^+\{o \cdot \text{inv } i\} \rightarrow$ ), we introduce a fresh index and the reornament of  $o$ . Upon a result (i.e. a code  $\mu^+\{o \cdot \text{inv } i\} \times$ ), we ask for a reornament of  $o$  indexed by the result of the base function.

DEFINITION

$$\begin{array}{l}
 \text{Patch } (T : \text{Type}) \quad (T^+ : \text{FunOrn } T) \quad (f : \llbracket T \rrbracket_{\text{Type}}) : \text{SET} \\
 \text{Patch } (\mu\{D \cdot u\} i \rightarrow T) \quad (\mu^+\{o \cdot \text{inv } i\} \rightarrow T^+) \quad f \quad \mapsto \\
 \quad (x : \mu D (u i)) \rightarrow \mu \llbracket [o] \rrbracket_{\text{orn}} (i, x) \rightarrow \text{Patch } T T^+ (f x) \\
 \text{Patch } (\mu\{D \cdot u\} i \times T) \quad (\mu^+\{o \cdot \text{inv } i\} \times T^+) \quad (x, xs) \quad \mapsto \\
 \quad \mu \llbracket [o] \rrbracket_{\text{orn}} (i, x) \times \text{Patch } T T^+ xs \\
 \text{Patch} \quad 1 \quad 1 \quad * \quad \mapsto \mathbb{1}
 \end{array}$$

*Example 5.16 (Patch of typeLookup<sup>52</sup>)*

The type of the coherent liftings of  $- < -$  by `typeLookup`, as defined by the Patch of  $- < -$  by `typeLookup`, unfolds to

$$\begin{array}{l}
 (m : \text{Nat})(m^+ : \mu \llbracket [\text{idO Nat-func}] \rrbracket_{\text{orn}} m) \rightarrow \\
 (n : \text{Nat})(vs : \mu \llbracket [\text{List } A] \rrbracket_{\text{orn}} n) \rightarrow \mu \llbracket [\text{Maybe } A] \rrbracket_{\text{orn}} (m < n) \times \mathbb{1}
 \end{array}$$

*Remark 5.17*

$\mu \llbracket [\text{idO Nat-func}] \rrbracket_{\text{orn}} m$  is isomorphic to  $\mathbb{1}$ : all the content of the datatype has been forced – the recursive structure of the datatype is entirely determined by its index – and detagged – the choice of constructors is entirely determined by its index, leaving no actual data in it. Being computationally uninteresting, we ignore this argument. On the other hand,  $\llbracket [\text{List } A] \rrbracket$  and  $\llbracket [\text{Maybe } A] \rrbracket$  are, respectively, the previously introduced vectors (Example 4.30) and indexed option (Example 4.31) types.

<sup>51</sup> MODEL: FunOrn.Patch

<sup>52</sup> MODEL: FunOrn.Patch.Examples.Lookup



Example 5.18 (Patch of type+<sup>53</sup>)

Similarly, the Patch of  $- + -$  by type+ unfolds to the type of the vector append function

$$(m : \text{Nat})(xs : \mu \llbracket \text{List } A \rrbracket_{\text{orn}} m) \rightarrow (n : \text{Nat})(ys : \mu \llbracket \text{List } A \rrbracket_{\text{orn}} n) \rightarrow \mu \llbracket \text{List } A \rrbracket_{\text{orn}} (m + n) \times \mathbb{1}$$

where, again, the datatype  $\mu \llbracket \text{List } A \rrbracket_{\text{orn}}$  corresponds exactly to vectors.

Theorem 5.19

Following our Remark 5.11, we have that a Patch is isomorphic to the pair of a lifting and its coherence proof:

— META-THEOREM —

For any function type  $T : \text{Type}$ , any functional ornament  $T^+ : \text{FunOrn } T$  of  $T$ , and any base function  $f : \llbracket T \rrbracket_{\text{Type}}$ , we have:

$$\text{Patch } T \ T^+ \ f \ \cong \ (f^+ : \llbracket T^+ \rrbracket_{\text{FunOrn}}) \times \text{Coherence } T^+ \ f \ f^+$$

That is, our definition of the Patch type enforces that its inhabitants are exactly those liftings that are coherent by construction.

*Proof*

For clarity, we shall only write the proof for arity one. The generalisation to multiple input and output arities is straightforward but laboriously verbose. So from a base function  $f : \mu D \ k \rightarrow \mu E \ l$ , we start with its lifting and the associated coherence property:

$$(f^+ : \mu \llbracket o_D \rrbracket_{\text{orn}} i \rightarrow \mu \llbracket o_E \rrbracket_{\text{orn}} j) \times (ds^+ : \mu \llbracket o_D \rrbracket_{\text{orn}} i) \rightarrow \text{forget } o_E \ (f^+ \ d^+) = f(\text{forget } o_D \ ds^+)$$

Applying intensional choice, we obtain the following isomorphic type:

$$\cong (ds : \mu D \ (u \ i)) \times (ds^+ : \mu \llbracket o_D \rrbracket_{\text{orn}} i) \times \text{forget } o_D \ ds^+ = ds \rightarrow (es^+ : \mu \llbracket o_E \rrbracket_{\text{orn}} j) \times \text{forget } o_E \ es^+ = f \ ds$$

Then we can simply use the characterisation of reornaments (Equation 4.20) to turn every pair  $(x^+ : \mu \llbracket o_X \rrbracket_{\text{orn}} i) \times t = \text{forget } o_X \ x^+$  into the isomorphic inductive type  $\mu \llbracket [o_X] \rrbracket_{\text{orn}} t$ :

$$\cong (ds : \mu D \ (u \ i)) \times \mu \llbracket [o_D] \rrbracket_{\text{orn}} ds \rightarrow \mu \llbracket [o_E] \rrbracket_{\text{orn}} (f \ ds)$$

which corresponds to the Patch type of this functional ornament. □

Remark 5.20 (Computational interpretation)

Constructively, we translate the left-to-right direction of this isomorphism into the pair of a patch function (Definition 5.22, which extracts the lifting) and a coherence proof (Definition 5.23, which establishes that such a lifting is coherent).

<sup>53</sup> MODEL: FunOrn.Patch.Examples.Append

*Remark 5.21 (When to index?)*

While these precisely indexed functions relieve us from the burden of theorem proving, this approach is not always applicable. For instance, if we were to implement a length-preserving list reversal function, our patching machinery would ask us to implement `vrev`:

$$\begin{aligned} \text{vrev } (xs : \text{Vec } A \ n) & : \text{Vec } A \ n \\ \text{vrev } \quad \text{nil} & \mapsto \text{nil} \\ \text{vrev } (\text{cons } a \ vs) & \mapsto \{(\text{vrev } vs) ++ (\text{cons } a \ \text{nil}) : \text{Vec } A \ (1 + n)\} \end{aligned}$$

To complete this goal calls for some proving in order to match up the types: we must appeal to the equational theory of addition. Here the term we put in the hole has type  $\text{Vec } A \ (n + 1)$  while the expected type is  $\text{Vec } A \ (1 + n)$ . The commutativity of addition is beyond the grasp of most type checkers, which are often limited to deciding definitional identities.

In the case of `vrev`, unless the type checker works up to equational theories, as done in CoqMT (Strub, 2010), the programmer is certainly better off using our machinery to generate the coherence condition (Section 5.2), implement the lifting, and write its coherence proof manually. While the patching machinery would still work, implementing a function realising the Patch specification would require some (cumbersome) rewritings of the types, thus littering the program with proofs.

This example gives a hint as to what can be seen as a ‘good’ coherence property: because we want the type checker to do all the proving, the equations we rely on at the type level have to be definitionally true, either because our logic decides a rich definitional equality, or because we rely on operations that satisfy these identities by definition.

### 5.4 Patching and coherence

At this stage, we can implement the `ilookup` function exactly as we did in Section 2. From there, we now want to obtain the `lookup` function and its coherence certificate. More generally, having implemented a function satisfying the `Patch` type, we want to extract the lifting and its coherence proof. Perhaps not surprisingly, we obtain this construction by looking at the meta-theorem of the previous section (Theorem 5.19) through our constructive glasses: indeed, since the `Patch` type is isomorphic to the class of liftings satisfying the coherence property, we effectively get a function taking every `Patch` to a lifting (Definition 5.22) and its coherence proof (Definition 5.23). More precisely, we obtain the lifting by generalising the reornament-induced `forget` functions to functional ornaments while we obtain the coherence proof by generalising the reornament-induced `coherentOrn` theorem.

*Definition 5.22 (Patching<sup>54</sup>)*

We call *patching* the action of projecting the coherent lifting from a Patch function. Again, it is defined by induction over the functional ornament:

DEFINITION				
$\text{patch } (T^+ : \text{FunOrn } T) (f : \llbracket T \rrbracket_{\text{Type}}) (f^{++} : \text{Patch } T \ T^+ \ f) :$	$\llbracket T^+ \rrbracket_{\text{FunOrn}}$			
$\text{patch } (\mu^+\{o \cdot \text{inv } i\} \rightarrow T^+) \ f \ \ f^{++}$	$\mapsto$			
$\lambda x^+. \text{patch } T^+ (f (\text{forget } o \ x^+))$				
$(f^{++} (\text{forget } o \ x^+) (\text{make } [o] \ x^+))$				
$\text{patch } (\mu^+\{o \cdot \text{inv } i\} \times T^+) (x, xs) (x^{++}, xs^{++})$	$\mapsto$			
$(\text{forget } [o] \ x^{++}, \text{patch } T^+ \ xs \ xs^{++})$				
$\text{patch} \quad 1 \quad \quad \quad * \quad \quad \quad *$	$\mapsto *$			

When ornamented arguments are introduced (i.e. with the code  $\mu^+\{o \cdot \text{inv } i\} \rightarrow$ ), we simply patch the body of the function. This is possible because from  $x^+ : \mu \llbracket o_D \rrbracket_{\text{orn}}$ , we can forget the ornament to compute  $f (\text{forget } o_D \ x^+)$ , and we can also make the reornament to compute  $f^{++} \_ (\text{make } [o] \ x^+)$ . When an ornamented result is to be returned (i.e. with the code  $\mu^+\{o \cdot \text{inv } i\} \times$ ), we simply forget the reornamentation computed by the coherent lifting.

*Definition 5.23 (Coherence of a patch<sup>55</sup>)*

Extracting the coherence proof follows a similar pattern. We introduce arguments as we go, just as we did with patch. When we reach a result, we have to prove the coherence of the result returned by the patched function, which is a straightforward application of the coherentOrn theorem:

DEFINITION				
$\text{coherence } (T^+ : \text{FunOrn } T) (f : \llbracket T \rrbracket_{\text{Type}})$	$(f^{++} : \text{Patch } T \ T^+ \ f) :$	$\text{Coherence } T^+ \ f$		
$\text{coherence } (\mu^+\{o \cdot \text{inv } i\} \rightarrow T^+) \ f \ \ f^{++}$	$\mapsto$			
$\lambda x^+. \text{coherence } T^+ (f (\text{forget } o \ x^+))$				
$(f^{++} (\text{forget } o \ x^+) (\text{make } [o] \ x^+))$				
$\text{coherence } (\mu^+\{o \cdot \text{inv } i\} \times T^+) (x, xs) (x^{++}, xs^{++})$	$\mapsto$			
$(\text{coherentOrn } x^+, \text{coherence } T^+ \ xs \ xs^{++})$				
$\text{coherence} \quad 1 \quad \quad \quad * \quad \quad \quad *$	$\mapsto *$			

<sup>54</sup> MODEL: FunOrn.Patch.Apply

<sup>55</sup> MODEL: FunOrn.Patch.Coherence

*Example 5.24 (Obtaining lookup and its coherence, for free<sup>56</sup>)*

This last step is a mere application of the patch and coherence functions. Hence, we define lookup as follows:

$$\begin{aligned} \text{lookup} & : \llbracket \text{typeLookup} \rrbracket_{\text{FunOrn}} \\ \text{lookup} & \mapsto \text{patch typeLookup } (- < -) \text{ ilookup} \end{aligned}$$

And we get its coherence proof, here spelled in full (up to a multiplication by  $\mathbb{1}$ ):

$$\begin{aligned} \text{cohLookup } (n : \text{Nat}) (xs : \text{List } A) & : \text{isJust } (\text{lookup } n \text{ } xs) = n < \text{length } xs \\ \text{cohLookup } n \quad xs & \mapsto \text{coherence typeLookup } (- < -) \text{ ilookup } n \text{ } xs \end{aligned}$$

*Remark 5.25 (Code readability)*

The lookup function thus defined is rather daunting, especially for a potential user of that piece of code. However, we must bear in mind that lookup is in fact entirely specified by ilookup: there is no point in inspecting the definition of lookup. In a programming environment, we could imagine some syntactic sugar akin to our notation for ornaments. For example, we would state that lookup is a functional ornamentation of  $- < -$ . We would be lead to  $-$  transparently  $-$  implement ilookup in lieu of lookup.

*Example 5.26 (Obtaining  $- ++ -$  and its coherence, for free<sup>57</sup>)*

Assuming that we have implemented the coherent lifting vappend, we obtain concatenation of lists and its coherence proof by simply running our generic machinery:

$$\begin{aligned} ++ & : \llbracket \text{type}++ \rrbracket_{\text{FunOrn}} \\ ++ & \mapsto \text{patch type}++ (- + -) \text{ vappend} \end{aligned}$$

$$\begin{aligned} \text{coh}++ (xs : \text{List } A) (ys : \text{List } A) & : \text{length } (xs ++ ys) = (\text{length } xs) + (\text{length } ys) \\ \text{coh}++ \quad xs \quad ys & \mapsto \text{coherence type}++ (- + -) \text{ vappend } xs \text{ } ys \end{aligned}$$

Looking back at the pedestrian construction of Section 2, we can measure the progress we have made. In the pedestrian approach, we had to (manually) index our datatypes (by defining Vec and IMaybe, and their projections back to, respectively, the list and option types), index the type signature of lookup (obtaining the type of ilookup), project lookup out of ilookup, and write its coherence proof (defining cohLookup from ilookup and the projection functions).

Functional ornaments let us focus on ornamenting the individual datatypes (Example 5.8). The rest is automatically generated for us: The coherence condition is computed by the generic Coherence type (Example 5.8), the indexed type of lookup is computed by the Patch type (Example 5.16), lookup is obtained by applying the patch (Example 5.24), and its coherence an instance of the generic coherence lemma (Example 5.24).

<sup>56</sup> MODEL: FunOrn.Lift.Examples.Lookup

<sup>57</sup> MODEL: FunOrn.Lift.Examples.Append

This is not just a convenient automation: a functional ornament establishes a strong connection between two functions. By pinning down this connection in this universe, we turn this knowledge into an effective object that can be manipulated and reasoned about within the type theory.

We make use of this concreteness when we construct the Patch induced by a functional ornament: this is again a construction that is generic now, while we had to tediously (and perhaps painfully) construct it in Section 2. Similarly, we get patching and extraction of the coherence proof for free now, while we had to manually fiddle with several projection and injection functions.

We presented the Patch type as the type of the liftings coherent by construction. As we have seen, its construction and further projection down to a lifting is entirely automated, hence effortless. This is a significant step forward: we could either implement lookup and then prove it coherent, or we could go through the trouble of manually defining carefully indexed types and write a function correct by construction. Manually crafting these finely indexed types and functions takes up time and adds complexity to a code base. By automating these constructions, using finely indexed types is now just as economic (time-wise and complexity-wise) as proving the coherence after the fact. From a programming perspective, the second approach is much more appealing. In a word, we have made an appealing technique extremely cheap!

*Remark 5.27 (No meta-theory)*

We must reiterate that none of the above constructions involve extending the type theory: building upon our universe of datatypes, ornaments, and functional ornaments is internalised as a few generic programs and inductive types. For systems, such as Agda, Coq, or an ML with GADTs, we would need to extend the language – and therefore the meta-theory – to be able to reify inductive definitions, and provide an ornament mechanism. The fact that our constructions – such as the patching operations (Definition 5.22 and Definition 5.23), and the liftings (introduced in the next section, Definition 6.5, and Definition 6.17) type check in our model suggests that adding these objects at the meta-level is consistent with a pre-existing meta-theory.

*Remark 5.28 (Efficiency considerations)*

The patching framework relies crucially on the duality between a reornament and its ornament presentation subject to a proof. While patching (Definition 5.22), we cross this isomorphism in both directions. In effect, this involves a traversal of each of the input datatypes and a traversal of each of the output datatypes. However, operationally, these traversal are identities: the only purpose of these terms is at the logical level, for the type checker to fix the types.

For example, the lookup function amounts to the following term:

$$\begin{aligned} \text{lookup} &\triangleq \text{patch typeLookup } (- < -) \text{ ilookup} \\ &\rightsquigarrow \lambda m : \text{Nat}. \lambda xs : \text{List } A. \pi_0(\text{forgetIMaybe } (\text{ilookup } m \text{ (makeVec } xs))) \end{aligned}$$

In this definition, we rely on makeVec, which traverses the (input) list to return a vector indexed by the list's length. Operationally, this is an identity. We also rely

$-$	$< -$	$: \llbracket \text{type} < \rrbracket_{\text{Type}}$	$\text{ilookup } (m : \text{Nat}) (vs : \text{Vec } A \ n) : \text{IMaybe } A \ (m < n)$
$m$	$< n$	$\Leftarrow \text{Nat-elim } n$	$\text{ilookup } m \quad vs \quad \Leftarrow \text{Vector-elim } vs$
$m$	$< 0$	$\mapsto \text{false}$	$\text{ilookup } m \quad \text{nil} \quad \mapsto \text{nothing}$
$m$	$< (\text{suc } n)$	$\Leftarrow \text{Nat-case } m$	$\text{ilookup } m \quad (\text{cons } a \ vs) \Leftarrow \text{Nat-case } m$
$0$	$< (\text{suc } n)$	$\mapsto \text{true}$	$\text{ilookup } 0 \quad (\text{cons } a \ vs) \mapsto \text{just } a$
	$(\text{suc } m) < (\text{suc } n)$	$\mapsto m < n$	$\text{ilookup } (\text{suc } m) \ (\text{cons } a \ vs) \mapsto \text{ilookup } m \ vs$

Fig. 6. Implementations of  $- < -$  and  $\text{ilookup}$ .

on  $\text{forget!Maybe}$ , which traverses the (output)  $\text{IMaybe}$  type to project it back to a non-indexed option type. Again, operationally, this is an identity.

In the future work, we would like to transform our library of smart constructors into a proper domain-specific language (DSL). This way, implementing a coherent lifting would amount to working in a domain-specific language for which an optimising compiler could compute away  $-$  by partial evaluation (Brady & Hammond, 2010) – the computationally irrelevant operations.

### 6 Lazy programmers, smart constructors

In our journey from  $- < -$  to  $\text{lookup}$ , we had to implement the  $\text{ilookup}$  function. It is instructive to put  $- < -$  and  $\text{ilookup}$  side-by-side (Figure 6). First, both functions follow the same recursion pattern: induction over  $n/vs$  followed by case analysis over  $m$ . Second, the returned constructors are related through the  $\text{Maybe}$  ornament: knowing that we have returned  $\text{true}$  or  $\text{false}$  when implementing  $- < -$ , we can deduce which of  $\text{just}$  or  $\text{nothing}$  will be used in  $\text{ilookup}$ . Interestingly, the only unknown, hence the only necessary input from the user, is the  $a$  in the  $\text{just}$  case: this is precisely the information that has been introduced by the  $\text{Maybe}$  ornament.

In this section, we are going to leverage our knowledge of the definition of the base function  $-$  such as  $- < -$  to guide the implementation of the coherent lifting  $-$  such as  $\text{ilookup}$ : instead of re-implementing  $\text{ilookup}$  by duplicating most of the code of  $- < -$ , the user indicates *what to transport* and only provides the *strictly necessary* inputs. We are primarily interested in transporting the following two forms of structure:

**Recursion pattern:** If the base function is a catamorphism  $(\llbracket \alpha \rrbracket)$  and the user provides us with a *coherent algebra*  $\alpha^{++}$  of  $\alpha$ , we construct the coherent lifting  $(\llbracket \alpha^{++} \rrbracket)$  of  $(\llbracket \alpha \rrbracket)$ ;

**Returned constructor:** If the base function returns a constructor  $C$  and the user provides us with a *coherent extension* of  $C$ , we construct the coherent lifting of  $C$ .

We shall formalise below what we understand by being a *coherent algebra* and a *coherent extension*. The key idea is to identify the strictly necessary inputs from the user, helped in that by the ornaments. It is then straightforward to build the lifted objects, automatically and generically.

6.1 Transporting recursion patterns

When transporting a function, we are very unlikely to change the recursion pattern of the base function. Indeed, the very reason why we *can* do this transformation is that the lifting uses exactly the same underlying structure to compute its results. Hence, most of the time, we could just ask the computer to use the recursion pattern induced by the base function: the only task left to the user will be to give an algebra.

Example 6.1 (Lifting a catamorphism)

To understand how we transport recursion patterns, let us look again at the coherence property of liftings, but this time specialising to a function that is a catamorphism:

$$\begin{array}{ccc}
 \mu \llbracket [O_D] \rrbracket_{\text{orn}} i & \xrightarrow{\langle \beta \rangle} & \mu \llbracket [O_E] \rrbracket_{\text{orn}} i \\
 \text{forget } o_D \downarrow & & \downarrow \text{forget } o_E \\
 \mu D(ui) & \xrightarrow{\langle \alpha \rangle} & \mu E(ui)
 \end{array}$$

By the fold-fusion theorem (Bird & de Moor, 1997), it is sufficient to work on the algebras, where we have the following diagram:

$$\begin{array}{ccc}
 \llbracket [O_D] \rrbracket_{\text{orn}} (\mu \llbracket [O_E] \rrbracket_{\text{orn}}) i & \xrightarrow{\beta} & \mu \llbracket [O_E] \rrbracket_{\text{orn}} i \\
 \downarrow \llbracket \llbracket [O_D] \rrbracket_{\text{orn}} \rrbracket^{\rightarrow} (\text{forget } o_E) & & \downarrow \text{forget } o_E \\
 \llbracket [O_D] \rrbracket_{\text{orn}} (\mu E \circ u) i & \xrightarrow{\text{forgetNT } O_D} \llbracket [D] \rrbracket (\mu E)(ui) & \xrightarrow{\alpha} \mu E(ui)
 \end{array}$$

We can therefore reduce the problem of describing the commuting square of catamorphisms (i.e. the Patch of  $\langle \alpha \rangle$ ) to the one consisting in working directly with their algebras. In effect, we are going to characterise the algebras  $\alpha^{++}$  whose catamorphism is coherent by construction (i.e. inhabits the Patch of  $\langle \alpha \rangle$ ).

Remark 6.2

We have established that if the square comprising the algebras commutes, then the square comprising their catamorphisms also commutes. However, the converse does not hold: Having that the square of catamorphisms commutes does not necessarily imply that the square of algebras commutes.

Example 6.3 (Lifting isSuc)

To illustrate our approach, let us work through a concrete example: We derive  $\text{hd} : \text{List } A \rightarrow \text{Maybe } A$  from  $\text{isSuc} : \text{Nat} \rightarrow \text{Bool}$  by transporting the algebra. For the

sake of argument, we artificially define `isSuc` by a catamorphism:

```

isSuc (n : Nat) : Bool
isSuc n ↦ (isSucAlg) n where
  isSucAlg (xs : [[Nat-func]] (λ*. Bool) *) : Bool
  isSucAlg ('0, *) ↦ false
  isSucAlg ('suc, xs) ↦ true
    
```

Our objective is thus to define the algebra for `hd`, which has the following type

$$\text{hdAlg} : \llbracket \text{List-func } A \rrbracket (\lambda*. \text{Maybe } A) * \rightarrow \text{Maybe } A$$

such that its catamorphism is coherent. By the fold-fusion theorem, it is sufficient for `hdAlg` to satisfy the following condition:

$$\begin{aligned}
 & (ms : \llbracket \text{List-func } A \rrbracket (\lambda*. \text{Maybe } A) *) \rightarrow \\
 & \text{isJust } (\text{hdAlg } ms) = \text{isSucAlg } (\text{forgetNT } (\text{List-Orn } A) (\llbracket \text{List-func } A \rrbracket^{\rightarrow} \text{isJust } ms))
 \end{aligned}$$

Following the same methodology we applied to define the `Patch` type, we can massage the type of `hdAlg` and its coherence condition to obtain an isomorphic definition enforcing the coherence by indexing. In this case, we obtain the type

$$\text{lift}_{\text{Alg}} \text{hdAlg} \triangleq \forall n. \llbracket \text{Vec-func } A \rrbracket (\lambda n'. \text{IMaybe } A (\text{isSuc } n')) n \rightarrow \text{IMaybe } A (\text{isSuc } n)$$

This construction generalises to any functional ornament. First, we define the notion of coherent algebra (Definition 6.4) as those algebras that are coherent by construction. We then compute the coherent liftings of these algebras (Definition 6.5).

*Definition 6.4 (Coherent algebra<sup>58</sup>)*

We define the *coherent algebras* over an algebra  $\alpha$  to be the inhabitants of the type

DEFINITION

$$\begin{aligned}
 & \text{lift}_{\text{Alg}} (\alpha : \forall k : K. \llbracket D \rrbracket (\lambda - . \llbracket T \rrbracket_{\text{Type}}) k \rightarrow \llbracket T \rrbracket_{\text{Type}}) (o : \text{orn } D \ u) (T^+ : \text{FunOrn } T) : \text{SET} \\
 & \text{lift}_{\text{Alg}} \alpha \ o \ T^+ \mapsto \forall (i, t) : (i : I) \times \mu \ D \ (u \ i). \\
 & \quad \llbracket [o] \rrbracket_{\text{orn}} (\lambda (i, t). \text{Patch } T \ T^+ ((\alpha) \ t)) (i, t) \rightarrow \text{Patch } T \ T^+ ((\alpha) \ t)
 \end{aligned}$$

*Definition 6.5 (Lifting of coherent algebra<sup>58</sup>)*

Constructively, we get that coherent algebras induce coherent liftings by the catamorphism of the coherent algebra:

DEFINITION

$$\begin{aligned}
 & \text{lift-fold } (\alpha : \forall k : K. \llbracket D \rrbracket (\lambda - . \llbracket T \rrbracket_{\text{Type}}) k \rightarrow \llbracket T \rrbracket_{\text{Type}}) \\
 & \quad (\alpha^{++} : \text{lift}_{\text{Alg}} \alpha \ o \ T^+) : \text{Patch } (\mu \{ D \cdot u \ i \} \rightarrow T) (\mu^+ \{ o \cdot \text{inv } i \} \rightarrow T^+) (\alpha) \\
 & \text{lift-fold } \alpha \ \alpha^{++} \mapsto \lambda x. \lambda x^{++}. (\alpha^{++}) \ x^{++}
 \end{aligned}$$

<sup>58</sup> MODEL: FunOrn.Lift.Fold



The treatment of induction is essentially the same, as hinted at by the fact that induction can be reduced to a catamorphism (Hermida & Jacobs, 1998). We first define the coherent inductive step and deduce an operation lifting induction principles.

*Definition 6.6 (Coherent inductive step<sup>59</sup>)*

We define the *coherent inductive step* over an inductive step  $\alpha$  to be the inhabitants of the type

$$\begin{array}{c} \text{--- DEFINITION ---} \\ \text{lift}_{\text{IH}} (\alpha : (k : K)(xs : \llbracket D \rrbracket (\mu D) k) \rightarrow \square_D (\lambda - . \llbracket T \rrbracket_{\text{Type}}) xs \rightarrow \llbracket T \rrbracket_{\text{Type}}) \\ (o : \text{orn } D u)(T^+ : \text{FunOrn } T) : \text{SET} \\ \text{lift}_{\text{IH}} \alpha o T^+ \mapsto ((i, t) : (i : I) \times \mu D (u i)) \rightarrow (xs : \llbracket [o] \rrbracket_{\text{orn}} (\mu \llbracket [o] \rrbracket_{\text{orn}}) (i, t)) \rightarrow \\ \square_{\llbracket [o] \rrbracket_{\text{orn}}} (\lambda(i, t). \text{Patch } T T^+ (\text{induction } \alpha t)) xs \rightarrow \\ \text{Patch } T T^+ (\text{induction } \alpha t) \end{array}$$

*Definition 6.7 (Lifting of inductive step<sup>60</sup>)*

As for algebras, a coherent inductive step  $\alpha^{++}$  induces a coherent lifting by merely applying the induction:

$$\begin{array}{c} \text{--- DEFINITION ---} \\ \text{lift-ind } (\alpha : (k : K)(xs : \llbracket D \rrbracket (\mu D) k) \rightarrow \square_D (\lambda - . \llbracket T \rrbracket_{\text{Type}}) xs \rightarrow \llbracket T \rrbracket_{\text{Type}}) \\ (\alpha^{++} : \text{lift}_{\text{IH}} \alpha o T^+) : \text{Patch } (\mu\{D \cdot u i\} \rightarrow T) (\mu^+\{o \cdot \text{inv } i\} \rightarrow T^+) (\text{induction } \alpha) \\ \text{lift-ind } \alpha \alpha^{++} \mapsto \lambda x. \lambda x^{++}. \text{induction } \alpha^{++} x^{++} \end{array}$$

*Definition 6.8 (Lifting of case analysis<sup>61</sup>)*

Lifting case analysis is trivial, since it is derivable from induction by stripping out the induction hypotheses (McBride *et al.*, 2004):

$$\begin{array}{c} \text{--- DEFINITION ---} \\ \text{lift-case } (\alpha : (k : K)(xs : \llbracket D \rrbracket (\mu D) k) \rightarrow \llbracket T \rrbracket_{\text{Type}}) \\ (\alpha^{++} : \text{lift}_{\text{IH}} (\lambda xs - . \alpha xs) o T^+) : \text{Patch } (\mu\{D \cdot u i\} \rightarrow T) \\ (\mu^+\{o \cdot \text{inv } i\} \rightarrow T^+) \\ (\text{induction } (\lambda xs - . \alpha xs)) \\ \text{lift-case } \alpha \alpha^{++} \mapsto \text{lift-ind } (\lambda xs - . \alpha xs) (\lambda xs - . \alpha^{++} xs) \end{array}$$

*Example 6.9 (Transporting the recursion pattern of isSuc<sup>62</sup>)*

<sup>59</sup> MODEL: FunOrn.Lift.Induction

<sup>60</sup> MODEL: FunOrn.Lift.Induction

<sup>61</sup> MODEL: FunOrn.Lift.Case

We can now apply our generic machinery to transport `isSuc` to `hd`: using a high-level notation, we write the command of Figure 7(a). This command instructs the system to generate the skeleton of the algebra, as shown in Figure 7(b). In the low-level type theory, this corresponds to the following term:

```

ihd. (vs : Vec A n) : IMaybe A (isSuc n)
ihd.   vs           ↦ lift-fold isSucAlg ihdAlg vs
where
  ihdAlg (vs : [Vec-func A]) (λn'. IMaybe A (isSuc n')) n : IMaybe A (isSuc n)
  ihdAlg (^nil, *)           ↦ {?}
  ihdAlg (^cons, (a, xs))   ↦ {?}
    
```

Note that we do not need to specify the arguments over which the catamorphism is lifted in Figure 7(a): indeed, this information is provided by the base function. This is reflected by the elaborated code: the arguments of `lift-fold` are only the algebras. The resulting catamorphism is applied to the correct variables by construction.

*Remark 6.10 (High-level notation)*

Formalising the elaboration process from the high-level notation to the low-level type theory is beyond the scope of this paper. The readers will convince themselves that the high-level notation contains all the information necessary to reconstruct a low-level term. Indeed, when lifting a recursion pattern, the goal – a `Patch` type – provides all the information concerning the functional ornament being constructed, including the algebra that is being lifted. Similarly, when lifting a constructor, the goal – still a `Patch` type – carries the functional ornament as well as the constructor being lifted. We shall use the high-level notation to succinctly describe our transformations, with the understanding that it builds a low-level term that type checks. We come back to the practicality of such a notation in Remark 6.22.

*Example 6.11 (Transporting the recursion pattern of  $- < -^{63}$ )*

To implement `ilookup`, we use `lift-ind` to transport the induction over `n`:

```

ilookup : Patch type< typeLookup (- < -)
ilookup  m m+  n      vs       $\overset{\text{lift}}{\leftarrow}$  lift-ind
ilookup  m m+  0      nil      {?}
ilookup  m m+ (suc n) (cons a vs) {?}
    
```

Followed by a `lift-case` to transport the case analysis over `m`:

```

ilookup : Patch type< typeLookup (- < -)
ilookup  m      m+  n      vs       $\overset{\text{lift}}{\leftarrow}$  lift-ind
ilookup  m      m+  0      nil      {?}
ilookup  m      m+  (suc n) (cons a vs)  $\overset{\text{lift}}{\leftarrow}$  lift-case
ilookup  0      0    0      nil      {?}
ilookup (suc m) (suc m+) 0      nil      {?}
    
```

<sup>62</sup> MODEL: FunOrn.Lift.Examples.Head

<sup>63</sup> MODEL: FunOrn.Lift.Examples.Lookup

The interactive nature of this construction is crucial: The user needs only to specify a lifting – symbolised by the  $\overset{\text{lift}}{\leftarrow}$  command – together with the action to be carried out, while the computer does all the heavy lifting and generates the resulting patterns.

*Example 6.12 (Transporting the recursion pattern of  $- + -$ <sup>64</sup>)*

In order to implement the concatenation of vectors, we can also benefit from our generic machinery. We simply have to instruct the machine that we want to lift the case analysis used in the definition of  $- + -$  and the computer comes back to us with the following goals:

```
vappend : Patch type+ type++ - + -
vappend   m      xs   n   ys    $\overset{\text{lift}}{\leftarrow}$  lift-ind
vappend   0      nil  n   ys   {?}
vappend (suc m) (cons a xs) n   ys   {?}
```

## 6.2 Transporting constructors

Just as the recursive structure, the returned values frequently mirror the original definition: we are often in a situation where the base function returns a given constructor and we would like to return its ornamented counterpart. Informing the computer that we simply want to lift that constructor, it should fill in the parts that are already determined and ask only for the missing information, i.e. the data newly introduced by the ornament.

Recall that, when constructing an inhabitant of a Patch type, we are working on the reornaments of the lifting. When returning a constructor-headed value, we are simply building an inhabitant of a reornament (Definition 5.15, case  $\mu^+\{o \cdot \text{inv } i\} \times$ ). By definition of reornaments (Section 4.5), all the information provided by the non-ornamented datatype – the index – is optimally used: every opportunity for deletion has been taken. In particular, none of the data provided by index – the non-ornamented data – needs to be duplicated within the reornamented datatype: only the extensions introduced by the ornament need to be provided.

This suggests the decomposition of the inhabitants of reornaments in two components:

- Giving the *extension* of the ornament, i.e. all the extra information introduced by the ornament.
- Giving the recursive arguments – dictated by its *structure* – of the reornamented datatype.

*Example 6.13 (Inhabiting the reornament of List-Orn)*

Let us illustrate this decomposition on the reornament of List-Orn. The reornament of List-Orn is structured as follows:

<sup>64</sup> MODEL: FunOrn.Lift.Examples.Append

- We retrieve the index, hence obtaining a number  $n : \text{Nat}$ .
- By inspecting the ornament `List-Orn`, we obtain the *exact* information by which  $n$  is *extended* into a list: if  $n = 0$ , no supplementary information is needed; if  $n = \text{succ } n'$ , we need to extend it with an  $a : A$ . We call this the extension – denoted `Extension` – of `List-Orn` at  $n$ :

$$\begin{aligned} \text{Extension (List-Orn } A *) (\text{'}0, *) &\rightsquigarrow \mathbb{1} \\ \text{Extension (List-Orn } A *) (\text{'}succ, n') &\rightsquigarrow (a : A) \times \mathbb{1} \end{aligned}$$

- By inspecting the ornament `List-Orn` again, and provided an extension of the index  $n$ , we obtain the recursive structure of the reornament at that index by extracting the *refined* indexing discipline: if  $n = 0$ , no argument is expected; if  $n = \text{succ } n'$ , we expect the tail to be a vector of size  $n'$ . We call this the (recursive) structure – denoted `Structure` – of `List-Orn` at  $n$ :

$$\begin{aligned} \text{Structure (List-Orn } A *) (\text{'}0, *) &\rightsquigarrow \mathbb{1} \\ \text{Structure (List-Orn } A *) (\text{'}succ, n') (a, *) &\rightsquigarrow \mu \llbracket \llbracket \text{List-Orn } A \rrbracket \rrbracket_{\text{orn}} (*, n') \end{aligned}$$

Provided an extension – an inhabitant  $e$  of `Extension (List-Orn  $A$  *)  $n$`  – and its recursive arguments – an inhabitant of `Structure (List-Orn  $A$  *)  $n$   $e$` , we have all the necessary data to inhabit of reornament of `List-Orn` (i.e. to inhabit a vector indexed by  $n$ ).

This decomposition generalises to any reornament. We define the *extension* of an ornament (Definition 6.14), and the *structure* of its reornament (Definition 6.15). Given an extension and its structure, we then show how to inhabit a reornament (Definition 6.16). In what follows, we take  $E : \text{func } I$  to be a description and  $o : \text{orn } E u$  to be an ornament of  $E$ .

*Definition 6.14 (Reornament extension<sup>65</sup>)*

The extension of an ornament is given by its insert codes. Therefore, the `Extension` function merely collects these insertions (the insert case). It also makes sure that the indexing respects the previously deleted data through equations (the delete case). On a  $\Sigma$  case, no data is required: the information is already available from the index.

<sup>65</sup> MODEL: `FunOrn.Lift.MkReorn`

Otherwise, it proceeds purely structurally (the `var`, `1`, and  $\Pi$  cases).

— DEFINITION —

Extension ( $O : \text{Orn } D u$ ) ( $xs : \llbracket D \rrbracket (\mu E)$ ) : SET  
 – Ask for freshly inserted data, it is the data missing from  $xs$ :  
 Extension ( $\text{insert } S D^+$ )  $xs \mapsto (s : S) \times \text{Extension } (D^+ s) xs$   
 – Do not duplicate the original data, it is already in  $xs$ :  
 Extension ( $\text{var } (\text{inv } i)$ )  $xs \mapsto \mathbb{1}$   
 Extension  $1$   $*$   $\mapsto \mathbb{1}$   
 Extension ( $\Pi T^+$ )  $f \mapsto (s : S) \rightarrow \text{Extension } (T^+ s) (f s)$   
 Extension ( $\Sigma T^+$ )  $(s, xs) \mapsto \text{Extension } (T^+ s) xs$   
 – Deleted data must be consistent with the index:  
 Extension ( $\text{delete } s T^+$ )  $(s', xs) \mapsto (q : s = s') \times \text{Extension } T^+ xs$

Note that while we copy the  $\Pi$  codes as a  $\Pi$ -type, we are not *duplicating* information: the codomain of the  $\Pi$ -type contains only new information, or is isomorphic to  $\mathbb{1}$  (in which case, the whole  $\Pi$ -type is itself isomorphic to  $\mathbb{1}$ ).

*Definition 6.15 (Reornament structure<sup>65</sup>)*

We capture the recursive structure of the reornament by traversing the ornament while peeling off the index  $xs$  along the way. The crucial step is the variable case (case `var`): we ask for a reornament  $\mu \llbracket [o] \rrbracket_{\text{orn}}$  taken at the index specified by the ornament and the current index  $xs$ . The other cases are only creating the necessary scaffolding to cover all the recursive arguments.

— DEFINITION —

Structure ( $O : \text{Orn } D u$ ) ( $xs : \llbracket D \rrbracket (\mu E)$ ) ( $e : \text{Extension } O xs$ ) : SET  
 – Extract the next index from the ornament and the index:  
 Structure ( $\text{var } (\text{inv } i)$ )  $xs \quad * \mapsto \mu \llbracket [o] \rrbracket_{\text{orn}} (i, xs)$   
 – Duplicate (only) the recursive structure:  
 Structure ( $\text{insert } S D^+$ )  $xs \quad (s, e) \mapsto \text{Structure } (D^+ s) xs e$   
 Structure  $1$   $*$   $*$   $\mapsto \mathbb{1}$   
 Structure ( $\Pi T^+$ )  $f \quad e \mapsto (s : S) \text{Structure } (T^+ s) (f s) (e s)$   
 Structure ( $\Sigma T^+$ )  $(s, xs) \quad e \mapsto \text{Structure } (T^+ s) xs e$   
 Structure ( $\text{delete } s T^+$ )  $(s, xs) (refl, e) \mapsto \text{Structure } T^+ xs e$

The decomposition of the reornament in terms of an extension and its recursive structure is formally expressed by the following isomorphism:

META-THEOREM

Let  $D : !\text{Desc } I$  be a description code and let  $O : \text{Orn } D u$  be an ornament code of  $D$ .  
 For all  $xs : \llbracket D \rrbracket (\mu E)$ , we have:  

$$(e : \text{Extension } O \text{ } xs) \times \text{Structure } O \text{ } xs e \cong \llbracket \llbracket O \rrbracket \rrbracket_{\text{orn } xs} (\mu o)$$

In practice, we are interested in the left-to-right direction of the isomorphism, which allows us to inhabit a reornament by focusing on the extension introduced by the ornament and its recursive arguments. Constructively, this translates into the `mkReorn` function below.

*Definition 6.16 (Inhabitation of reornaments<sup>66</sup>)*

For a given ornament  $O : \text{Orn } D u$  and some index  $xs : \llbracket D \rrbracket (\mu E)$ , we can therefore combine an extension of  $O$  at  $xs$  with its recursive arguments to inhabit the reornament of  $O$ . To do so, we proceed by case analysis over the ornament  $O$ : we find that the data required by the reornament is either provided by the extension (case `insert`), or the structure (case `var`). The other cases contain no data *per se*, only the recursive structure of the datatype.

DEFINITION

`mkReorn` ( $O : \text{Orn } D u$ ) ( $xs : \llbracket D \rrbracket (\mu E)$ )  
 $(e : \text{Extension } O \text{ } xs) (a : \text{Structure } O \text{ } xs e) : \llbracket \llbracket O \rrbracket \rrbracket_{\text{orn } xs} (\mu \llbracket \llbracket o \rrbracket \rrbracket_{\text{orn}})$

`mkReorn` (`insert`  $S D^+$ )  $xs$   $(s, e)$   $a \mapsto (s, \text{mkReorn } (D^+ s) e a)$   
`mkReorn` (`var` (`inv`  $i$ ))  $xs$   $*$   $a \mapsto a$   
`mkReorn`  $1$   $*$   $*$   $*$   $\mapsto *$   
`mkReorn`  $(\Pi T^+)$   $f$   $e$   $a \mapsto \lambda s. \text{mkReorn } (T^+ s) (f s) (e s) (a s)$   
`mkReorn`  $(\Sigma T^+)$   $(s, xs)$   $e$   $a \mapsto \text{mkReorn } (T^+ s) xs e a$   
`mkReorn` (`delete`  $s T^+$ )  $(s, xs)$   $(\text{refl}, e)$   $a \mapsto (\text{refl}, \text{mkReorn } T^+ xs e a)$

*Definition 6.17 (Lifting of constructor<sup>67</sup>)*

This clear separation of concerns is a blessing for us: when lifting a constructor, we only have to provide the extension and the arguments of the datatype, nothing

<sup>66</sup> MODEL: `FunOrn.Lift.MkReorn`

<sup>67</sup> MODEL: `FunOrn.Lift.Constructor`

more. The implementation is as simple as:

DEFINITION

lift-constructor $(e : \text{Extension } (o\ i)\ xs)$	– coherent extension
$(a : \text{Structure } (o\ i)\ xs\ e)$	– recursive arguments
$(t^{++} : \text{Patch } T\ T^+\ t)$	
$: \text{Patch } (\mu\{D \cdot u\ i\} \times T) (\mu^+\{o \cdot \text{inv } i\} \times T^+) (\text{in } xs, t)$	
lift-constructor $e\ a\ t^{++} \mapsto (\text{in } (\text{mkReorn } (o\ i)\ xs\ e\ a), t^{++})$	

For convenience, we extend our high-level notation with a gadget for returning a lifted constructor. We shall therefore write

$$\dots \overset{\text{lift}}{\mapsto} e[a]$$

to denote the low-level term

$$\text{lift-constructor } e\ a\ *$$

A few examples illustrating this notation follow (Examples 6.18 and 6.19).

*Example 6.18 (Transporting the constructors of isSuc<sup>68</sup>)*

Let us finish the implementation of hd from isSuc. Our task is simply to transport the true and false constructors along the Maybe ornament. In a high-level notation, we would write the command shown in Figure 7(c). The interactive system would then respond by generating the code of Figure 7(d). The unit goals are trivially solved. The only information the user has to provide is a value of type *A*, which is required by the just constructor.

*Example 6.19 (Transporting the constructors of – < –<sup>69</sup>)*

As for ilookup, we want to lift the constructors true and false to the Maybe ornament. In a high-level notation, this would be represented as follows:

$$\begin{array}{llllll} \text{ilookup} & : & \text{Patch } \text{type} < \text{type} & \text{Lookup } (- < -) & & \\ \text{ilookup} & m & m^+ & n & vs & \overset{\text{lift}}{\Leftarrow} \text{lift-ind} \\ \text{ilookup} & m & m^+ & 0 & \text{nil} & \overset{\text{lift}}{\mapsto} \text{nothing } *[*] \\ \text{ilookup} & m & m^+ & (\text{suc } n) (\text{cons } a\ vs) & & \overset{\text{lift}}{\Leftarrow} \text{lift-case} \\ \text{ilookup} & 0 & 0 & (\text{suc } n) (\text{cons } a\ vs) & & \overset{\text{lift}}{\mapsto} \text{just } \{a : A\} [*] \\ \text{ilookup} & (\text{suc } m) (\text{suc } m^+) (\text{suc } n) (\text{cons } a\ vs) & & & & \{?\} \end{array}$$

As before, in an interactive setting, the user would instruct the machine to execute the command  $\overset{\text{lift}}{\mapsto}$  and the computer would come back with the skeleton of the expected inputs. Finishing the implementation of ilookup is now a baby step away

<sup>68</sup> MODEL: FunOrn.Lift.Examples.Head  
<sup>69</sup> MODEL: FunOrn.Lift.Examples.Lookup

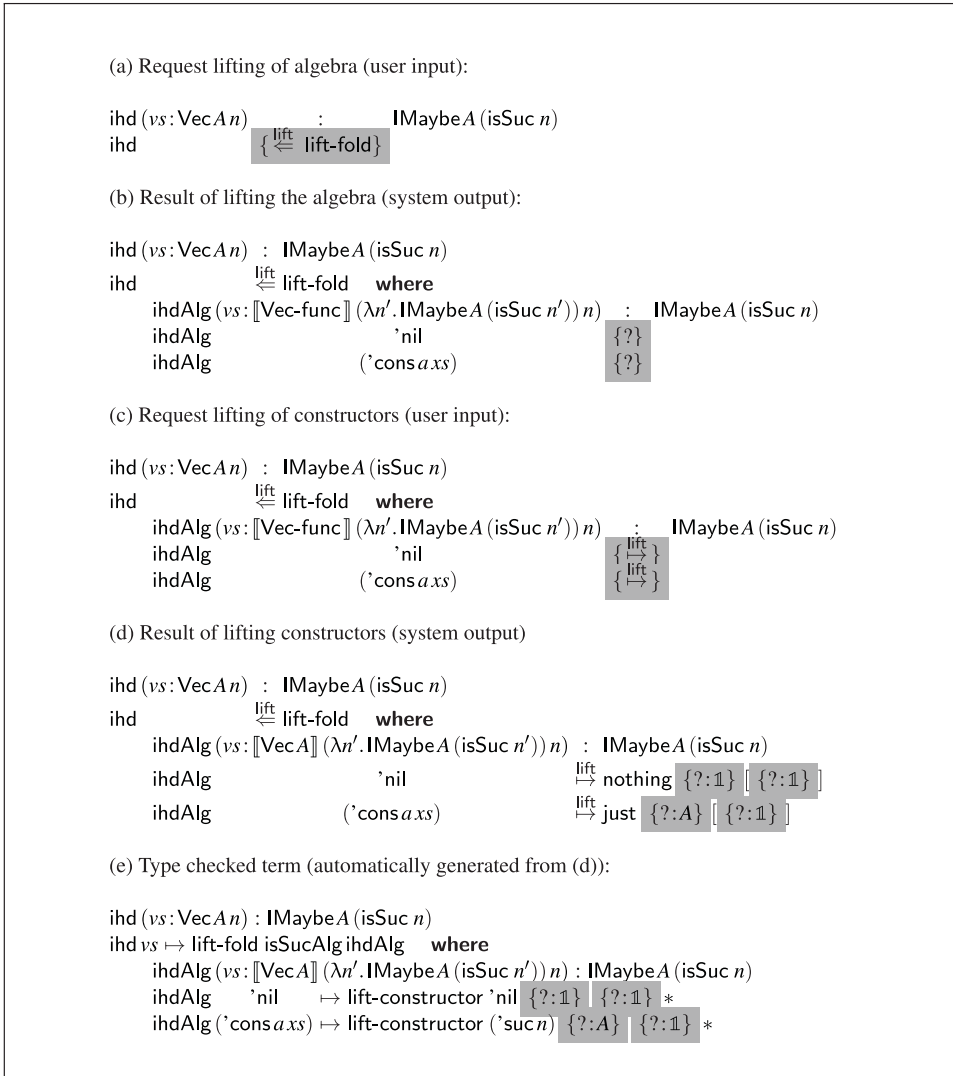


Fig. 7. Guided implementation of ihd.

for the programmer:

$$\text{illookup} : \text{Patch type} < \text{typeLookup } (- < -)$$

$$\text{illookup} \quad m \quad m^+ \quad n \quad vs \quad \left\{ \begin{array}{l} \text{lift} \\ \leftarrow \text{lift-ind} \end{array} \right\}$$

$$\text{illookup} \quad m \quad m^+ \quad 0 \quad \text{nil} \quad \left\{ \begin{array}{l} \text{lift} \\ \rightarrow \text{nothing } * [ * ] \end{array} \right\}$$

$$\text{illookup} \quad m \quad m^+ \quad (\text{suc } n) \ (\text{cons } a \ vs) \quad \left\{ \begin{array}{l} \text{lift} \\ \leftarrow \text{lift-case} \end{array} \right\}$$

$$\text{illookup} \quad 0 \quad 0 \quad (\text{suc } n) \ (\text{cons } a \ vs) \quad \left\{ \begin{array}{l} \text{lift} \\ \rightarrow \text{just } a [ * ] \end{array} \right\}$$

$$\text{illookup } (\text{suc } m) \ (\text{suc } m^+) \ (\text{suc } n) \ (\text{cons } a \ vs) \mapsto \text{illookup } m \ m^+ \ n \ vs$$

This last step is out of reach of our framework: the recursive call is justified by the first induction over the vector *vs*, which gives us access to a higher-order induction



hypothesis (taking natural numbers to the IMaybe type). We have to fully apply this induction hypothesis to  $m$  and  $im$  to perform the recursive call, an operation for which we offer no support.

*Remark 6.20 (Lifting vs. manual construction)*

Had we ignored the structural ties between  $- < -$  and `lookup`, we would have constructed `ilookup` by duplicating its underlying structure:

```

ilookup : Patch type< typeLookup (- < -)
ilookup  m    m+  n    vs    ⇐ Vector-elim vs
ilookup  m    m+  0    nil    ↳ nothing
ilookup  m    m+  (suc n) (cons a vs) ⇐ Nat-case m+
ilookup  0    0    (suc n) (cons a vs) ↳ just a
ilookup (suc m) (suc m+) (suc n) (cons a vs) ↳ ilookup m m+ n vs
    
```

That is, we would have duplicated the induction over the second argument ( $\dots \Leftarrow \text{Vec-elim } vs$ ), and the induction over the first argument ( $\dots \Leftarrow \text{Nat-elim } m$ ). We would have also duplicated the returned constructor ( $\dots \mapsto \text{nothing}$  and  $\dots \mapsto \text{just } a$ ).

Ignoring the structural ties has two consequences. First, this provides less opportunities for the system to guide the implementation of `ilookup`: the search space is less constrained. Second, having lost the connection between  $- < -$  and `ilookup`, a modification of the former will not impact the latter. In the course of a development, the two implementations might diverge in incompatible ways.

*Example 6.21 (Transporting the constructors of  $- + -$ <sup>70</sup>)*

We can also benefit from the automatic lifting of constructors to fill out the `cons` case of vector `append`. We instruct the system that we want to lift the `suc` constructor, which results in the following goals:

```

vappend : Patch type+ type++ - + -
vappend  m    xs  n  ys    lift ⇐ lift-ind
vappend  0    nil n  ys    {?}
vappend (suc m) (cons a xs) n  ys    lift ↳ cons {?:A} [ {?} ]
    
```

Concluding the implementation of `vappend` is then left to the programmer:

```

vappend : Patch type+ type++ - + -
vappend  m    xs  n  ys    lift ⇐ lift-ind
vappend  0    nil n  ys    ↳ ys
vappend (suc m) (cons a xs) n  ys    lift ↳ cons a [vappend m xs n ys]
    
```

*Remark 6.22 (About an interactive system)*

<sup>70</sup> MODEL: Fun0rn.Lift.Examples.Append

To convey our message to the reader, we have used an (informal) notation, extending the Epigram programming gadgets with lifting specific gadgets. We have not given much information about their implementability, or even hinted at a formal specification. It would certainly be interesting to elaborate on such a language extension. However, as for the notation for ornaments (Section 4.1), this notation was meant to convey high-level intuitions *to the reader*, and to keep us from flooding these pages with lambda terms.

In terms of implementation, elaborating this notation (or a less ambiguous version thereof) might be arduous. A more pragmatic alternative would be to implement a semi-decision procedure *à la* Agsy (Lindblad & Benke, 2004) that would attempt to automatically lift a function. In this setting, the lifting constructors that we have defined in this section serve as a precise language in which to express the lifting problem, and over which to compute its solution. They thus narrow the search space and guide the decision procedure.

## 7 Related works

Our work is an extension of the work of McBride (to appear) on ornaments, originally introduced to organise datatypes according to their common structure. This gave rise to the notion of ornamental algebras – forgetting the extra information of an ornamented datatype – and algebraic ornaments – indexing a datatype according to an algebra. This, in turn, induced the notion of algebraic ornament by ornamental algebras, which is a key ingredient of our work. However, for simplicity of exposition, these ornaments had originally been defined on a less index-aware universe of datatypes. As a consequence, computation over indices was impossible and deletion of duplicated information was impossible. A corollary of this was that reornaments contained a lot of duplication, hence making the lifting of values from ornamented to reornamented datatypes extremely tedious.

Our presentation of algebraic ornament has been greatly improved by the categorical model developed by Atkey *et al.* (2012): the authors gave a conceptually clear treatment of algebraic ornament in a Lawvere fibration. At the technical level, the authors connected the definition of algebraic ornament with truth-preserving liftings, which are also used in the construction of induction principles, and op-reindexing, which models  $\Sigma$ -types in the type theory. While the authors did not explicitly address the issue of transporting functions across ornaments, much of the infrastructure was implicitly there: for instance, lifting of catamorphisms is a trivial specialisation of induction.

In their work on realizability and parametricity for Pure Type Systems, Bernardy & Lasson (2011) have shown how to build a logic from a programming language. In such a system, terms of type theory can be precisely segregated based on their computational and logical contribution. In particular, the idea that natural numbers realise lists of the corresponding length appears in this system under the guise of vectors, the reflection of the realizability predicate. The strength of the realizability interpretation is that it is naturally defined on functions: while McBride (to appear) and Atkey *et al.* (2012) only consider ornaments on datatypes, Bernardy & Lasson's

(2011) work is the first, to our knowledge, to capture a general notion of functions realising – i.e. ornamenting – other functions.

Bernardy & Guilhem (2013) have further shown that this technique can be internalised in a type theory with colour, for which the logical system and the programming language are a single entity. In this setting, the realizability predicate is specialised to an (internalised) parametricity result. This parametricity result gives ‘theorems for free’ (Wadler, 1989), relating functions operating on coloured types (akin to our functional ornaments) to functions operating on colour-erased types (akin to our base types). On inductive types, colours allow a user to specify *restrictions* of types (dually to the *extension* mechanism offered by ornaments) by filtering out some colours from a definition. This difference is mostly methodological. Our work is focused on creating more precise datatypes from less precise ones, and lifting functions from basic types to richer types: hence our focus on extensions. Being guided by erasure, Bernardy & Guilhem (2013) focus on extracting functions on less precise types from the more informative ones: hence their focus on restrictions. In our setting, the erasure-based approach corresponds to the right-to-left direction of the Patch isomorphism (Theorem 5.19). The *refinement* mechanism offered by ornaments seems absent from the initial proposal of the calculus of coloured constructions: this suggests a natural generalisation of the calculus with inductive families. Our base types and functional ornaments are however limited to a first-order, simply typed setting, while the calculus of coloured constructions defines erasure for  $\Pi$ -types and  $\Sigma$ -types: it would be interesting to extend our universe of function types and functional ornaments in that direction (following Remark 5.2).

Following the steps of Bernardy & Lasson (2011), Ko & Gibbons (2011) adapted the realizability interpretation to McBride’s universe of datatypes and explored the other direction of the Patch isomorphism (Theorem 5.19) using reornaments to generate coherence properties: They describe how one could take list append together with a proof that it is coherent with respect to addition and obtain the vector append function. Their approach would shift neatly to our index-aware setting, where the treatment of reornaments is streamlined by the availability of deletion.

However, we prefer to exploit the direction of the isomorphism which internalises coherence: we would rather use the full power of dependent types to avoid explicit proof. Hence, in our framework, we simultaneously induce list append and implicitly prove its coherence with addition just by defining vector append. Of course, which approach is appropriate depends on one’s starting point. Moreover, our universe of function types takes a step beyond the related work by supporting the mechanised construction of liftings, leaving to the user the task of supplying a minimal patch. Our framework could easily be used to mechanise the realizability predicates of Bernardy & Lasson (2011) and Ko & Gibbons (2011).

## 8 Conclusions

In this paper, we have adapted McBride’s ornaments to our universe of datatypes, a cosmetic evolution of an earlier presentation (Chapman *et al.*, 2010). This gave us the

ability to compute over indices, hence introducing the deletion ornament. Deletion ornaments are a key ingredient for the internalisation of Brady's optimisation over inductive families. By applying these ideas, we obtained a simpler implementation of reornaments.

We then developed the notion of functional ornament as a generalisation of ornaments to functions: from a universe of function type, we define a functional ornament as the ornamentation of each of its inductive components. A function of the resulting type will be subject to a coherence property, akin to the ornamental forgetful map of ornaments. We have constructively presented this object by building a small universe of functional ornaments.

We have finally shown how to achieve code reuse by transporting functions along a functional ornament in such a way that the coherence property holds. Instead of asking the user to write cumbersome proofs, we defined a `Patch` type as the type of all the functions that satisfies the coherence property by construction. Hence, we make extensive use of the dependently typed programming machinery: in this setting, the type checker, that is the computer, is working with us to construct a term, not waiting for us to produce a proof.

Having implemented a function correct by construction, one then gets, for free, the lifting and its coherence certificate. This is a straightforward application of the isomorphism between the `Patch` type and the set of coherent functions. These projection functions have been implemented in the type theory by simple generic programming over the universe of functional ornaments.

To further improve code reuse, we provide a few smart constructors to implement a `Patch` type: the idea is to use the structure of the base function to guide the implementation of coherent lifting. Hence, if the base function uses a specific induction principle or returns a specific constructor, we make it possible for the users to specify that they want to lift this structure one level up. This way, the function is not duplicated: only the new information, as determined by the ornament, is necessary.

To conclude, we believe that this is a first yet interesting step towards code reuse for dependently typed programming systems. With ornaments, we were given the ability to organise datatypes by their structure. With functional ornaments, we are now able to organise functions by their structure-preserving computational behaviour. For a large class of functional ornaments, the original program and its lifting share a similar recursion pattern and returned value. To take advantage of this structural similarity, we have developed some appealing automation to assist their implementation, without any proving required, hence making this approach even more accessible.

**Future work** While we have deliberately chosen a simple universe of types, we plan to extend it in various directions. Supporting higher-order functions and adding type dependency ( $\Pi$ -types and  $\Sigma$ -types) is a necessary first step. Inspired by Bernardy & Lasson (2011), we would like to add a parametric quantifier: In the implementation of `ilookup`, we would mark the index  $A$  of `List A` as parametric so that in the `cons a` case, the  $a$  could automatically be carried over.

The universe of functional ornaments could be extended as well, especially once the universe of function types has been extended with dependent quantifiers. For instance, we want to consider the introduction and deletion of quantifiers, as we are currently doing on datatypes. While we have only looked at least fixpoints in this paper, we also want to generalise our universe with greatest fixpoints and the lifting of co-inductive definitions.

Besides enriching the universe, its systematic exploration offers exciting prospects. For pedagogical reasons, this paper is confined to a handful of ornaments (natural numbers to lists, Booleans to the option type, *etc.*) and focuses on two functional ornaments (the comparison and the addition). A quick comparison between natural numbers and lists reveals a few other opportunities, such as the  $--/drop$ ,  $null/head$ , or  $pred/tl$ . Keeping with non-indexed data-structures, a whole zoo of ornaments is available for tree-like structures, depending on whether one stores the data at the leaves, nodes, or both. One could imagine writing the structural operations on the bare structure and to instantiate them for specific data-storage strategies by lifting. Finally, the indexed setting – where ornaments find their *raison d'être* – is most promising. For example, we would like to exploit the fact that the simply typed lambda calculus (Example 3.10) is an ornament of the untyped one and lift its substitution operators from the one defined over the untyped calculus.

### Acknowledgments

We owe many thanks to the ICFP and JFP reviewers, their comments having significantly improved this paper. We are also very grateful to Guillaume Allais, Stevan Andjelkovic, and Peter Hancock for their meticulous reviews of this paper. We shall also thank Edwin Brady for suggesting the study of lookup functions, and Andrea Vezzosi for spotting an issue in our definition of reornaments. Finally, this paper would have remained a draft without the help and encouragement of José Pedro Magalhães. The authors are supported by the Engineering and Physical Sciences Research Council Grant EP/G034699/1.

### References

- Atkey, R., Johann, P & Ghani, N. (2012) Refining inductive types. *Logic. Methods Comput. Sci.* **8**(2), 9. 10.2168/LMCS-8(2:9)2012.
- Benton, N., Hur, C.-K., Kennedy, A. J. & McBride, C. (2012) Strongly typed term representations in coq. *J. Autom. Reason.* **49**(2), 141–159. 10.1007/s10817-011-9219-0.
- Bernardy, J.-P. & Guilhem, M. (2013) Type-theory in color. In *Proceedings of the International Conference on Functional Programming*, pp. 61–72. 10.1145/2500365.2500577.
- Bernardy, J.-P. & Lasson, M. (2011) Realizability and parametricity in pure type systems. *Foundations of Software Science and Computation Structures*, Lecture Notes in Computer Science, vol. 6604. Berlin, Germany: Springer, pp. 108–122. 10.1007/978-3-642-19805-28.
- Bird, R. S. & de Moor, O. (1997). *Algebra of Programming*. Upper Saddle River, NJ: Prentice Hall.

- Brady, E. & Hammond, K. (2010). Scrapping your inefficient engine: Using partial evaluation to improve domain-specific language implementation. In *International Conference in Functional Programming*, pp. 297–308. 10.1145/1863543.1863587.
- Brady, E., McBride, C. & McKinna, J. (2003) Inductive families need not store their indices. *Types for Proofs and Programs*. Berlin, Germany: Springer. 10.1007/978-3-540-24849-18.
- Chapman, J., Dagand, P.-É., McBride, C., & Morris, P. (2010). The gentle art of levitation. In *International Conference on Functional Programming*, pp. 3–14. 10.1145/1863543.1863547.
- Cheney, J. & Hinze, R. (2003) *First-Class Phantom Types*. Technical Report. Cornell University, Ithaca, NY.
- Dagand, P.-E. (2013) *Reusability and Dependent Types*. PhD thesis, University of Strathclyde, Glasgow, UK.
- Dagand, P.-E. & McBride, C. (2012) Transporting functions across ornaments. In *Proceedings of the 17th International Conference on Functional Programming (ICFP 2012)*, pp. 103–114. 10.1145/2364527.2364544.
- Dagand, P.-E. & McBride, C. (2013a) A categorical treatment of ornaments. In *Twenty-Eighth Annual ACM/IEEE Symposium on Logics in Computer Science (LICS 2013)*. 10.1109/LICS.2013.60.
- Dagand, P.-E. & McBride, C. (2013b) Elaborating inductive definitions. *Journées francophones des langages applicatifs*. Available at: <http://hal.inria.fr/hal-00778975>.
- Dybjer, P. (1994) Inductive families. *Form. Asp. Comput.* **6**(4), 440–465. 10.1007/BF01211308.
- Freeman, T. & Pfenning, F. (1991) Refinement types for ML. In *Programming Language Design and Implementation*, pp. 268–277. 10.1145/113445.113468.
- Fumex, C. (2012) *Induction and Coinduction Schemes in Category Theory*. PhD thesis, University of Strathclyde, Glasgow, UK.
- Gonthier, G., Mahboubi, A. & Tassi, E. (2008) *A Small Scale Reflection Extension for the Coq System*. Research Report RR-6455. Valbonne, France: INRIA.
- Hermida, C. & Jacobs, B. (1998) Structural induction and coinduction in a fibrational setting. *Inf. Computat.* **145**(2), 107–152. 10.1006/inco.1998.2725.
- Hofmann, M. & Streicher, T. (1994) The groupoid model refutes uniqueness of identity proofs. *Proceedings of the Symposium on Logic in Computer Science*, pp. 208–212. 10.1109/LICS.1994.316071.
- Ko, H.-S. & Gibbons, J. (2011) Modularising inductive families. *Workshop on Generic Programming*. ACM, pp. 13–24.
- Lindblad, F. & Benke, M. (2004) A tool for automated theorem proving in Agda. In *Types for Proofs and Programs*. Berlin, Germany: Springer, pp. 154–169. 10.1007/1161799010.
- McBride, C. (1999). *Dependently Typed Functional Programs and Their Proofs*. PhD thesis, LFCS, University of Edinburgh, Edinburgh, UK.
- McBride, C. (2002). Elimination with a motive. In *Types for Proofs and Programs*. Berlin, Germany: Springer, 197–216. 10.1007/3-540-45842-513.
- McBride, C. (to appear). Ornamental algebras, algebraic ornaments. *J. Funct. Program.*
- McBride, C., Goguen, H. & McKinna, J. (2004) A few constructions on constructors. *Proceedings of International Workshop, Types for Proofs and Programs (TYPES 2004)*, pp. 186–200 10.1007/1161799012.
- McBride, C. & McKinna, J. (2004). The view from the left. *J. Funct. Program.* **14**(1), 69–111. 10.1007/1178027427.
- Morris, P., Altenkirch, T. & Ghani, N. (2009) A universe of strictly positive families. *Int. J. Found. Comput. Sci.* **20**(1), 83–107. 10.1142/S0129054109006462.

- Paulin-Mohring, C. (1989) *Extraction de Programmes dans le Calcul des Constructions*. PhD thesis, Université Paris VII, France.
- Schrijvers, T., Peyton Jones, S., Sulzmann, M. & Vytiniotis, D. (2009) Complete and decidable type inference for GADTs. In *Proceedings of International Conference on Functional Programming*, pp. 341–352. 10.1145/1596550.1596599.
- Strub, P.-Y. (2010) Coq modulo theory. *Comput. Sci. Logic*. pp. 529–543. 10.1007/978-3-642-15205-440.
- Swamy, N., Chen, J., Fournet, C., Strub, P.-Y., Bhargavan, K. & Yang, J. (2011) Secure distributed programming with value-dependent types. In *Proceedings of International Conference on Functional Programming*, pp. 266–278. 10.1145/2034773.2034811.
- Wadler, P. (1989) Theorems for free! In *Proceedings of Conference on Functional Programming Languages and Computer Architecture*, pp. 347–359. 10.1145/99370.99404.

## Appendix A. Worked example: from comparison to lookup

### A.1 The comparison function

(a) Specify the type of the comparison function:

type< : Type  
 type<  $\mapsto \mu\{\text{Nat-func} \cdot *\} \rightarrow \mu\{\text{Nat-func} \cdot *\} \rightarrow \mu\{\text{Bool-func} \cdot *\} \times 1$

(b) Implement the comparison function:

— < — :  $\llbracket \text{type} < \rrbracket_{\text{Type}}$   
 $m < n \Leftarrow \text{Nat-elim } n$   
 $m < 0 \mapsto \text{false}$   
 $m < (\text{suc } n) \Leftarrow \text{Nat-case } m$   
 $0 < (\text{suc } n) \mapsto \text{true}$   
 $(\text{suc } m) < (\text{suc } n) \mapsto m < n$

### A.2 The functional ornament

(a) Specify the ornamented type of the lookup function:

typeLookup : FunOrn type<  
 typeLookup  $\mapsto \mu^+\{\text{idO Nat-func} \cdot \text{inv } *\} \rightarrow \mu^+\{\text{List-Orn } A \cdot \text{inv } *\} \rightarrow \mu^+\{\text{Maybe-Orn } A \cdot \text{inv } *\} \times 1$

(b) Implement its Patch type:

ilookup : Patch type< typeLookup (— < —)  
 ilookup  $m m^+ n vs \{\ ? \}$

(c) Lift the induction:

ilookup : Patch type< typeLookup (— < —)  
 ilookup  $m m^+ n vs \overset{\text{lift}}{\Leftarrow} \text{lift-ind} \{\ ? \}$   
 ilookup  $m m^+ 0 \text{ nil} \{\ ? \}$   
 ilookup  $m m^+ (\text{suc } n) (\text{cons } a vs) \{\ ? \}$

(d) Lift the case analysis:

```

illookup : Patch type< typeLookup (− < −)
illookup  m    m+  n    vs     $\stackrel{\text{lift}}{\Leftarrow}$  lift-ind
illookup  m    m+  0    nil     $\{\ ? \}$ 
illookup  m    m+  (suc n) (cons a vs)  $\stackrel{\text{lift}}{\Leftarrow}$  lift-case
illookup  0    0    0    nil     $\{\ ? \}$ 
illookup (suc m) (suc m+) 0    nil     $\{\ ? \}$ 
    
```

(e) Lift the constructors:

```

illookup : Patch type< typeLookup (− < −)
illookup  m    m+  n    vs     $\stackrel{\text{lift}}{\Leftarrow}$  lift-ind
illookup  m    m+  0    nil     $\mapsto$  nothing *[*]
illookup  m    m+  (suc n) (cons a vs)  $\stackrel{\text{lift}}{\Leftarrow}$  lift-case
illookup  0    0    (suc n) (cons a vs)  $\mapsto$  just {a : A} [*]
illookup (suc m) (suc m+) (suc n) (cons a vs)  $\{\ ? \}$ 
    
```

(f) Finish the definition:

```

illookup : Patch type< typeLookup (− < −)
illookup  m    m+  n    vs     $\stackrel{\text{lift}}{\Leftarrow}$  lift-ind
illookup  m    m+  0    nil     $\mapsto$  nothing *[*]
illookup  m    m+  (suc n) (cons a vs)  $\stackrel{\text{lift}}{\Leftarrow}$  lift-case
illookup  0    0    (suc n) (cons a vs)  $\mapsto$  just a[*]
illookup (suc m) (suc m+) (suc n) (cons a vs)  $\mapsto$  illookup m m+ n vs
    
```

### A.3 Extracting the lookup function

(a) Obtain the lookup function by applying the patch:

```

lookup :  $\llbracket$ typeLookup $\rrbracket_{\text{FunOrn}}$ 
lookup  $\mapsto$  patch typeLookup (− < −) illookup
    
```

(b) Obtain a proof of its coherence:

```

cohLookup (n : Nat) (xs : List A) : isJust (lookup n xs) = n < length xs
cohLookup  n    xs     $\mapsto$  coherence typeLookup (− < −) illookup n xs
    
```



## Appendix B. Definitions

### B.1 Universe of descriptions

<b>data</b> $\text{IDesc } [I : \text{SET}] : \text{SET}_1$ <b>where</b>	$\llbracket (D : \text{IDesc } I) \rrbracket (X : I \rightarrow \text{SET}) : \text{SET}$
$\text{IDesc } I \ni \text{var } (i : I)$	$\llbracket \text{var } i \rrbracket X \mapsto X \ i$
$\quad   \ 1$	$\llbracket 1 \rrbracket X \mapsto \mathbb{1}$
$\quad   \ \Pi (S : \text{SET}) (T : S \rightarrow \text{IDesc } I)$	$\llbracket \Pi S \ T \rrbracket X \mapsto (s : S) \rightarrow \llbracket T \ s \rrbracket X$
$\quad   \ \Sigma (S : \text{SET}) (T : S \rightarrow \text{IDesc } I)$	$\llbracket \Sigma S \ T \rrbracket X \mapsto (s : S) \times \llbracket T \ s \rrbracket X$
<b>func</b> $(I : \text{SET}) : \text{SET}_1$	$\llbracket (D : \text{func } I) \rrbracket (X : I \rightarrow \text{SET}) : I \rightarrow \text{SET}$
<b>func</b> $I \mapsto I \rightarrow \text{IDesc } I$	$\llbracket D \rrbracket X \mapsto \lambda i. \llbracket D \ i \rrbracket X$

Code and interpretation

<b>data</b> $\mu [D : \text{func } I](i : I) : \text{SET}$ <b>where</b>
$\mu D \ i \ni \text{in } (xs : \llbracket D \rrbracket (\mu D) \ i)$
<b>induction</b> $:\forall P : \forall i : I. \mu D \ i \rightarrow \text{SET}.$
$(\alpha : (i : I)(xs : \llbracket D \rrbracket (\mu D) \ i) \rightarrow \square_D P \ xs \rightarrow P \ (\text{in } xs))$
$(x : \mu D \ i) \rightarrow P \ x$

Least fixpoint and induction principle

### B.2 Universe of ornaments

<b>data</b> $\text{Orn } (D : \text{IDesc } K)[u : I \rightarrow K] : \text{SET}_1$ <b>where</b>	
$\text{-- Extend with } S :$	
$\text{Orn } D \ u \ni \text{insert } (S : \text{SET})$	$\llbracket (O : \text{Orn } D \ u) \rrbracket_{\text{orn}} : \text{IDesc } I$
$\quad (D^+ : S \rightarrow \text{Orn } D \ u)$	$\llbracket \text{insert } S \ D^+ \rrbracket_{\text{orn}} \mapsto \Sigma S \ \lambda s. \llbracket D^+ \ s \rrbracket_{\text{orn}}$
$\text{-- Refine index:}$	
$\text{Orn } (\text{var } k) \ u \ni \text{var } (i : u^{-1} k)$	$\llbracket \text{var } (\text{inv } i) \rrbracket_{\text{orn}} \mapsto \text{var } i$
$\text{-- Copy the original:}$	
$\text{Orn } 1 \ u \ni 1$	$\llbracket 1 \rrbracket_{\text{orn}} \mapsto 1$
$\text{Orn } (\Pi S \ T) \ u \ni \Pi (T^+ : (s : S) \rightarrow \text{Orn } (T \ s) \ u)$	$\llbracket \Pi T^+ \rrbracket_{\text{orn}} \mapsto \Pi S \ \lambda s. \llbracket T^+ \ s \rrbracket_{\text{orn}}$
$\text{Orn } (\Sigma S \ T) \ u \ni \Sigma (T^+ : (s : S) \rightarrow \text{Orn } (T \ s) \ u)$	$\llbracket \Sigma T^+ \rrbracket_{\text{orn}} \mapsto \Sigma S \ \lambda s. \llbracket T^+ \ s \rrbracket_{\text{orn}}$
$\text{-- Delete } S :$	
$\quad   \ \text{delete } (s : S)$	$\llbracket \text{delete } s \ T^+ \rrbracket_{\text{orn}} \mapsto \llbracket T^+ \rrbracket_{\text{orn}}$
$\quad \quad (T^+ : \text{Orn } (T \ s) \ u)$	
<b>orn</b> $(D : \text{func } K) (u : I \rightarrow K) : \text{SET}_1$	$\llbracket (o : \text{orn } D \ u) \rrbracket_{\text{orn}} : \text{func } I$
<b>orn</b> $D \ u \mapsto (i : I) \rightarrow \text{Orn } (D \ (u \ i)) \ u$	$\llbracket o \rrbracket_{\text{orn}} \mapsto \lambda i. \llbracket o \ i \rrbracket_{\text{orn}}$

Code and interpretation

$\text{forgetNT} : (o : \text{orn } D \ u) \rightarrow \llbracket o \rrbracket (X \circ u) \ i \rightarrow \llbracket D \rrbracket X \ (u \ i)$
$\text{forgetAlg} : (o : \text{orn } D \ u) \rightarrow \llbracket o \rrbracket_{\text{orn}} (\mu D \circ u) \ i \rightarrow \mu D \ (u \ i)$
$\text{forget} : (o : \text{orn } D \ u) \rightarrow \mu \llbracket o \rrbracket_{\text{orn}} i \rightarrow \mu D \ (u \ i)$

Ornamental algebra

$(D : \text{func } K)^{\langle \alpha \rangle} \llbracket D \rrbracket^{X \rightarrow X} : \text{orn } D (\pi_0 : (k : K) \times X \ k \rightarrow K)$   
 $\text{coherentOrn} : (t^\alpha : \mu \llbracket D^\alpha \rrbracket_{\text{orn}}(k, x)) \rightarrow \langle \alpha \rangle (\text{forget } D^\alpha \ t^\alpha) = x$   
 $\text{make } (D : \text{func } I)^{\langle \alpha \rangle} \llbracket D \rrbracket^{X \ i \rightarrow X \ i} : (t : \mu \ D \ k) \rightarrow \mu \llbracket D^\alpha \rrbracket_{\text{orn}}(k, \langle \alpha \rangle \ t)$

Algebraic ornament

$\llbracket (o : \text{orn } D \ u) \rrbracket : \text{orn } \llbracket o \rrbracket_{\text{orn}} (\pi_0 : (k : K) \times X \ k \rightarrow K)$

Reornament

**B.3 Universe of function types**

**data** Type : SET<sub>1</sub> **where**  
 Type  $\ni \mu \{ (D : \text{func } K) \cdot (k : K) \} \rightarrow (T : \text{Type})$   
           |  $\mu \{ (D : \text{func } K) \cdot (k : K) \} \times (T : \text{Type})$   
           | 1  
  
 $\llbracket (T : \text{Type}) \rrbracket_{\text{Type}} : \text{SET}$   
 $\llbracket \mu \{ D \cdot k \} \rightarrow T \rrbracket_{\text{Type}} \mapsto \mu \ D \ k \rightarrow \llbracket T \rrbracket_{\text{Type}}$   
 $\llbracket \mu \{ D \cdot k \} \times T \rrbracket_{\text{Type}} \mapsto \mu \ D \ k \times \llbracket T \rrbracket_{\text{Type}}$   
 $\llbracket 1 \rrbracket_{\text{Type}} \mapsto \mathbb{1}$

Code and interpretation

**B.4 Universe of functional ornaments**

**data** FunOrn (T : Type) : SET<sub>1</sub> **where**  
 FunOrn  $(\mu \{ D \cdot k \} \rightarrow T) \ni \forall u : I \rightarrow K. \mu^+ \{ (o : \text{orn } D \ u) \cdot (i : u^{-1} \ k) \} \rightarrow (T^+ : \text{FunOrn } T)$   
 FunOrn  $(\mu \{ D \cdot k \} \times T) \ni \forall u : I \rightarrow K. \mu^+ \{ (o : \text{orn } D \ u) \cdot (i : u^{-1} \ k) \} \times (T^+ : \text{FunOrn } T)$   
 FunOrn 1  $\ni 1$   
  
 $\llbracket (T^+ : \text{FunOrn } T) \rrbracket_{\text{FunOrn}} : \text{SET}$   
 $\llbracket \mu^+ \{ o \cdot \text{inv } i \} \rightarrow T^+ \rrbracket_{\text{FunOrn}} \mapsto \mu \llbracket o \rrbracket_{\text{orn}} \ i \rightarrow \llbracket T^+ \rrbracket_{\text{FunOrn}}$   
 $\llbracket \mu^+ \{ o \cdot \text{inv } i \} \times T^+ \rrbracket_{\text{FunOrn}} \mapsto \mu \llbracket o \rrbracket_{\text{orn}} \ i \times \llbracket T^+ \rrbracket_{\text{FunOrn}}$   
 $\llbracket 1 \rrbracket_{\text{FunOrn}} \mapsto \mathbb{1}$

Code and interpretation

Coherence (T<sup>+</sup> : FunOrn T) (f :  $\llbracket T \rrbracket_{\text{Type}}$ ) (f<sup>+</sup> :  $\llbracket T^+ \rrbracket_{\text{FunOrn}}$ ) : SET  
 Coherence (μ<sup>+</sup>{o · inv i} → T<sup>+</sup>) f f<sup>+</sup>  $\mapsto$   
           (x<sup>+</sup> : μ  $\llbracket o \rrbracket_{\text{orn}}$  i) → Coherence T<sup>+</sup> (f (forget o x<sup>+</sup>)) (f<sup>+</sup> x<sup>+</sup>)  
 Coherence (μ<sup>+</sup>{o · inv i} × T<sup>+</sup>) (x, xs) (x<sup>+</sup>, xs<sup>+</sup>)  $\mapsto$   
           forget o x<sup>+</sup> = x × Coherence T<sup>+</sup> xs xs<sup>+</sup>  
 Coherence 1 \* \*  $\mapsto \mathbb{1}$

Coherence

**B.5 Patches**

Patch	$(T : \text{Type})$	$(T^+ : \text{FunOrn } T)$	$(f : \llbracket T \rrbracket_{\text{Type}})$	$:\text{ SET}$
Patch	$(\mu\{D \cdot u\} \rightarrow T)$	$(\mu^+\{o \cdot \text{inv } i\} \rightarrow T^+)$	$f$	$\mapsto$
	$(x : \mu D (u i)) \rightarrow \mu \llbracket [o] \rrbracket_{\text{orn}} (i, x)$		$\rightarrow \text{Patch } T T^+ (f x)$	
Patch	$(\mu\{D \cdot u\} \times T)$	$(\mu^+\{o \cdot \text{inv } i\} \times T^+)$	$(x, xs)$	$\mapsto$
	$\mu \llbracket [o] \rrbracket_{\text{orn}} (i, x) \times \text{Patch } T T^+ xs$			
Patch	1	1	*	$\mapsto \mathbb{1}$

Patch

patch	$(T^+ : \text{FunOrn } T)$	$(f : \llbracket T \rrbracket_{\text{Type}})$	$(f^{++} : \text{Patch } T T^+ f)$	$:\llbracket T^+ \rrbracket_{\text{FunOrn}}$
patch	$(\mu^+\{o \cdot \text{inv } i\} \rightarrow T^+)$	$f$	$f^{++}$	$\mapsto$
	$\lambda x^+. \text{patch } T^+ (f (\text{forget } o x^+))$			
			$(f^{++} (\text{forget } o x^+) (\text{make } [o] x^+))$	
patch	$(\mu^+\{o \cdot \text{inv } i\} \times T^+)$	$(x, xs)$	$(x^{++}, xs^{++})$	$\mapsto$
	$(\text{forget } [o] x^{++}, \text{patch } T^+ xs xs^{++})$			
patch	1	*	*	$\mapsto *$
coherence	$(T^+ : \text{FunOrn } T)$	$(f : \llbracket T \rrbracket_{\text{Type}})$	$(f^{++} : \text{Patch } T T^+ f)$	$:\text{Coherence } T^+ f (\text{patch } T^+ f f^{++})$
coherence	$(\mu^+\{o \cdot \text{inv } i\} \rightarrow T^+)$	$f$	$f^{++}$	$\mapsto$
	$\lambda x^+. \text{coherence } T^+ (f (\text{forget } o x^+))$			
			$(f^{++} (\text{forget } o x^+) (\text{make } [o] x^+))$	
coherence	$(\mu^+\{o \cdot \text{inv } i\} \times T^+)$	$(x, xs)$	$(x^+, xs^{++})$	$\mapsto$
	$(\text{coherentOrn } x^+, \text{coherence } T^+ xs xs^{++})$			
coherence	1	*	*	$\mapsto *$

Patching and its coherence proof

**B.6 Transporting recursion patterns**

lift <sub>Alg</sub>	$(\alpha : \forall k : K. \llbracket D \rrbracket (\lambda - . \llbracket T \rrbracket_{\text{Type}}) k \rightarrow \llbracket T \rrbracket_{\text{Type}})$	$(o : \text{orn } D u)$	$(T^+ : \text{FunOrn } T)$	$:\text{ SET}$
lift <sub>Alg</sub>	$\alpha o T^+ \mapsto \forall (i, t) : (i : I) \times \mu D (u i).$			
	$\llbracket [o] \rrbracket_{\text{orn}} (\lambda (i, t). \text{Patch } T T^+ ((\alpha) t)) (i, t)$		$\rightarrow \text{Patch } T T^+ ((\alpha) t)$	
lift-fold	$(\alpha : \forall k : K. \llbracket D \rrbracket (\lambda - . \llbracket T \rrbracket_{\text{Type}}) k \rightarrow \llbracket T \rrbracket_{\text{Type}})$			
	$(\alpha^{++} : \text{lift}_{\text{Alg}} \alpha o T^+)$	$:\text{ Patch } (\mu\{D \cdot u\} \rightarrow T)$	$(\mu^+\{o \cdot \text{inv } i\} \rightarrow T^+)$	$(\llbracket \alpha \rrbracket)$
lift-fold	$\alpha \alpha^{++} \mapsto \lambda x. \lambda x^{++}. \llbracket \alpha^{++} \rrbracket x^{++}$			

Coherent algebra and its lifting

$\text{lift}_{\text{IH}} (\alpha : (k : K)(xs : \llbracket D \rrbracket (\mu D) k) \rightarrow \square_D (\lambda - . \llbracket T \rrbracket_{\text{Type}}) xs \rightarrow \llbracket T \rrbracket_{\text{Type}})$   
 $(o : \text{orn } D u)(T^+ : \text{FunOrn } T) : \text{SET}$   
 $\text{lift}_{\text{IH}} \alpha o T^+ \mapsto ((i, t) : (i : I) \times \mu D (u i)) \rightarrow (xs : \llbracket [o] \rrbracket_{\text{orn}} (\mu \llbracket [o] \rrbracket_{\text{orn}}) (i, t)) \rightarrow$   
 $\square_{\llbracket [o] \rrbracket_{\text{orn}}} (\lambda(i, t). \text{Patch } T T^+ (\text{induction } \alpha t)) xs \rightarrow$   
 $\text{Patch } T T^+ (\text{induction } \alpha t)$   
 $\text{lift-ind } (\alpha : (k : K)(xs : \llbracket D \rrbracket (\mu D) k) \rightarrow \square_D (\lambda - . \llbracket T \rrbracket_{\text{Type}}) xs \rightarrow \llbracket T \rrbracket_{\text{Type}})$   
 $(\alpha^{++} : \text{lift}_{\text{IH}} \alpha o T^+) : \text{Patch } (\mu\{D \cdot u i\} \rightarrow T) (\mu^+\{o \cdot \text{inv } i\} \rightarrow T^+) (\text{induction } \alpha)$   
 $\text{lift-ind } \alpha \alpha^{++} \mapsto \lambda x. \lambda x^{++}. \text{induction } \alpha^{++} x^{++}$

Coherent inductive step and its lifting

$\text{lift-constructor } (e : \text{Extension } (o i) xs) \quad \text{-- coherent extension}$   
 $(a : \text{Structure } (o i) xs e) \quad \text{-- recursive arguments}$   
 $(t^{++} : \text{Patch } T T^+ t)$   
 $: \text{Patch } (\mu\{D \cdot u i\} \times T) (\mu^+\{o \cdot \text{inv } i\} \times T^+) (\text{in } xs, t)$   
 $\text{lift-constructor } e a t^{++} \mapsto (\text{in } (\text{mkReorn } (o i) xs e a), t^{++})$

Constructor lifting