

Notiz: Der Code für alle 3 Ansätze ist quasi fertig. Aktuell schreibe ich also fast ausschließlich an der Arbeit an sich. Dieses PDF ist eine unfertige Arbeitsversion. Einige bereits geschriebene Abschnitte sind noch unfertig oder an der falschen Position in der Arbeit.

# Implementing a library for scoped algebraic effects in Agda

HTWK Leipzig

Jonas Höfer  
Informatik  
69555

2020

## **Abstract**

# Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Goals . . . . .	4
1.2	Structure . . . . .	4
<b>2</b>	<b>Preliminaries</b>	<b>5</b>
2.1	Agda . . . . .	5
2.1.1	Basic Syntax . . . . .	5
2.1.2	Dependent Types . . . . .	5
2.1.3	Propositions as Types . . . . .	7
2.1.4	Notions of Equality and Equality Types . . . . .	7
2.1.5	Termination Checking . . . . .	8
2.1.6	Strict Positivity . . . . .	9
2.2	Curry . . . . .	10
2.2.1	Call-Time-Choice . . . . .	11
2.2.2	Permutation Sort . . . . .	11
2.3	Algebraic Computational Effects . . . . .	11
2.3.1	Algebraic Theories . . . . .	12
2.3.2	Effect Handler . . . . .	13
2.3.3	Free Monad . . . . .	13
2.3.4	Scoped Effects . . . . .	13
<b>3</b>	<b>First Order</b>	<b>14</b>
3.1	Functors à la carte . . . . .	14
3.1.1	The Free Monad for Effect Handling . . . . .	16
3.1.2	Properties . . . . .	17
3.2	Handler . . . . .	17
3.2.1	Nondeterministic Choice . . . . .	18
3.2.2	State . . . . .	20
3.2.3	Handling Combined Effects . . . . .	21
3.3	Effects with Scopes using Brackets . . . . .	22
3.3.1	Cut and Call . . . . .	22
3.4	Call-Time Choice as Effect . . . . .	24
3.4.1	Deep Effects . . . . .	24
3.4.2	Sharing Handler . . . . .	25
3.4.3	Share Operator . . . . .	26
3.4.4	Examples . . . . .	27
3.4.5	Laws of Sharing . . . . .	28
<b>4</b>	<b>Higher Order Syntax</b>	<b>29</b>
4.1	Higher Order Syntax . . . . .	29
4.2	Representing Strictly Positive Higher Order Functors . . . . .	29
4.3	Effectful Data and Existential Types . . . . .	31
4.4	The Problem with Indexing . . . . .	32

<b>5</b>	<b>Scoped Algebras</b>	<b>33</b>
5.1	The Monad $E$ . . . . .	33
5.2	The <b>Prog</b> Monad . . . . .	34
5.2.1	Folds for Nested Data Types . . . . .	34
5.2.2	Induction Schemes for Nested Data Types . . . . .	36
5.2.3	Proving the Monad Laws . . . . .	37
5.3	Combining Effects . . . . .	38
5.4	Nondet . . . . .	38
5.4.1	As Scoped Algebra . . . . .	39
5.4.2	As Modular Handler . . . . .	40
5.5	Exceptions . . . . .	42
5.6	State . . . . .	42
5.7	Share . . . . .	43
<b>6</b>	<b>Conclusion</b>	<b>46</b>
6.1	Summary . . . . .	46

# Chapter 1

## Introduction

Algebraic effects and their handlers, first introduced by Plotkin, Powers and Pretnar [TODO; PP09], are a theoretical well studied representation for certain computational effects.

Algebraic effects are generally more modular than traditional monad transformers. Wu et al. noticed a lack of modularity when combining multiple operations with scopes. They introduced several solutions for the problem, by using new syntax to delimit scopes.

### 1.1 Goals

The goal of this thesis is the implementation of an effect library based on the work by Wu et al. [WSH14; Pir+18] in the dependently typed, functional programming language Agda [Nor07]. To allow use as a proof assistant, Agda programs are subject to constraints not present in other functional languages such as Haskell. All Agda programs have to be total (and therefore terminate), all data types have to be strictly positive and all universe levels have to be consistent. These restrictions prevent a direct translation of Haskell code to Agda.

This thesis will explore multiple Haskell implementations of scoped effects and study how well these translate to Agda. Furthermore it will present a set of standard solutions for common problems, arising during the implementation of the three approaches.

Agda’s builtin theorem proving capabilities allow direct, machine checked correctness proofs for the implemented library. Alongside the implementation of scoped effects, the library should contain proofs for common properties of these effects. Furthermore, the library itself can be used to simulate semantics of other programming languages, such as Curry’s call-time choice, and allow verification of equivalent programs written in these languages in Agda. To allow the latter, these library should be able to represent deep effects i.e. data structures with effectful components.

### 1.2 Structure

Chapter 2 contains short introductions to Agda and dependent types, Curry and its call-time choice semantics (which are a central example for a scoped effect throughout the thesis) and algebraic effects.

Chapter 3 and 4 explore the two approaches based on “Effect Handlers in Scope” by Wu et al. The former of the two approaches was already partially explored by Bunkeburg in Coq and can also be implemented easily in Agda. The latter of the two approaches tries to fix some inherent problems of the first one, but sadly cannot fully be implemented in Agda due to some inherent problems with universe consistency.

Chapter 5 describes an implementation of a novel representation for scoped effects by Piróg et al. [Pir+18] which also fixes the problems of the first approach, while avoiding the universe inconsistencies of the second one. Furthermore, the implementation explores some ideas to modularize the exemplary Haskell implementation by Piróg et al.

# Chapter 2

## Preliminaries

### 2.1 Agda

Agda is a dependently typed functional programming language. The current version<sup>1</sup> was originally developed by Ulf Norell under the name Agda2 [Nor07]. Due to its type system Agda can be used as a programming language and as a proof assistant.

This section contains a short introduction to Agda, dependent types and the idea of “Propositions as types” under which Agda can be used for theorem proving.

#### 2.1.1 Basic Syntax

Agda's syntax is similar to Haskell's. Data types are declared with syntax similar to Haskell's GADTs. Functions declarations and definitions are also similar to Haskell, except that Agda uses a single colon for the typing relation. In the following definition of `N`, `Set` is the type of all (small) types.

```
data N : Set where
  zero : N
  suc  : N → N
```

Ordinary function definitions are syntactically similar to Haskell. Agda allows the definition of infix operators. A infix operator is an arbitrary list of symbols (builtin symbols like colons are not allowed as part of operators). Underscores in the operator name are placeholders for future parameters. A infix operator can be applied partially by writing underscores for the omitted parameters.

In the following definition of plus for natural numbers `+` is a binary operator and therefore contains two underscores.

```
_+_ : N → N → N
zero + m = m
suc n + m = suc (n + m)
```

#### 2.1.2 Dependent Types

The following type theoretic definitions are taken from the homotopy type theory book [Uni13]. In type theory a type of types is called a universe. Universes are usually denoted  $\mathcal{U}$ . A function whose codomain is a universe is called a type family or dependent type.

$$F : A \rightarrow \mathcal{U} \quad \text{where} \quad B(a) : \mathcal{U} \quad \text{for} \quad a : A$$

To avoid Russell's paradox, a hierarchy of universes  $\mathcal{U}_1 : \mathcal{U}_2 : \dots$  is introduced. Usually the universes are cumulative i.e. if  $\tau : \mathcal{U}_n$  then  $\tau : \mathcal{U}_k$  for  $k > n$ . by default this is not the case in Agda. Each type is member of a unique universe, forcing us to do additional bookkeeping. Since Agda 2.6.1 an experimental `--cumulativity` flag exists.

---

<sup>1</sup><https://github.com/agda/agda>

**Dependent Function Types ( $\Pi$ -Types)** are a generalization of function types. The codomain of a  $\Pi$  type is not fixed, but values with the argument the function is applied to. The codomain is defined using a type family of the domain, which specifies the type of the result for each given argument.

$$\prod_{a:A} B(a) \quad \text{with} \quad B : A \rightarrow \mathcal{U}$$

An element of the above type is a function which maps every  $a : A$  to a  $b : B(a)$ . In Agda the builtin function type  $\Rightarrow$  is a  $\Pi$ -type. An argument can be named by replacing the type  $\tau$  with  $x : \tau$ , allowing us to use the value as part of later types.

**Dependent Sum Types ( $\Sigma$ -Types)** are a generalization of product types. The type of the second component of the product is not fixed, but varies with the value of the first.

$$\sum_{a:A} B(a) \quad \text{with} \quad B : A \rightarrow \mathcal{U}$$

An element of the above type is a pair consisting of an  $a : A$  and a  $b : B(a)$ . In Agda **records** represent  $n$ -ary  $\Sigma$ -types. Each field can be used in the type of the following fields.

**Programming with Dependent Types** A common example for dependent types are fixed length vectors. The data type depends on a type **A** and a value of type **N**.

```
data Vec (A : Set) : N → Set where
  _::_ : {n : N} → A → Vec A n → Vec A (suc n)
  []   : Vec A 0
```

Arguments on the left-hand side of the colon are called parameters and are the same for all constructors. Arguments on the right-hand side of the colon are called indices and can differ for each constructor. Therefore **Vec A** is a family of types indexed by **N**.

The **[]** constructor allows us to create an empty vector of any type, but forces the index to be zero. The **\_::\_** constructor appends an element to the front of a vector of the same element type and increases the index by 1. Only these two constructors can be used to construct vectors. Therefore the index is always equal to the amount of elements stored in the vector.

By encoding more information about data in its type we can add extra constraints to functions working with it. The following definition of **head** avoids error handling or partiality by excluding the empty vector as a valid argument.

```
head : ∀ {A n} → Vec A (suc n) → A
head (x :: _) = x
```

When pattern matching on the argument of **head** there is no case for **[]**. The argument has type **Vec A (suc n)** and **[]** has type **Vec A 0**. Those two types cannot be unified, because **suc** and **zero** are different constructors of **N**. Therefore, the **[]** case does not apply. By constraining the type of the function we were able to avoid the case, which usually requires error handling or introduces partiality.

We can extend this idea to type safe indexing. A vector of length  $n$  is indexed by the first  $n$  natural numbers. The type **Fin n** represents the subset of natural numbers smaller than  $n$ .

```
data Fin : N → Set where
  zero : {n : N} → Fin (suc n)
  suc   : {n : N} → Fin n → Fin (suc n)
```

Because 0 is smaller than every positive natural number, **zero** can only be used to construct an element of **Fin (suc n)** i.e. for every type except **Fin 0**.

If any number is smaller than  $n$ , then its successor is smaller than  $n + 1$ . Therefore, if any number is an element of **Fin n** then its successor is an element of **Fin (suc n)**.

So we can construct a  $k < n$  of type **Fin n** by starting with **zero** of type **Fin (n - k)** and applying **suc k** times. Using this definition of the bounded subsets of natural numbers we can define **!\_** for vectors.



```

_!_ : ∀ {A n} → Vec A n → Fin n → A
(x :: _) ! zero = x
(_ :: xs) ! suc i = xs ! i

```

Notice that similar to `head` there is no case for `[]`. `n` is used as index for `Vec A` and `Fin`. The constructors for `Fin` only use `suc`, therefore the type `Fin zero` is not inhabited and the cases for `[]` do not apply.

By case splitting on the vector first we could have obtained the term `[] ! i`. By case splitting on `i` we notice that no constructor for `Fin zero` exists. Therefore, this case cannot occur, because the type of the argument is uninhabited. It's impossible to call the function, because we cannot construct an argument of the correct type. In this example we can either omit the case or explicitly state that the argument is impossible to construct, by replacing it with `()`, allowing us to omit the definition of the right-hand side of the equation.

```

[] ! () -- no right-hand side

```

The other two cases are straightforward. For index `zero` we return the head of the vector. For index `suc i` we call `_!_` recursively with the smaller index and the tail of the vector. Notice that the types for the recursive call change. The tail of the vector `xs` and the smaller index `i` are indexed over the predecessor of `n`.

### 2.1.3 Propositions as Types

An more in depth explanation and an overview over the history of the idea can be found in Wadlers paper of the same name [Wad15].

FOL	MLTT	Agda
$\forall x \in A : P(x)$	$\prod_{x:A} P(x)$	$(x : A) \rightarrow P\ x$
$\exists x \in A : P(x)$	$\sum_{x:A} P(x)$	$\Sigma [ x \in A ] P\ x$ mit $\_,_ : (x : A) \rightarrow P\ x \rightarrow \Sigma A\ P$
$P \wedge Q$	$P \times Q$	$A \times B$
$P \vee Q$	$P + Q$	$A \uplus B$
$P \Rightarrow Q$	$P \rightarrow Q$	$A \rightarrow B$
<b>t</b>	<b>1</b>	<b>tt</b> : $\top$
<b>f</b>	<b>0</b>	$\perp$

### 2.1.4 Notions of Equality and Equality Types

In the last section we saw how we can encode propositions from propositional and predicate logic as types. One of the most important proposition is equality i.e. the proposition that given two terms  $a, b : A$  that  $a$  and  $b$  are equal. When using Agda for theorem proving we have to express propositions like  $a + b = b + a$  and  $2 = 1$ , which could be true or false, to be able to prove or disprove them. In type theory and therefore in Agda we have to consider different notions of equality.

When defining a program rule like `truth = 42` we are making an *equality judgement*. The symbol `truth` is *definitional equal* to `42`. A judgment is always true. We define one term to be equal to another one i.e. we allow Agda to reduce the left hand side of the equality to the right hand side.

The next notion of equality is *computational equality*. Two terms  $t_1$  and  $t_2$  are computational equal if they reduce to the same term. For example, given the above definition of `+` the terms  $0 + (0 + n)$  and  $n$  are computational equal, because using the first rule in the definition of plus  $0 + (0 + n)$   $\beta$ -reduces to  $n$ . On the other hand  $n + 0$  and  $n$  are not computational equal, because for a free variable  $n$  none of the program rules for `+` can be used to reduce the term further. Therefore computational equality is not the right notion of equality, because the later equality should also hold.

To talk about the equality of two terms we have to use *propositional equality* i.e. we have to define a proposition representing the fact that two terms of type  $A$  are equal. This proposition is usually encapsulated in an *equality type* of  $A$ .

```

infix 4 _≡_
data _≡_ {A : Set} (x : A) : A → Set where
  refl : x ≡ x

```

The type  $x \equiv y$  represents the proposition that  $x$  and  $y$  are equal. The only way to construct evidence for the proposition is using the `refl` constructor i.e. if  $x$  and  $y$  are actually the same.

This notion of equality has the usually expected properties like transitivity, symmetry and congruence. The definition of `cong` shows the typical way of working with equality proofs.

```
cong : ∀ {A B x y} → (f : A → B) → x ≡ y → f x ≡ f y
cong f refl = refl
```

We expect that  $\equiv$  is a congruence relation i.e. if  $x$  and  $y$  are equal then  $fx$  and  $fy$  should also be equal. We cannot produce a value of type  $fx \equiv fy$  because the two are not equal. By pattern matching in the argument of type  $x \equiv y$  i.e. by inspecting the evidence that  $x$  and  $y$  are equal we obtain more information about the goal. Because `refl` can only be constructed if the two values are the same the two variables are unified. We therefore have to produce a proof that  $fx$  is equal to itself, which is given by reflexivity.

By pattern matching on variables used in the equality type we can obtain more information about the goal. Either because the constructors themselves restrict the use of the variables or because the terms used in the equality type can be reduced further. Consider the following example.

```
+identr : ∀ n → n + 0 ≡ n
+identr 0      = refl
+identr (suc m) = cong suc (+identr m)
```

By pattern matching on the variable  $n$  we obtain two cases, one for each constructor (this is analogous to a proof by exhaustion). In both cases the term  $n + 0$  can now be reduced further. In the `0` case we obtain  $0 + 0$  on the left hand side, which can be reduced to `0`. The return type simplifies to  $0 \equiv 0$  for which we can simply construct evidence using `refl`.

The second case is more complex. The left hand side still contains the free variable  $m$ , but reduces to `suc (m + 0)` using the second rule for `+_+`. Using a recursive call we obtain evidence for  $m + 0 \equiv m$ . The recursive call to obtain evidence for a smaller case corresponds to the use of the induction hypothesis in an inductive proof. By applying `suc` on both sides of the equality we obtain a proof for the correct proposition.

We obtained a non obvious equality by using just definitional and computational equality together with the analogs of proofs by exhaustion and induction. This proof can now be used to rewrite arbitrary terms containing terms corresponding to or containing the left- or right-hand of the equality.

### 2.1.5 Termination Checking

The definition of non-terminating functions entails logical inconsistency. Agda therefore only allows the definition of terminating functions. Due to the undecidability of the halting problem Agda uses a heuristic termination checker. The termination checker proves termination by observing structural recursion. Consider the following definitions of `List` and `map`.

```
data List (A : Set) : Set where
  _::_ : A → List A → List A
  []    : List A

map : {A B : Set} → (A → B) → (List A → List B)
map f (x :: xs) = f x :: map f xs
map f []       = []
```

The `[]` case does not contain a recursive call. In the `_::_` case the recursive call to `map` occurs on a structural smaller argument i.e.  $xs$  is a subterm of the argument  $x :: xs$ . Because elements of `List A` are finite the function `map` terminates for every argument.

### Sized Types

In more complex recursive functions the structural recursion can be obscured. Agda does not inline functions containing pattern matches during termination checking and therefore cannot prove the termination. A common example are recursive calls in lambdas, which are passed to higher order functions like `map` and `>>=`.

Consider a monad like `List` or `Maybe`. It is not obvious that the argument of the continuation of `>>=` is a subterm of the first argument.

TODO: explain better via [SEMI-CONTINUOUS SIZED TYPES AND TERMINATION ABEL]

A possibility to still proof termination are Sized Types. Agda has a special builtin, well-ordered type `Size`.

```
open import Agda.Builtin.Size public
renaming ( SizeU to SizeUniv ) -- sort SizeUniv
using ( Size                -- Size : SizeUniv
      ; Size<_              -- Size<_ : Size → SizeUniv
      ; ↑_                  -- ↑_ : Size → Size
      ; _⊔^s_               -- _⊔^s_ : Size → Size → Size
      ; ∞ )                -- ∞ : Size
```

By augmenting a data type with an index of type `Size` its size can be represented on the type level. If a value of type `Size` decreases with every recursive call, the functions has to termination, because there exist no infinitely decreasing chains on elements of `Size`.

A common idiom for data types is to mark all non-inductive constructors and recursive occurrences with an arbitrary size  $i$  and all inductive constructors with the next larger size  $↑ i$ . The size therefore corresponds to the height of the tree described by the term (+ the initial height for the lowest non-inductive constructor).

A common example for sized types are rose trees. The size index can be intuitively thought of as the height of the tree.

```
data Rose (A : Set) : Size → Set where
  rose : ∀ {i} → A → List (Rose A i) → Rose A (↑ i)
```

When `fmap` for rose trees is defined in terms of `map` the termination is obscured. The argument of the functions passed to `map` is not recognized as structurally smaller than the given rose tree. Using size annotations we can fix this problem.

```
map-rose : {A B : Set} {i : Size} → (A → B) → (Rose A i → Rose B i)
map-rose f (rose x xs) = rose (f x) (map (map-rose f) xs)
```

By pattern matching on the argument of type `Rose A` of size  $↑ i$  we obtain a `List` of trees of size  $i$ . The recursive calls via `map` therefore occur on smaller trees. Therefore the functions has to terminates.

In this case inlining the call of `map` would also solve the termination problem. When generalizing the definition of the tree from `List` to an arbitrary functor this wouldn't be possible. In many cases inlining all helper functions is either not feasible or would lead to large and unreadable programs.

### 2.1.6 Strict Positivity

In a type system with arbitrary recursive types, it is possible to to implement a fixpoint combinator and therefore non terminating functions without explicit recursion. As explained in section 2.1.5 this entails logical inconsistency. Agda allows only strictly positive data types. A data type  $D$  is strictly positive if all constructors are of the form

$$A_1 \rightarrow A_2 \rightarrow \dots \rightarrow A_n \rightarrow D$$

where  $A_i$  is either not inductive (does not mention  $D$ ) or are of the form

$$A_1 \rightarrow B_2 \rightarrow \dots \rightarrow B_n \rightarrow D$$

where  $B_j$  is not inductive. By restricting recursive occurrences of a data type in its definition to strict positive positions strong normalization is preserved.

#### Container

Because of the strict positivity requirement it is not allowed to apply generic type constructors to inductive occurrences of a data type in its definition. The reason for this restriction is that

a type constructor is not required to use its argument only in strictly positive positions. To still work generically with type constructors or more precise functors we need a more restrictive representation, which only uses its argument in a strictly positive position. One representation of such functors are containers.

Containers are a generic representation of data type, which store values of an arbitrary type. They were introduced by Abbott, Altenkirch and Ghani [AAG03]. A container is defined by a type of shapes  $S$  and a type of positions for each of its shapes  $P : S \rightarrow \mathcal{U}$ . Usually containers are denoted  $S \triangleright P$ . A common example are lists. The shape of a list is defined by its length, therefore the shape type is  $\mathbb{N}$ . A list of length  $n$  has exactly  $n$  places or positions containing data. Therefore, the type of positions is  $\prod_{n:\mathbb{N}} \text{Fin } n$  where  $\text{Fin } n$  is the type of natural numbers smaller than  $n$ . The extension of a container is a functor  $\llbracket S \triangleright P \rrbracket$ , whose lifting of types is given by

$$\llbracket S \triangleright P \rrbracket X = \sum_{s:S} P s \rightarrow X.$$

A lifted type corresponds to the container storing elements of the given type e.g.  $\llbracket \mathbb{N} \triangleright \text{Fin} \rrbracket A \cong \text{List } A$ . The second element of the dependent pair sometimes called position function. It assigns each position a stored value. The functors action on functions is given by

$$\llbracket S \triangleright P \rrbracket f \langle s, pf \rangle = \langle s, f \circ pf \rangle.$$

We can translate these definition directly to Agda. Instead of a `data` declaration we can use `record` declarations. Similar to other languages `records` are pure product types. A `record` in Agda is an  $n$ -ary dependent product type i.e. the type of each field can contain all previous values.

```
record Container : Set1 where
  constructor _▷_
  field
    Shape : Set
    Pos : Shape → Set
  open Container public
```

As expected, a container consists of a type of shapes and a dependent type of positions. Notice that `Container` is an element of `Set1`, because it contains a type from `Set` and therefore has to be larger. Next we define the lifting of types i.e. the container extension, as a function between universes.

```
open import Data.Product using (Σ-syntax; _,_) -- TODO: define and explain earlier
open import Function using (_∘_)
[ ] : Container → Set → Set
[ S ▷ P ] A = Σ[ s ∈ S ] (P s → A)
```

Using this definition we can define `fmap` for containers.

```
fmap : ∀ {A B C} → (A → B) → ([ C ] A → [ C ] B)
fmap f (s , pf) = (s , f ∘ pf)
```

## 2.2 Curry

Curry [HKM95] is a functional logic programming language. It combines paradigms from functional programming languages like Haskell with those logical languages Prolog. Curry is based on Haskell i.e. its syntax and semantics not involving nondeterminism closely resemble Haskell. Curry integrates logical features, such as nondeterminism and free variables with a few additional concepts.

When defining a function with overlapping patterns on the left-hand side of equations all matching right-hand sides are executed. This introduces non determinism. Nondeterminism is integrated as an ambient effect i.e. the effect is not represented at type level. The simplest example of a nondeterministic function is the choice operator `?`.

```

(?) :: A -> A -> A
x ? _ = x
_ ? y = y

```

Both equations always match, therefore both arguments are returned i.e. `?` introduces a nondeterministic choice between its two arguments. Using choice we can define a simple nondeterministic program.

```

coin :: Int
coin = 0 ? 1

twoCoins :: Int
twoCoins = coin + coin

```

`coin` chooses non-deterministically between 0 and 1. Executing `coin` therefore yields these two results. When executing `twoCoins` the two calls of `coin` are independent. Both choose between 0 and 1, therefore `twoCoins` yields the results 0, 1, 1 and 2.

### 2.2.1 Call-Time-Choice

Next we will take a look at the interactions between nondeterminism and function calls.

```

double :: Int -> Int
double x = x + x

doubleCoin :: Int
doubleCoin = double coin

```

When calling `double` with a nondeterministic value two behaviors are conceivable. The first possibility is that the choice is moved into the function i.e. both `x` chose independent of each other yielding the results 0, 1, 1 and 2. The second possibility is choosing a value before calling the function and choosing between the results for each possible argument. In this case both `x` have the same value, therefore the possible results are 0 and 2. This option is called **Call-Time-Choice** and it is the one implemented by Curry.

Similar to Haskell, Curry programs are evaluated lazily. The evaluation of an expression is delayed until its result is needed and each expression is evaluated at most once. The later is important when expressions are named and reused via `let` bindings or lambda abstraction. The named expression is evaluated the first time it is needed. If the result is needed again the old value is reused. This behavior is called **sharing**. Usually function application is defined using the `let` primitive. Applying a non variable expression to a function introduces a new intermediate result, which bound using `let`.

$$(\lambda x.\sigma)\tau = \text{let } y = \tau \text{ in } \sigma[x \mapsto y]$$

We therefore expect a variable bound by a `let` to behave similar to one bound by a function. This naturally extends **Call-Time-Choice** to `let`-bindings in lazily evaluated languages.

```

sumCoin :: Int
sumCoin = let x = coin in x + x

```

As expected this function yields the results 0 and 2.

### 2.2.2 Permutation Sort

Introduce Free Variables + Explain for Later Example

## 2.3 Algebraic Computational Effects

Giving a concrete definition for computational effects is hard. Examples include I/O, exceptions, nondeterminism, state and delimited continuations [Bau18]. Algebraic effects are computational

effects, which can be described using an algebraic theory. They were first presented by Plotkin and Power [PP02].

Handlers for algebraic effects were first presented by Plotkin and Pretnar as a generalization of exception handlers [PP09]. Handlers can be used to describe non-algebraic operations, which include operations with scopes such as `catch` and `once`.

Wu et al. describe a problem with this approach when multiple handlers interact. The ordering of handlers induces a semantic for the program, but simultaneously the handlers also delimit scopes. The correct ordering for scoping and semantics maybe not coincide. Wu et al. fix this problem by introducing new syntactic constructs to delimit scopes, removing the responsibility from the handler [WSH14; Pir+18].

### 2.3.1 Algebraic Theories

The following definition is similar to the one given by Bauer [Bau18].

An algebraic theory consists of a signature describing the syntax of the operations together with a set of equations. A signature is a set of operation symbols together with an arity set and an additional parameter. Operations of this form are usually denoted with a colon and  $\rightsquigarrow$  between the three sets, suggesting that they describe special functions.

$$\Sigma = \{\text{op}_i : P_i \rightsquigarrow A_i\}_{i \in \mathbf{N}}$$

Given a signature  $\Sigma$  we can build terms over a set of variables  $\mathbb{X}$ .

$$x \in \text{Term}_\Sigma(\mathbb{X}) \quad \text{for } x \in \mathbb{X} \quad \text{op}_i(p, \kappa) \in \text{Term}_\Sigma(\mathbb{X}) \quad \text{for } p \in P_i, \kappa : A_i \rightarrow \text{Term}_\Sigma(\mathbb{X})$$

Terms can be used to form equations of the form  $x \mid l = r$ . Each equation consists of two terms  $l$  and  $r$  over a set of variables  $x$ . A signature  $\Sigma_T$  together with a set of equations  $\mathcal{E}_T$  forms an algebraic theory  $T$ .

$$T = (\Sigma_T, \mathcal{E}_T)$$

An interpretation  $I$  of a signature is given by a carrier set  $|I|$  and an interpretation for each operation  $\llbracket \cdot \rrbracket_I$ . An interpretation of an operation  $\text{op}_i$  is given by a functions to the carrier set  $|I|$ , that takes an additional parameter from  $P_i$  and  $|A_i|$  parameters as a function from the arity set to the carrier set  $|I|$ .

$$\llbracket \text{op}_i \rrbracket_I : P_i \times |I|^{A_i} \rightarrow |I|$$

Given a function  $\iota : \mathbb{X} \rightarrow |I|$ , assigning each variable a value, we can give an interpretation for terms  $\llbracket \cdot \rrbracket_{(I, \iota)}$ .

$$\llbracket x \rrbracket_{(I, \iota)} = \iota(x)$$

$$\llbracket \text{op}_i(p, \kappa) \rrbracket_{(I, \iota)} = \llbracket \text{op}_i \rrbracket_I(p, \lambda p. \llbracket \kappa(p) \rrbracket_{(I, \iota)})$$

An interpretation for  $T$  is called  $T$ -model if it validates all equations in  $\mathcal{E}_T$ .

#### Free Model

For each algebraic theory  $T$  we can generate a so called free model  $\text{Free}_T(\mathbb{X})$ . The free model is the optimal model for the theory i.e. it validates just equations from  $\mathcal{E}_T$  and the ones directly following from them and no more.

The set  $\text{Tree}_T(\mathbb{X})$  contains term trees, built from the variables in  $\mathbb{X}$  and the operations of the signature  $\Sigma_T$ .

$$\text{pure } x \in \text{Tree}_T(\mathbb{X}) \quad \text{op}_i(p, \kappa) \in \text{Tree}_T(\mathbb{X}) \quad \text{for } p \in P_i \quad \kappa : A_i \rightarrow \text{Tree}_T(\mathbb{X})$$

The free model for  $T$  is given by

$$\text{Free}_T(\mathbb{X}) = \text{Tree}_T(\mathbb{X}) / \sim_T$$

where  $\sim_T$  is the least equivalence relation, such that for all equations  $x \mid l = r \in \mathcal{E}_T$ ,  $l \sim_T r$ . Furthermore  $\sim_T$  is required to be a congruence relation for the operations of the signature i.e.

$$\forall i \in \{1, \dots, n\}. x_i \sim_T y_i \Rightarrow \text{op}(x_1, \dots, x_i) \sim_T \text{op}(y_1, \dots, y_i)$$

In section 2.3.3 we will see that the free model forms the basis for implementing algebraic effects.

### 2.3.2 Effect Handler

### 2.3.3 Free Monad

The syntax of an algebraic effect is described using the free monad. The usual definition of the free monad in Haskell is the following.

```
data Free f a = Pure a | Impure (f (Free f a))

instance (Functor f) => Monad (Free f) where
  return = Pure

Pure x    >>= k = k x
Impure fa >>= k = Impure (fmap (>>= k) fa)
```

The free monad corresponds to the free model for an algebraic theory  $T$  without equations i.e. the equivalence relation  $\sim_T$  is just the identity relation on  $\text{Tree}_T(\mathbb{X})$ . As a result some trees which should be equal aren't. When the syntax is interpreted by a correct handler these trees should be equal again and the equations should hold.

When defining the free monad in Agda we cannot use an arbitrary functor as in Haskell, because it would violate the strict positivity requirement. Instead we will represent the functor as the extension of a container as described in section 2.1.6.

```
data Free (C : Container) (A : Set) : Set where
  pure   : A → Free C A
  impure : [ C ] (Free C A) → Free C A
```

The free monad represents an arbitrary branching tree with values of type  $A$  in its leafs. The **pure** constructor builds leafs containing just a value of type  $A$ . The **impure** constructor takes a value of the **Free** monad lifted by the container functor of  $C$ . Based on the choice of container the actual value could contain an arbitrary number of values i.e. **Free** monads or subtrees. Furthermore for each shape from the **Shape** type the number of subtrees can differ or contain additional arbitrary values. The container has no access to the type parameter of the free monad.

**Containers** correspond to operations. The constructors for **Shape** correspond to the operations  $\text{op}_i$  and simultaneously store the parameter  $P_i$ . A constructor without extra arguments corresponds to the operation with parameter set  $\mathbb{1}$ . The type of positions corresponds to the arity set  $A_i$ . The **Pos** type depends on a value of type **Shape** i.e. it assigns an arity to each shape/operation. In the free model the parameters/child trees are given by a function mapping from the arity to the carrier set. This function corresponds to the position function in the **Container** extension, which maps from the type of positions to the held type, in this case the free monad i.e. the carrier type.

The  $\gg$  operator for free monads traverses the trees and applies the continuation to the values stored in the leafs, replacing them.  $\gg$  therefore substitutes leafs with new subtrees generated from the values stored in each leaf. It corresponds to variable substitution. Algebraic operations are those which commute with  $\gg$  i.e. for an  $n$ -ary algebraic operations the following holds.

$$\text{op}(x_1, \dots, x_n) \gg \kappa = \text{op}(x_1 \gg \kappa, \dots, x_n \gg \kappa)$$

For common scoping operations like **once**, **catch** or **fork** this does obviously not hold. They are not algebraic but can be represented as an effect handler. Representing these operations as a handler moves the syntactic problem of scoping to the level of the handler i.e. to a semantics level. Decoupling the two leads to the idea of scoped effects.

### 2.3.4 Scoped Effects

# Chapter 3

## First Order

The following sections describe the implementation of unscoped and scoped effects in the first order setting. They focus on implementation details specific to Agda like termination checks. The scoped effects are implemented using explicit scope delimiters as described by Wu et al. [WSH14].

### 3.1 Functors à la carte

When modelling effects each functor represents the syntax i.e. the operations of an effect. For containers each shape constructor corresponds to an operation symbol and the type of position for a shape corresponds to the arity set for the operation. The additional parameter of an operation is embedded in the shape. The free monad over a container describes a program using the effects syntax i.e. its the free model for the algebra without the equations. To combine the syntax of multiple effects we can combine the underlying functors, because the free monad preserves coproducts.

The approach described by Wu et al. is based on “Data types à la carte”[Swi08]. The functor coproduct is modelled as the data type `data (f :+: g) a = Inl (f a) | Inr (g a)`, which is again a **Functor** in **a**. In Agda functors are represented as containers, a concrete data type not a type class. We could use a similar data type to combine the extensions of two containers, but we would loose the advantages of containers i.e. a container extension is a strictly positive functor. Therefore, we will combine containers directly. Containers are closed under multiple operations, coproducts being one of them [AAG03]. The coproduct of two containers  $F$  and  $G$  is the container whose **shape** is the disjoint union of  $F$ s and  $G$ s shapes and whose position function **pos** is the coproduct mediator of  $F$ s and  $G$ s position functions<sup>1</sup>.

$$\begin{aligned} \_ \oplus \_ &: \text{Container} \rightarrow \text{Container} \rightarrow \text{Container} \\ (\text{Shape}_1 \triangleright \text{Pos}_1) \oplus (\text{Shape}_2 \triangleright \text{Pos}_2) &= (\text{Shape}_1 \uplus \text{Shape}_2) \triangleright [\text{Pos}_1, \text{Pos}_2] \end{aligned}$$

The functor represented by the coproduct of two containers is isomorphic to the functor coproduct of their representations. The container without shapes is neutral element for the coproduct of containers. This allows us to define  $n$ -ary coproducts for containers.

$$\begin{aligned} \text{sum} &: \text{List Container} \rightarrow \text{Container} \\ \text{sum} &= \text{foldr } (\_ \oplus \_) (\bot \triangleright \lambda()) \end{aligned}$$

To generically work with arbitrary coproducts of functors we will define two utility functions. Given a value  $x : A$  we want to be able to inject it into any coproduct mentioning  $A$ . Given any coproduct mentioning  $A$  we want to be able to project a value of type  $A$  from the coproduct, if  $A$  is the currently held alternative.

In the “Data types à la carte”[Swi08] approach the type class `:<:` is introduced. `:<:` relates a functor to a coproduct of functors, marking it as an option in the coproduct. `:<:`s functions can be used to inject values into or maybe extract values from a coproduct. The two instances for `:<:` mark  $F$  as an element of the coproduct if it’s an on the left-hand side of the coproduct (in the head) or if it’s already in the right-hand side (in the tail).

<sup>1</sup>The function `[_]` corresponds to the Haskell function `either :: (a -> c) -> (b -> c) -> Either a b -> c`.



```

class (Syntax sub, Syntax sup) => sub <: sup where
  inj :: sub m a -> sup m a
  prj :: sup m a -> Maybe (sub m a)

instance {-# OVERLAPPABLE #-} (Syntax f, Syntax g) => f <: (f :+: g) where
  inj = Inl
  prj (Inl a) = Just a
  prj _ = Nothing

instance {-# OVERLAPPABLE #-} (Syntax h, f <: g) => f <: (h :+: g) where
  inj = Inr . inj
  prj (Inr ga) = prj ga
  prj _ = Nothing

```

The two instances overlap resulting in possible slower instance resolution. Furthermore, `:+:` is assumed to be right associative and only to be used in a right associative way to avoid backtracking. Because in Agda the result of `_⊕_` is another container, not just a value of a simple data type, instance resolution using `_⊕_` is not as straight forward as in Haskell and in some cases extremely slow<sup>2</sup>.

This implementation of the free monad uses an approach similar to the Idris effect library [Bra13]. The free monad is not parameterised over a single container, but a list *ops* of containers. This has the benefit that we cannot associate coproducts to the left by accident. The elements of the list are combined later using `sum`. To track which functors are part of the coproduct we introduce the new type `_∈_`.

```

data _∈_ {ℓ : Level} {A : Set ℓ} (x : A) : List A → Set ℓ where
instance
  here : ∀ {xs} → x ∈ x :: xs
  there : ∀ {y xs} → [ x ∈ xs ] → x ∈ y :: xs

```

The type `x ∈ xs` represents the proposition that `x` is an element of `xs`. The two constructors can be read as rules of inference. One can always construct a proof that `x` is in a list with `x` in its head and given a proof that `x ∈ xs` one can construct a proof that `x` is also in the extended list `y :: xs`.

The two instances still overlap resulting in  $\mathcal{O}(c^n)$  instance resolution. Using Agdas internal instance resolution can be avoided by using a tactic to infer `_∈_` arguments. For simplicity the following code will still use instance arguments. This version can easily be adapted to one using macros, by replacing the instance arguments with hidden ones with `tactic` annotations.

Using this proposition we can define functions for injection into and maybe projection out of coproducts.

```

inject : ∀ {C ops ℓ} {A : Set ℓ} → C ∈ ops → [ C ] A → [ sum ops ] A
inject here (s, pf) = (inj1 s), pf
inject (there [ p ]) prog with inject p prog
... | s, pf = (inj2 s), pf

project : ∀ {C ops ℓ} {A : Set ℓ} → C ∈ ops → [ sum ops ] A → Maybe ([ C ] A)
project here (inj1 s, pf) = just (s, pf)
project here (inj2 _, _) = nothing
project there (inj1 _, _) = nothing
project (there [ p ]) (inj2 s, pf) = project p (s, pf)

```

Both `inject` and `project` require a proof/evidence that specific container is an element of the list used to construct the coproduct.

Let us consider `inject` first. By pattern matching on the evidence we acquire more information about type `sum ops`. In case of `here` we know that `op` is in the head of the list i.e. that the given value `C` is the same as the one in the head of the list. Therefore the `Shape` types are the same and we can use our given `s` and `pf` to construct the coproduct. In case of `there` we obtain a proof that the container is in the tail of the list, which we can use to make a recursive call. By pattern matching on and repackaging the result we obtain a value of the right type.

<sup>2</sup>I encountered cases where type checking of overlapping instances involving `_⊕_` did not seem to terminate.

**project** functions similarly. By pattern matching on the proof we either know that the value we found has the correct type or we obtain a proof for the tail of the list allowing us to either make a recursive call or stop the search.

### 3.1.1 The Free Monad for Effect Handling

Using the coproduct machinery we can now define a version of the free monad, suitable for working with effects. In contrast to the first definition, this free monad is parameterized over a list of containers. In the **impure** constructor the containers are combined using **sum**. The parameterization over a list ensures that the containers are not combined prematurely.

```
data Free (ops : List Container) (A : Set) : {Size} → Set where
  pure  : ∀ {i} → A → Free ops A {i}
  impure : ∀ {i} → [ sum ops ] (Free ops A {i}) → Free ops A {↑ i}
```

Next we define utility functions for working with the free monad. **inj** and **prj** provide the same functionality as the ones used by Wu et al. **inj** allows to inject syntax into a program whose signature allows the operation. **prj** allows to inspect the next operation of a program, restricted to a specific signature. Furthermore we add the functions **op** and **upcast**. **op** generates the generic operation for any operation symbol. **upcast** transforms a program using any signature to one using a larger signature. Notice that upcast preserves the size of its input, because it just traverses the tree and repackages the contents.

```
inj : ∀ {C ops A} → [ C ∈ ops ] → [ C ] (Free ops A) → Free ops A
inj [ p ] = impure ∘ inject p

prj : ∀ {C ops A i} → [ C ∈ ops ] → Free ops A {↑ i} → Maybe ([ C ] (Free ops A {i}))
prj [ p ] (pure x) = nothing
prj [ p ] (impure x) = project p x

op : ∀ {C ops} → [ C ∈ ops ] → (s : Shape C) → Free ops (Pos C s)
op s = inj (s , pure)

upcast : ∀ {C ops A i} → Free ops A {i} → Free (C :: ops) A {i}
upcast (pure x) = pure x
upcast (impure (s , κ)) = impure (inj2 s , upcast ∘ κ)
```

The free monad is indexed over an argument of Type **Size**. **pure** values have an arbitrary size. When constructing an **impure** value the new value is strictly larger than the ones produced by the containers position function. The size annotation therefore corresponds to the height of the tree described by the free monad. Using the annotation it's possible to prove that functions preserve the size of a value or that complex recursive functions terminate.

Consider the following definition of **fmap** for the free monad<sup>3</sup>.

```
fmap _<$>_ : {F : List Container} {i : Size} → (A → B) → Free F A {i} → Free F B {i}
f <$> pure x = pure (f x)
f <$> impure (s , pf) = impure (s , (f <$>_) ∘ pf)

fmap = _<$>_
```

**fmap** applies the given function *f* to the values stored in the **pure** leaves. The height of the tree is left unchanged. This fact is witnessed by the same index *i* on the argument and return type.

In contrast to **fmap**, **bind** does not preserve the size. **bind** replaces every **pure** leaf with a subtree, which is generated from the stored value. The resulting tree is therefore at least as high as the given one. Because there is no  $+$  for sized types the only correct size estimate for the returned value is “unbounded”. The return type is not explicitly indexed, because the compiler correctly infers  $\infty$ .

```
_>=>_ : ∀ {ops} → Free ops A → (A → Free ops B) → Free ops B
pure x >=> k = k x
```

<sup>3</sup>in the following code *A*, *B* and *C* are arbitrary types

$$\begin{aligned}
&\text{impure } (s, pf) \gg k = \text{impure } (s, (\_ \gg k) \circ pf) \\
&\_ \gg \_ : \forall \{ops\} \rightarrow \text{Free } ops A \rightarrow \text{Free } ops B \rightarrow \text{Free } ops B \\
&ma \gg mb = ma \gg \lambda \_ \rightarrow mb
\end{aligned}$$

To complete our basic set of monadic functions we also define `ap`.

$$\begin{aligned}
&\_ \langle * \rangle \_ : \forall \{ops\} \rightarrow \text{Free } ops (A \rightarrow B) \rightarrow \text{Free } ops A \rightarrow \text{Free } ops B \\
&\text{pure } f \quad \langle * \rangle ma = f \langle \$ \rangle ma \\
&\text{impure } (s, pf) \langle * \rangle ma = \text{impure } (s, (\_ \langle * \rangle ma) \circ pf)
\end{aligned}$$

### 3.1.2 Properties

This definition of the free monad is a functor because it satisfies the two functor laws. Both properties are proven by structural induction over the free monad. Notice that to proof the equality of the position functions, in the induction step, the axiom of extensionality is invoked.

$$\begin{aligned}
&\text{fmap-id} : \forall \{ops\} \rightarrow (p : \text{Free } ops A) \rightarrow \text{fmap id } p \equiv p \\
&\text{fmap-id } (\text{pure } x) = \text{refl} \\
&\text{fmap-id } (\text{impure } (s, pf)) = \text{cong } (\text{impure } \circ (s, \_)) (\text{extensionality } (\text{fmap-id } \circ pf))
\end{aligned} \tag{1}$$

$$\begin{aligned}
&\text{fmap-}\circ : \forall \{ops\} (f : B \rightarrow C) (g : A \rightarrow B) (p : \text{Free } ops A) \rightarrow \\
&\quad \text{fmap } (f \circ g) p \equiv (\text{fmap } f \circ \text{fmap } g) p \\
&\text{fmap-}\circ f g (\text{pure } x) = \text{refl} \\
&\text{fmap-}\circ f g (\text{impure } (s, pf)) = \text{cong } (\text{impure } \circ (s, \_)) (\text{extensionality } (\text{fmap-}\circ f g \circ pf))
\end{aligned} \tag{2}$$

Later we will need the interchange law for applicative functors.

$$\begin{aligned}
&\text{interchange} : \forall a (f : \text{Free } ops (A \rightarrow B)) \rightarrow \\
&\quad (f \langle * \rangle \text{pure } a) \equiv (\text{pure } (\_ \$ a) \langle * \rangle f) \\
&\text{interchange } a (\text{pure } f) = \text{refl} \\
&\text{interchange } a (\text{impure } (s, \kappa)) = \text{cong } (\text{impure } \circ (s, \_)) (\text{extensionality } (\text{interchange } a \circ \kappa))
\end{aligned}$$

This definition of the free monad also satisfies the three monad laws.

$$\begin{aligned}
&\text{bind-ident}^l : \forall \{ops\} (f : A \rightarrow \text{Free } ops B) (x : A) \rightarrow (\text{pure } x \gg f) \equiv f x \\
&\text{bind-ident}^l f x = \text{refl}
\end{aligned} \tag{3}$$

$$\begin{aligned}
&\text{bind-ident}^r : \forall \{ops\} (x : \text{Free } ops A) \rightarrow (x \gg \text{pure}) \equiv x \\
&\text{bind-ident}^r (\text{pure } x) = \text{refl} \\
&\text{bind-ident}^r (\text{impure } (s, pf)) = \text{cong } (\text{impure } \circ (s, \_)) (\text{extensionality } (\text{bind-ident}^r \circ pf))
\end{aligned} \tag{4}$$

$$\begin{aligned}
&\text{bind-assoc} : \forall \{ops\} (f : A \rightarrow \text{Free } ops B) (g : B \rightarrow \text{Free } ops C) (p : \text{Free } ops A) \rightarrow \\
&\quad ((p \gg f) \gg g) \equiv (p \gg (\lambda x \rightarrow f x \gg g)) \\
&\text{bind-assoc } f g (\text{pure } x) = \text{refl} \\
&\text{bind-assoc } f g (\text{impure } (s, pf)) = \text{cong } (\text{impure } \circ (s, \_)) (\text{extensionality } (\text{bind-assoc } f g \circ pf))
\end{aligned} \tag{5}$$

## 3.2 Handler

Usually, an effect handler interprets and removes the syntax of an effect and injects corresponding code into the program. Some handlers manipulate syntax of other effects or the structure of the program itself. The handler for an algebraic effect defines its semantics.

All handlers will have the same basic structure. They will take a program i.e. a variable of type `Free C A`, where the head of `C` is the effect interpreted by the handler. Each handler produces a program without the interpreted syntax i.e. just the tail of `C` in it's effect stack and potentially modify the type `A` to one modelling the result of the effect. For example a handler for

exceptions would remove exception syntax and transform a program producing a value of type  $A$  to one producing a value of type  $E \uplus A$ , either an exception or a result.

A simple but important handler is the one handling the empty effect stack and therefore the **Void** effect. A program containing just **Void** syntax contains no impure constructors, because **Void** has no operations i.e. its **Shape** type has no constructors. Pattern matching on the impure constructor therefore yields  $()$ .

Therefore, we can always produce a value of type  $A$ . This handler is important, because it can be used to escape the **Free** context after all other effects have been handled.

```
run : Free [] A → A
run (pure x) = x
```

The following two sections will describe the implementation of handlers for **State** and **Nondeterminism**. They will exemplarily describe the construction of a handler as well as lay ground work for more complex handlers.

### 3.2.1 Nondeterministic Choice

The nondeterminism effect has two operations **??** and **fail**. **??** introduces a nondeterministic choice between two execution paths and **fail** discards the current path. We therefore have a nullary and a binary operation, both without additional parameters.

$$\Sigma_{\text{Nondet}} = \{?? : \mathbf{1} \leadsto \mathbf{2}, \text{fail} : \mathbf{1} \leadsto \mathbf{0}\}$$

Expressed as a container we have a shape with two constructors, one for each operation and both without parameters.

```
data Nondets : Set where ??s fails : Nondets
```

When constructing the container we assign the correct arities to each shape.

```
Nondet : Container
Nondet = Nondets ▷ λ where
  ??s → Bool
  fails → ⊥
```

We can now define smart constructors for each operation. These are not the generic operations, but helper functions based on them. The generic operations take no parameters and always use **pure** as continuation. These versions of the operations already process the continuations parameter.

```
__??__ : ∀ {ops} → [ Nondet ∈ ops ] → Free ops A → Free ops A → Free ops A
p ?? q = inj (??s , (if_then p else q))

fail : ∀ {ops} → [ Nondet ∈ ops ] → Free ops A
fail = inj (fails , λ())
```

With the syntax in place we can now move on to semantics and define a handler for the effect. By introducing **pattern** declarations for each operations the handler can be simplified. Furthermore we introduce a **pattern** for other operations, i.e. those who are not part of the currently handled signature.

```
pattern Other s κ = impure (inj2 s , κ)
pattern Fail κ    = impure (inj1 fails , κ)
pattern Choice κ  = impure (inj1 ??s , κ)
```

The handler interprets **Nondet** syntax and removes it from the program. Therefore **Nondet** is removed from the front of the effect stack and the result is wrapped in a **List**. The **List** contains the results of all successful execution paths.

```
solutions : ∀ {ops} → Free (Nondet :: ops) A → Free ops (List A)
```

The **pure** constructor represents a program without effects. The singleton list is returned, because no nondeterminism is used in a **pure** calculation.

`solutions (pure x) = pure (x :: [])`

The `fail` constructor represents an unsuccessful calculation. No result is returned.

`solutions (Fail κ) = pure []`

In case of a `Choice` both paths can produce an arbitrary number of results. We execute both programs recursively using `solutions` and collect the results in a single `List`.

`⟦` and `⟩` are *idiom brackets* and denote applicative functor style function application i.e. `pure f <*> ... <*> ... <*> ...`. In this case the function `f` is the mixfix operator `_++_` which can still be written in infix notation.

`solutions (Choice κ) = ⟦ solutions (κ true) ++ solutions (κ false) ⟧`

In case of syntax from another effect we just execute `solutions` on every subtree by mapping the function over the container. Note that the newly constructed value has a different type. Since `Nondet` syntax was removed from the tree the proof for `_∈_`, which is passed to `impure` changes.

`solutions (Other s κ) = impure (s, solutions ∘ κ)`

## Properties

As explained in section 2.3.3, the free monad represents the free model for the theory without equations i.e. some terms should be equal but aren't. The handler for an algebraic effect defines its semantics by removing and interpreting its syntax. The result of a handler should again be a model for the effect i.e. the equations characterizing the effect should hold. We can proof that our handler produces a valid (but not necessarily free) model for our equations by verifying that the laws holds after interpreting the terms. The ability to rigorously proof these laws about the program is one of the main advantages of Agda.

We have four laws governing our `Nondet` effect. The first law states that `const fail` should be an absorbing element for the Kleisli composition.

$$\begin{aligned} \text{bind-fail} : \{k : A \rightarrow \text{Free (Nondet :: ops) } B\} \rightarrow \\ \text{solutions (fail } \gg k) &\equiv \text{solutions fail} \\ \text{bind-fail} &= \text{refl} \end{aligned} \tag{6}$$

The proof is trivial. Simplifying both sides yields `fail`.

The other three laws state that `??` and `fail` form a monoid. The proofs for all three are similar. By using monad functor, applicative and monad laws one can reduce the proof to one for pure lists and simply use the corresponding equality from the standard library.

```

??-identl : (q : Free (Nondet :: ops) A) → solutions (fail ?? q) ≡ solutions q
??-identl q = begin
  solutions (fail ?? q)                ≡⟨ ⟩ -- definition of handler for ??
  _++_ <$> solutions fail <*> solutions q ≡⟨ ⟩ -- definition of handler for fail
  _++_ <$> pure [] <*> solutions q      ≡⟨ ⟩ -- definition of <$>
  pure ([ ++_]) <*> solutions q        ≡⟨ ⟩ -- definition of <*> / ap-ident-left
  [] ++_ <$> solutions q                ≡⟨ ⟩ -- definition of ++ / +-ident-left
  id <$> solutions q                    ≡⟨ ⟩ fmap-id (solutions q)
  solutions q                          ■

```

The proof for the left identity is straight forward. No standard library equality is needed, because `++` is recursive in it's first argument. to eliminate the `<$>` a functor law is needed.

```

??-identr : (p : Free (Nondet :: ops) A) → solutions (p ?? fail) ≡ solutions p
??-identr p = begin
  solutions (p ?? fail)                ≡⟨ ⟩ -- definition of handler
  _++_ <$> solutions p <*> pure []      ≡⟨ ⟩ interchange [] (_++_ <$> solutions p)
  pure (_$ []) <*> (_++_ <$> solutions p) ≡⟨ ⟩ -- definition of <*> / ap-ident-left
  (_$ []) <$> (_++_ <$> solutions p) ≡⟨ ⟩ sym (fmap-∘ (_$ []) _++_ (solutions p))

```

```

(⟦_ $ []⟧)      ◦  _++_  ⇔ solutions p ≡ ⟨ -- definition of ◦ and $
(⟦_ ++ []⟧)     ⇔ solutions p ≡ ⟨ cong (⟦_ $⟧ solutions p)
                                   (extensionality ++-identityr) ⟩

id              ⇔ solutions p ≡ ⟨ fmap-id (solutions p) ⟩
solutions p    ■

```

Proofing the right identity is more complicated, because `fail` is on the right-hand side of `??`. All monad functions from section 3.1.1 are recursive in their left argument, therefore most propositions involving right argument don't follow trivially from the definition and need own proofs.

This is a common pattern. Because `++` is recursive in its first argument, the left identity is given by definitional equality, while the right one is not, but follows from the definition. Notice that partially applying `++` with `[]` is only equal to `id` on the left without invoking `extensionality`.

Using the proofs from section 3.1.2 we can simplify the equations and reduce them to a problem for normal `List`. The proof for associativity is longer, but follows the same patterns.

### 3.2.2 State

The state effect has two operations `get` and `put`. The whole effect is parameterized over the state type `s`.

`get` simply returns the current state. The operation takes no additional parameters and has `s` positions. This can either be interpreted as `get` being an `s`-ary operation (one child for each possible state) or simply the parameter of the continuation being a value of type `s`.

`put` updates the current state. The operation takes an additional parameter, the new state. The operation itself is unary i.e. the continuation is called with `tt` to start the rest of the program.

$$\Sigma_{State} = \{\text{get} : \mathbf{1} \rightsquigarrow s, \text{put} : s \rightsquigarrow \mathbf{1}\}$$

As before we will translate this definition in a corresponding container and define `patterns` to simplify the handler.

```

data States (S : Set) : Set where
  gets : States S
  puts : S → States S

State : Set → Container
State S = States S ▷ λ where
  gets      → S
  (puts _) → ⊤

pattern Get κ = impure (inj1 gets, κ)
pattern Put s κ = impure (inj1 (puts s), κ)

```

To simplify working with the `State` effect we add smart constructors. These correspond to the generic operations, which we can implement using `op`.

```

get : ∀ {ops S} → [ State S ∈ ops ] → Free ops S
get = op gets

put : ∀ {ops S} → [ State S ∈ ops ] → S → Free ops ⊤
put s = op (puts s)

```

Using these definitions for the syntax we can define the handler for `State`.

The effect handler for `State` takes an initial state together with a program containing the effect syntax. The final state is returned in addition to the result.

$$\text{runState} : \forall \{ops S\} \rightarrow S \rightarrow \text{Free} (\text{State } S :: ops) A \rightarrow \text{Free } ops (S \times A)$$

A `pure` calculation doesn't change the current state. Therefore, the initial is also the final state and returned in addition to the result of the calculation.

$$\text{runState } s_0 (\text{pure } x) = \text{pure } (s_0, x)$$

The continuation/position function for `get` takes the current state to the rest of the calculation. By applying  $s_0$  to  $\kappa$  we obtain the rest of the computation, which we can evaluate recursively.

$$\text{runState } s_0 (\text{Get } \kappa) = \text{runState } s_0 (\kappa s_0)$$

`put` updates the current state, therefore we pass the new state  $s_1$  to the recursive call of `runState`.

$$\text{runState } \_ (\text{Put } s_1 \kappa) = \text{runState } s_1 (\kappa \text{tt})$$

Similar to the handler for `Nondet` we apply the handler to every subterm of non `State` operations.

$$\text{runState } s_0 (\text{Other } s \kappa) = \text{impure } (s, \text{runState } s_0 \circ \kappa)$$

### Example

Here is a simple example for a function using the `State` effect. The function `tick` returns `tt` and as side effect increases the state.

$$\begin{aligned} \text{tick} &: \forall \{ops\} \rightarrow \llbracket \text{State } \mathbb{N} \in ops \rrbracket \rightarrow \text{Free } ops \top \\ \text{tick} &= \text{do } i \leftarrow \text{get} ; \text{put } (1 + i) \end{aligned}$$

Using the `runState` handler we can evaluate programs, which use the `State` effect.

$$(\text{run } \$ \text{runState } 0 \$ \text{tick} \gg \text{tick}) \equiv (2, \text{tt})$$

### Properties

$$\begin{aligned} &\text{module StateLaws } (S : \text{Set}) (ops : \text{List Container}) (s_0 : S) \text{ where} \\ &\quad \text{go} : \text{Free } (\text{State } S :: ops) A \rightarrow \text{Free } ops (S \times A) \\ &\quad \text{go} = \text{runState } \{ \_ \} \{ ops \} s_0 \\ &\quad \text{put-put} : \{s_1 s_2 : S\} \rightarrow (\text{go } \$ \text{put } s_1 \gg \text{put } s_2) \equiv (\text{go } \$ \text{put } s_2) \\ &\quad \text{put-put} = \text{refl} \\ &\quad \text{put-get} : \{s : S\} \rightarrow (\text{go } \$ \text{put } s \gg \text{get}) \equiv (\text{go } \$ \text{put } s \gg \text{pure } s) \\ &\quad \text{put-get} = \text{refl} \\ &\quad \text{get-get} : \{k : S \rightarrow S \rightarrow \text{Free } (\text{State } S :: ops) A\} \\ &\quad \quad \rightarrow (\text{go } \$ \text{get} \gg \lambda s \rightarrow \text{get} \gg k s) \equiv (\text{go } \$ \text{get} \gg \lambda s \rightarrow k s s) \\ &\quad \text{get-get} = \text{refl} \\ &\quad \text{get-put} : (\text{go } \$ \text{get} \gg \text{put}) \equiv (\text{go } \$ \text{pure } \text{tt}) \\ &\quad \text{get-put} = \text{refl} \end{aligned}$$

### 3.2.3 Handling Combined Effects

As described in section 3.1, signatures can be combined by combining the underlying functors. Handlers can be used to partially evaluate programs over a combined signature. Consider the following program using nondeterminism and state.

$$\begin{aligned} \text{chooseTick} &: \llbracket \text{Nondet} \in ops \rrbracket \rightarrow \llbracket \text{State } \mathbb{N} \in ops \rrbracket \rightarrow \text{Free } ops \mathbb{N} \\ \text{chooseTick} &= \text{tick} \gg ((\text{tick} \gg \text{get}) ?? (\text{tick} \gg \text{tick} \gg \text{get})) \end{aligned}$$

For the interaction of `State` and `Nondet` two semantics are conceivable.

**Local State** Each branch in the nondeterministic calculation has its own state. When `??` is used to choose between two results both branches continue with own states, which initially have the same value.

**Global State** All branches share a single, global state. Based on the evaluation strategy for the nondeterminism (first result/all results; depth first search/breath first search/fair search) an ordering for all operations in the tree is induced. The state operations are executed in this order and all act on the same state.

The handlers for the two effects define semantics for their operations. Operations of the other signature are just traversed. The interaction semantics are induced by the ordering of the handlers. We obtain two combined handlers, each corresponding to one of the two cases above.

```
localState : S → Free (State S :: Nondet :: []) A → List (S × A)
localState s0 = run ∘ solutions ∘ runState s0

globalState : S → Free (Nondet :: State S :: []) A → S × List A
globalState s0 = run ∘ runState s0 ∘ solutions
```

Let us consider the above example under both combined handlers with initial state 0.

**Local State** The first `tick` increases the state to 1. Both branches are executed independently with initial state 1. The first ticks once, therefore the `get` yields 2. The second ticks twice, therefore the `get` yields 3.

```
localState 0 chooseTick ≡ (2 , 2) :: (3 , 3) :: []
```

**Global State** The `nondet` handler executes the branches from left to right. The final state of one branch is the initial one for the next branch. Therefore, the second branch continues with state 2 increasing it twice.

```
globalState 0 chooseTick ≡ (4 , 2 :: 4 :: [])
```

### 3.3 Effects with Scopes using Brackets

To correctly handle operations with local scopes Wu et al. introduced scoped effects [WSH14]. They presented two solutions to explicitly declare how far an operations scopes over a program using arbitrary syntax. In the following section we will implement the scoped effect `Cut` using the first order approach in Agda. The central idea is to add new effect syntax, representing explicit scope delimiters. Whenever an opening delimiter is encountered the handler can be run again on the scoped program. Thanks to a closing delimiters the end of a scope can be found. Therefore, calling `>>=` on a scoped operation to extend the continuation isn't a problem, because the continuation can be separated in the part inside and outside the scope.

#### 3.3.1 Cut and Call

First we will define the syntax for the new effect and its delimiters.

```
data Cuts : Set where cutfails : Cuts
data Calls : Set where bcalls ecalls : Calls

pattern Cutfail = impure (inj1 cutfails , _)
pattern BCall κ = impure (inj1 bcalls , κ)
pattern ECall κ = impure (inj1 ecalls , κ)

Cut Call : Container
Cut = Cuts ▷ λ _ → ⊥
Call = Calls ▷ λ _ → ⊤
```

The `Cut` effect has just a single operation, `cutfail`. `cutfail` can only be used in a context with nondeterminism. When `cutfail` is called it will prunes all unexplored branches and calls `fail`. The Agda implementation of the handlers is identical to the one by Wu et al.

The handler itself calls the function `go`, which accumulates the unexplored alternatives in its second argument. `fail` is the neutral element for `??` and therefore the default argument. Since this



handler is not orthogonal (i.e it interacts with another effect) **Nondet** is required to be in scope, but its position is irrelevant.

To prove termination we mark the second argument with an arbitrary but fixed size  $i$ . The position functions for each case return subterms indexed with a smaller size. Recursive calls to **go** with these terms as argument therefore terminate.

```
call : [ Nondet ∈ ops ] → Free (Cut :: ops) A → Free ops A
call = go fail
where
  go : [ Nondet ∈ ops ] → Free ops A → Free (Cut :: ops) A {i} → Free ops A
```

In case of a **pure** value no **cutfail** happened. We therefore return a calculation choosing between the value and the earlier separated alternatives.

$$\text{go } q \text{ (pure } a) = (\text{pure } a) ?? q$$

In case of a **cutfail** we terminate the current computation by calling **fail** and prune the alternatives by ignoring  $q$ .

$$\text{go } \_ \text{ Cutfail} = \text{fail}$$

To interact with **Nondet** syntax we have to find it. We have a proof that the **Nondet** effect is an element of the effect list. Whenever we find syntax from another effect we can therefore try to project the **Nondet** option from the coproduct. Notice that **prj** hides the structural recursion but decreases the **Size** index. We can therefore still proof that the function terminates.

$$\text{go } q \text{ p@(\text{Other } s \kappa) \text{ with prj } \{\text{Nondet}\} p$$

The case for **??** separates the main branch from the alternative. Using **go** the **Cut** syntax is removed from both alternatives, but the results are handled asymmetrically. The left option is directly passed to the recursive call of **go**. The handled right option is the new alternative for the left one and therefore could be pruned if left contains a **cutfail** call.

$$\dots \mid \text{just } (??^s, \kappa') = \text{go } (\text{go } q \text{ (}\kappa' \text{ false)}) (\kappa' \text{ true})$$

When encountering a **fail** we continue with the accumulated alternatives.

$$\dots \mid \text{just } (\text{fail}^s, \_) = q$$

Syntax from other effects is handled as usual.

$$\dots \mid \text{nothing} = \text{impure } (s, \text{go } q \circ \kappa)$$

With the handler for **Cut** in place we can define the handler for the scope delimiters. The implementation is again similar to the one presented by Wu et al., but to proof termination we again have to add **Size** annotations to the functions.

The **bcall** and **ecall** handler remove the scope delimiter syntax from the program and run **call** (the handler for **cut**) at the beginning of each scope. Whenever a **BCall** is found the handler **ecall** is used to handle the rest of the program. **ecall** searches for the end of the scope and returns the program up to that point. The rest of the program is the result of the returned program.

A valid upper bound for the size of the rest of the program is  $i$ , the size of the program before separating the syntax after the closing delimiter. This fact is curcial to proof that the recursive calls to **bcall** and **ecall** using  $\gg$  terminate.

Calling the handler on the extracted program guaranties that the handler does not interact with syntax outside the intended scope. Nested scopes are handled using recursive calls to **ecall** if **BCall** operations are encountered while searching a closing delimiter.

Since the delimiters could be placed freely it is possible to mismatch them. If we encounter a closing before and opening delimiter, we know that they are mismatched. Wu et al. use Haskell's **error** function to terminate the program. In Agda we are not allowed to define partial functions, therefore we have to handle the error. We could either correct the error and just continue or short circuit the calculation using exceptions in form of e.g. a **Maybe** monad. For simplicity we will use

the former approach. In a real application it would be advisable to inform the programmer about the error, either using exceptions or at least trace the error.

```

bcall : { Nondet ∈ ops } → Free (Call :: Cut :: ops) A {i} → Free (Cut :: ops) A
ecall : { Nondet ∈ ops } → Free (Call :: Cut :: ops) A {i}
        → Free (Cut :: ops) (Free (Call :: Cut :: ops) A {i})

bcall (pure x)      = pure x
bcall (BCall κ)     = upcast (call (ecall (κ tt))) >>= bcall
bcall (ECall κ)     = bcall (κ tt) -- Unexpected ECall! We just fix the error.
bcall (Other s κ)   = impure (s , bcall ∘ κ)

ecall (pure x)      = pure (pure x)
ecall (BCall κ)     = upcast (call (ecall (κ tt))) >>= ecall
ecall (ECall κ)     = pure (κ tt)
ecall (Other s κ)   = impure (s , ecall ∘ κ)

```

Using the handlers defined above we can define a handler for scoped **Cut** syntax, which removes **Cut** and **Call** syntax simultaneously. The delimiters and correctly scoped **Cut** syntax is removed using **bcall** and potential unscoped **Cut** syntax is removed with a last use of **call**. The function **call'** is a smart constructor for the scope delimiters.

```

runCut : { Nondet ∈ ops } → Free (Call :: Cut :: ops) A → Free ops A
runCut = call ∘ bcall

call' : { Call ∈ ops } → Free ops A → Free ops A
call' p = do op bcalls ; x ← p ; op ecalls ; pure x

```

### 3.4 Call-Time Choice as Effect

Bunkenburg presented an approach to model call-time choice as a stack of scoped algebraic effects [Bun19]. In this section we will extend the nondeterminism effect from section 3.2.1 to one modelling call-time choice.

As explained in section 2.2.1, call-time choice semantics describe the interaction between sharing and nondeterminism. The current implementation of **Nondet** does not support sharing i.e. it is not possible for two choice to be linked. Based on Bunkenburg's implementation we will make two changes to the nondeterminism effect. Each choice is augmented with an optional identifier consisting of a triple of natural numbers, called *choice id*. The first two are used to identity the current scope and will be refereed to as *scope id*. The third number identifies the choice inside its scope. Furthermore, instead of producing a list the handler will now produce a tree of choices. This change allows to choose the evaluation strategy, e.g. depth first or breath first search, independent of the handler.

#### 3.4.1 Deep Effects

In Haskell and Curry ambient effects, like partiality, tracing and nondeterminism, can occur in components of data structures. Each argument of a constructor could be an effectful computation. For example, in Curry the tail of a list could be a nondeterministic choice between two possible tails. Such effects are sometimes called *deep effects*.

We want to simulate this behavior with algebraic effects. The effects have to be modelled explicitly using the **Free** type. We will lift data types using a standard construction, which is commonly used to simulate ambient deep effects [Abe+05; DCT19; CDB19]. The following example of an effectful **List** demonstrates the the general construction<sup>4</sup>.

```

data ListM (ops : List Container) (A : Set) : {Size} → Set where
  nil  : ListM ops A {i}
  cons : Free ops A → Free ops (ListM ops A {i}) → ListM ops A {↑ i}

```

<sup>4</sup>In the following code effectful data structures and lifted versions of functions are marked with a suffix <sup>M</sup>

$\text{List}^M \text{ ops } A$  represents a `List`  $A$  in whose components effects from the given effect stack  $\text{ops}$  can occur. To easily construct and work with lifted values we introduce smart constructors in the form of pattern synonyms.

```
pattern []M = pure nil
pattern _::M_ mx mxs = pure (cons mx mxs)
```

The size annotations on the lifted data structures are needed to proof termination of structural recursive functions. To pattern match on a lifted value we have to use  $\gg$ . Therefore the structural recursion is obscured.

```
_++M_ : Free ops (ListM ops A {i}) → Free ops (ListM ops A) → Free ops (ListM ops A)
mxs ++M mys = mxs >> λ where
  nil      → mys
  (cons mx mxs') → mx ::M mxs' ++M mys
```

### Normalization of Effectful Data

Based on Bunkenburg's code [Bun19] we will introduce a type class for normalizing effectful data structures i.e. moving interleaved `Free` layers to the outside using  $\gg$ .

```
record Normalform (ops : List Container) (A B : Set) : Set where
  field
    nf : A → Free ops B
  open Normalform { ... } public

!_ : { Normalform ops A B } → Free ops A → Free ops B
! mx = mx >> nf
```

The type class allow to normalize elements of type  $A$  (intuitively containing effectful calculations) to computations producing of elements of type  $B$  (intuitively a version of  $B$  without the effects). Instead of  $A$  and  $B$  we could have parameterized the type class over a type family of an effect stack, with `nf` producing an element of the type family applied to an empty stack. This implementation would allow us to restrict the normalizable types, but prohibit us from producing elements of standard data types.

In contrast to Bunkenburg's implementation we do not expect a lifted argument. Simplifying the type and introducing the helper function `!_` removes the need for auxiliary normalization lemmas for `pure` and `impure` values in proofs. The extra degree of freedom, introduced by a monadic argument, was not used in the original implementation.

```
instance
  N-normalform : Normalform ops ℕ ℕ
  Normalform.nf N-normalform = pure

  ListM-Normalform : { Normalform ops A B } →
    Normalform ops (ListM ops A {i}) (List B)
  Normalform.nf ListM-Normalform nil = pure []
  Normalform.nf ListM-Normalform (cons mx mxs) = ( ! mx :: ! mxs )
```

The data stored in an effectful list could also be effectful and therefore has to be normalized. We simply require a `Normalform` instance for the stored type. To allow normalization of general types and effectful data structures containing them, we have to implement dummy instances for data types like builtin natural numbers or booleans.

### 3.4.2 Sharing Handler

The idea of the following sharing handler is identical to the one presented by Bunkenburg. Thanks to the more flexible infrastructure described in the earlier sections we are able to define a more modular handler and avoid some inlining, necessary to prove termination in Coq. Similar to `Cut` the sharing handler is not orthogonal to other effects, but interacts with existing `Nondet` syntax.

The scoping operation `share` takes an additional argument, the unique identifier for the created scope. Similar to `put` the parameter is part of the container shape.

```
data Shares : Set where bshares eshares : ℕ × ℕ → Shares
pattern BShare n κ = impure (inj1 (bshares n) , κ)
pattern EShare n κ = impure (inj1 (eshares n) , κ)

Share : Container
Share = Shares ▷ λ _ → T
```

The handler has the same structure as other handlers for scoped effects like `Cut`. The `bshare` handler searches for opening delimiters, which are subsequently handled by `eshare`. `eshare` handles the part of the program in scope and returns the unhandled continuations, which is again handled using `bshare`. Nested scopes are handled using recursive `eshare` calls. To implement sharing the handler modifies the program in scope. Using `prj`, `NonDet` syntax is extracted and reinjected. Choice nodes are modified to now include the unique choice id. The identifier is generated from the scope id of the current sharing scope and a counter, which is managed by the handler. When ever a choice is tagged with an id the counter is increased. The uniqueness of the scope identifiers is not managed by the handler, but the share operator.

Due to the size annotations termination is proven on the type level. To implement the sharing handler it's not necessary to combine the two cases, as done by Bunkeburg in his Coq implementation.

```
bshare : { NonDet ∈ ops } → Free (Share :: ops) A {i} → Free ops A
eshare : { NonDet ∈ ops } → ℕ → ℕ × ℕ → Free (Share :: ops) A {i}
        → Free ops (Free (Share :: ops) A {i})

bshare (pure x) = pure x
bshare (BShare sid κ) = eshare 0 sid (κ tt) >>= bshare
bshare (EShare sid κ) = bshare (κ tt) -- mismatched scopes, we just continue!
bshare (Other s κ) = impure (s , bshare ∘ κ)

eshare next sid (pure x) = pure (pure x)
eshare next sid (BShare sid' κ) = eshare 0 sid' (κ tt) >>= eshare next sid
eshare next sid (EShare sid' κ) = pure (κ tt) -- usually test that sid' = sid
eshare next sid p@(Other s κ) with prj {NonDet} p
... | just (??s _ , κ') = inj $ ??s (just $ sid , next) , eshare (1 + next) sid ∘ κ'
... | just (fails , κ') = inj $ fails , λ()
... | nothing = impure (s , eshare next sid ∘ κ)
```

### 3.4.3 Share Operator

Next we will define the `share` operator as described by Bunkenburg. The operator generates new unique scope identifiers using a `State` effect. Furthermore, it shares all choices in the components of effectful data structures.

To map the operator over arbitrary structures the `Shareable` type class is introduced. The `shareArgs` function calls `share` recursively on the components of the shared data structure. Similar to `Normalform`, trivial instances for simple data types are introduced.

```
record Shareable (ops : List Container) (A : Set) : Set1 where
  field
    shareArgs : A → Free ops A
open Shareable { ... } public

instance
  shareable-ℕ : Shareable ops ℕ
  Shareable.shareArgs shareable-ℕ = pure
```

Using the instances for data we can implement Bunkenburg's version of the operator. The operator itself relies on a `State` effect, which is later executed as first effect in the stack, to generate the

identifiers. Given a computation producing values of type  $A$  the operator returns a computation of computations of type  $A$  i.e. the result has two **Free ops** layers. The outer layer is usually execute (injected at into the larger program at the current point) immediately using  $\gg$ . The outer computation generates a new identifier. The inner computation captures the identifier, therefore binding the inner computation multiple times yields multiple scopes with the same id. An in depth explanation can be found in “Modeling Call-Time Choice as Effect using Scoped Free Monads” [Bun19].

```

share : { Shareable ops A } → { Share ∈ ops } → { State (N × N) ∈ ops } →
  Free ops A → Free ops (Free ops A)
share p = do (i, j) ← get
            put (1 + i, j)
            pure do op $ bshares (i, j)
                  put (i, 1 + j)
                  x ← p
                  x' ← shareArgs x
                  put (1 + i, j)
                  op $ eshares (i, j)
                  pure x'

```

Using **share** we can implement a shareable instance for effectful lists. In the original Haskell implementation **shareArgs** is a higher order function, which takes **share** as an additional argument. For simplicity and to avoid termination problems this is not the case in the Agda implementation.

```

instance
  ListM-shareable : { Shareable ops A } → { Share ∈ ops } → { State (N × N) ∈ ops }
    → Shareable ops (ListM ops A {i})
  Shareable.shareArgs ListM-shareable nil = []M
  Shareable.shareArgs ListM-shareable (cons mx mxs) = cons <$ share mx <*> share mxs

```

### 3.4.4 Examples

Using the handler we can simulate call-time choice semantics using effects in Agda. Call-time choice can be simulated with the following effect stack

```

CTC : List Container
CTC = State (N × N) :: Share :: NonDet :: []

```

Before calling any handlers the data is normalized, so that not only surface, but also deep effects are evaluated. State is evaluated first to generate the identifiers for sharing. Sharing is evaluated next to tag all choices with their scopes identifiers. At last nondeterminism is evaluated to collect the results of all possible branches, taking the scope ids into account.

```

runCTC : { Normalform CTC A B } → Free CTC A → List B
runCTC p = dfs empty $ run $ runNonDet $ bshare $ evalState (0, 0) (! p)

```

Now we can implement the **doubleCoin** example from section 2.2.

```

coin : { NonDet ∈ ops } → Free ops N
coin = pure 0 ??' pure 1

doubleCoin : { Share ∈ ops } → { State (N × N) ∈ ops } → { NonDet ∈ ops } →
  Free ops N
doubleCoin = share coin >> λ c → c + c

```

By calling **share** the choice in **coin** is shared. By binding the result of **share** the computation tree generating the ids (i.e. the outer layer) is expanded. The argument of the continuation  $c$  is itself a program, it's the original coin function wrapped into a sharing scope, which captures the generated id of the outer scope. By binding  $c$  this computation is injected into the whole computation. Binding  $c$  multiple times yields the same scope, because the scope identifier is captured. Equal scope identifier yield equal decisions during the evaluation of **NonDet**.

```

runCTC doubleCoin ≡ 0 :: 2 :: []

```

$$\begin{array}{ll}
\text{pure } x \gg k = k \ x & (\text{ident-left}) \\
m x \gg \text{pure} = m x & (\text{ident-right}) \\
m x \gg f \gg g = m x \gg \lambda x \rightarrow f x \gg g & (\text{assoc}) \\
\\ 
\text{fail} \gg k = \text{fail} & (\text{fail-absorb}) \\
(p \text{ ?? } q) \gg k = (p \gg k) \text{ ?? } (q \gg k) & (\text{??-algebraic}) \\
\\ 
\text{share fail} = \text{pure fail} & (\text{share-fail}) \\
\text{share } \perp = \text{pure } \perp & (\text{share-}\perp) \\
\text{share } (p \text{ ?? } q) = \text{share } p \text{ ?? share } q & (\text{share-??}) \\
\text{share } (c \ x_1 \dots x_n) = \text{share } x_1 \gg \lambda y_1 \dots \text{share } x_n \gg \lambda y_n \rightarrow \text{pure } (\text{pure } (c \ y_1 \dots y_n)) & (\text{HNF})
\end{array}$$

Figure 3.1: laws for a monad with sharing by Fischer et al.

### 3.4.5 Laws of Sharing

Fischer et al. introduced a set of equations characterizing call-time choice semantics [FKS09]. The equations can be found in figure 3.1. The first three laws are just the monad laws, which were proven in section 3.1.2. Section 3.2.1 contains a proof for the fourth law. The fifth law is the algebraicity of `??`, which follows for any operation directly from the definition of `≫`.

$$\begin{array}{l}
\text{??-algebraic} : \llbracket \_ : \text{Normalform CTC } B \ C \rrbracket \rightarrow \llbracket \_ : \text{Shareable CTC } B \rrbracket \rightarrow \\
(p \ q : \text{Free CTC } A) \ (k : A \rightarrow \text{Free CTC } B) \rightarrow \\
\text{runCTC } ((p \text{ ??' } q) \gg k) \equiv \text{runCTC } ((p \gg k) \text{ ??' } (q \gg k)) \\
\text{??-algebraic } p \ q \ k = \text{refl}
\end{array}$$

In addition to the monad laws and equations for `??` they introduced equations involving `share`.

$$\begin{array}{l}
\text{share-fail} : \llbracket \_ : \text{Normalform CTC } A \ B \rrbracket \rightarrow \llbracket \_ : \text{Shareable CTC } A \rrbracket \rightarrow \\
\text{runCTC } \{A\} \ \{B\} \ (\text{share fail' } \gg \text{id}) \equiv \text{runCTC } \{A\} \ \{B\} \ (\text{pure fail' } \gg \text{id}) \\
\text{share-fail} = \text{refl}
\end{array}$$

The second law involving `share` does not apply to our effect stack, because we have no notion of `undefined`. Partiality can be implemented identical to `fail` with carrier `Maybe`. The effect would be placed last in the stack to allow canceling all running calculations. The law can be proven analogous to the one for `fail`.

The third law involving `share` states that `share` distributes over `??`. This law doesn't hold for this implementation, because there is no guarantee that `get` or `put` aren't called outside the sharing operator. Developing another implementation satisfying the laws in all cases is outside the scope of this thesis.

The last law states that `share` distributes over the components of effectful data structures. Since our representation for effectful data isn't uniform this law has to be proven on a case by case basis. One could try to automate this proves using tactics, find an equivalent formulation which doesn't refer to constructors directly or use a different representation for effectful data (e.g. fixed points of polynomial functors, since they can be made effectful generically).

## Chapter 4

# Higher Order Syntax

To address problems of the first order approach, like mismatched scope delimiters and explicit control over the continuation, Wu et al. introduced a second approach utilizing higher order syntax [WSH14]. Bunkenburg already tried to implement some scoped effects using this approach, but failed due to limitations of Coq [Bun19].

Chapter 3 demonstrated how the first order approach could be transferred to Agda utilizing container representations for functors and sized types. This chapter focuses on the implementation of effects using higher order syntax. It partially follows Bunkenburg’s approach, because the limitation of Coq described by him does not exist in Agda. Therefore this chapter focuses on expanding his approach further. Due to other limitations, needed for the consistency of Agda, this approach ultimately failed again.

### 4.1 Higher Order Syntax

In the first order approach effects only store possible continuations. In the higher order approach by Wu et al. scoped effects store possible continuations as well as the part of the program in their scope.

In the first order approach the functors, which describe the syntax, are applied to types of the form `Free F A` i.e. programs consisting of syntax as described by `Free F`, which produce values of type `A`. In the higher order approach these functors are generalized to higher order functors i.e. in Haskell a data type of kind `(* -> *) -> (* -> *)`. These functors are applied to `Free F` and `A` separately.

Because the program type is separated in syntax and result type it is possible to store programs, which use the same signature but produce values of different types. Consider the following definition of the higher order exception syntax as given by Wu et al.

```
data HExc e m a = Throw e | forall x. Catch (m x) (e -> m x) (x -> m a)
```

The catch operation stores the computation in the scope of the catch block `m x`, the handler producing an alternative value in case of an error `e -> m x` as well as the continuation `x -> m a`. The three programs agree on an arbitrary, but per `catch` fixed type `x`.

Calling `>>=` on a higher order term just extends the continuation i.e. just substitutes the variables in the trees of type `m a`. See figure 4.1 for an example. Therefore these operations aren’t algebraic but also capture the notation of scopes.

### 4.2 Representing Strictly Positive Higher Order Functors

In Haskell the generalization to higher order syntax is straight forward. In Agda we again have to find an appropriate representation for functor to guaranty strict positivity, which leads to the idea

The diagram illustrates the application of the `>>=` operator to a term. It shows a term `Throw e` being transformed into `Catch (m x) (e -> m x) (x -> m a)`, where the scope `x` is introduced and the continuation `x -> m a` is substituted into the original term.

Figure 4.1: calling `>>=` on operations with and without scopes (TODO)



of an indexed container as described by Altenkirch et al. [Alt+15]<sup>1</sup>.

Indexed containers from the paper as well in the Agda standard library are defined as follows<sup>2</sup>.

```
record IndexedContainer (I O : Set1) : Set1 where
  field
    Shape : O → Set
    Pos : ∀ {o} → Shape o → Set
    Ctx : ∀ {o} → (s : Shape o) → Pos s → I

  [ ] : (I → Set) → (O → Set)
  [ ] F A = Σ [ s ∈ Shape A ] ((p : Pos s) → F (Ctx s p))
```

Allowing indices of arbitrary levels and instantiating  $I$  and  $O$  with  $\text{Set}$  gives rise to a container extension of the correct shape.

The above definition is similar to Bunkenburg’s first definition of a container representation for a higher order functor. His definition is given below.

```
record HContainer : Set2 where
  field
    Shape : Set1
    Pos : Shape → Set
    Ctx : (s : Shape) → Pos s → Set → Set

  [ ] : (Set → Set1) → (Set → Set1)
  [ ] F A = Σ [ s ∈ Shape ] ((p : Pos s) → F (Ctx s p A))
```

In the second definition the  $\text{Shape}$  and  $\text{Pos}$  types cannot depend on the given index i.e. the argument for the returned functor. Otherwise, the both definitions are quite similar. All stored elements are lifted by the given functor  $F$ . The type of the  $F$ ’s argument is generated using  $\text{Ctx}$ .  $\text{Ctx}$  has access to the chosen shape, accessed position and the argument type  $A$ . Conceptually,  $\text{Ctx}$  is used to choose between the stored  $X$  and the argument type  $A$  i.e. programs inside or outside the operations scope.

We can define  $\text{hmap}$  for both, which preserves identity and composition. As noted by Bunkenburg, we cannot define  $\text{emap}$  for all extensions of a such a higher-order functor i.e. the produced type constructor is not necessarily a functor.

```
hmap : {F G : Set → Set1} → (F → G) → ([ ] F → [ ] G)
hmap (s , pf) = s , ◦ pf

emap : {F : Set → Set1} → (F A → F B) → [ ] F A → [ ] F B
emap f (s , pf) = s , λ p → {! it’s not clear if the type of pf p involves A!}
```

Similar to the Haskell implementation by Wu et al. we could define a type class to implement  $\text{emap}$  for all valid higher-order functors. Both representations share another problem, the produced type constructor is not necessarily strictly positive. This is a necessary requirement to define inductive, effectful data structures.

Bunkenburg fixed this problem by switching to version of a Bi-Container. A Bi-Container has two position types for each shape. Its extension is a Bifunctor, which is strictly positive in both arguments. One set of positions can be used to store computations producing values of type  $A$ , while the (using the indexing mechanism from above) stores computations producing values involving the captured type  $X$ . Defining inductive, effectful data types with this approach isn’t a problem, because the positions for  $A$  are used identical to the first-order approach.

Alternatively, one could fix the positivity problem by returning a first order container instead of a type constructor from  $\text{Ctx}$ . In most effects  $A$  is only used directly i.e. the Haskell functor contains  $\mathbf{a}$  only as  $\mathbf{m} \ \mathbf{a}$ . For the following simple examples we can therefore simplify  $\text{Ctx}$  further to avoid complicated representations, which aren’t needed. Alternatively, we could use the indexed Bi-Container. Going forward we will use the simplified indexed container, because it resembles the Haskell implementation more closely.

<sup>1</sup>Note that this is not the first publication related to indexed containers. Papers of the same name, by the same author(s) exist, as well as data types, known as “Interaction Structures” with essentially the same shape.

<sup>2</sup>The names of the fields are changed to highlight differences between the different definitions.



```

record Container : Set2 where
  constructor _◁_/_
  field
    Shape : Set1
    Pos : Shape → Set
    Ctx : (s : Shape) → Pos s → Maybe Set1

[ ] : (Set1 → Set1) → Set1 → Set1
[ ] F A = Σ[ s ∈ Shape ] ((p : Pos s) → F (fromMaybe A (Ctx s p)))

hmap : {F G : Set1 → Set1} → (F → G) → ([ ] F → [ ] G)
hmap (s , pf) = s , ◦ pf

emap : {F : Set1 → Set1} {X Y : Set1} → (F X → F Y) → [ ] F X → [ ] F Y
emap {F} {X} {Y} f (s , pf) = s , λ p → helper s p (pf p)
  where helper : (s : Shape) (p : Pos s) →
    F (fromMaybe X (Ctx s p)) → F (fromMaybe Y (Ctx s p))
    helper s p x with Ctx s p
    ... | nothing = f x
    ... | just _ = x
open Container

```

Ultimately the choice of representation for the functor doesn't matter, because all approaches based on storing a type directly encounter the problem described in section 4.3.

Using our choice of functor representation we can define the free monad for higher order syntax. As in Haskell, the argument for the functor in the `impure` case is split.

```

data Prog (C : Container) (A : Set1) : Set1 where
  pure   : A → Prog C A
  impure : [ C ] (Prog C) A → Prog C A

```

Notice that due to the potentially captured type in the `Shape`, stored in the container extension, the universe level for `Prog` increased to 1. This allows us to increase the universe level of `A` to one, allowing us to define effectful data structures.

### 4.3 Effectful Data and Existential Types

A central problem with this approach is that it cannot model deep effects without involving variable levels. Consider the the following definition of an effectful list.

```

data ListM (C : Container) (A : Set1) : Set1 where
  nil   : ListM C A
  cons : Prog C A → Prog C (ListM C A) → ListM C A

```

`ListM C A` is an element of `Set1`, because it stores elements of type `Prog C X`, which is an element of `Set1`. `Prog C X` is an element of `Set1`, because it holds values of the container extension i.e. elements of the `Shape` type, which is an element `Set1`, because it has to store the result type of the subcomputation `X`. Therefore the `ListM C A` is too large to be stored as result type of a subcomputation. Therefore it is not possible to call a scoped operation (such as `share`) on an effectful data structure.

More generally speaking, let us fix the universe level of the result type `X` of the subcomputation  $\ell_X = l$ . The type is stored in the `Shape`, therefore the universe level of the `Shape` type is given by  $\ell_S = l + 1$ . Because the `Prog` stores an element of the `Shape` its level is given by  $\ell_P = \ell_S$ . Effectful data structures live in the same universe as `Prog`, but are simultaneously required to be stored in the subcomputation. We obtain the contradictory requirements  $\ell_E = \ell_P = \ell_S = l + 1$  and  $\ell_E \leq l$ .

Holding on to the idea of storing types in the `Shape`, the only way to fix this problem is to let all levels vary as needed. This leads to different levels across the program, which are different to unify. Furthermore, when mapping a scoped operation over a recursive data structure (e.g. `share`) the increase in the universe level depends on the depth of the structure. Both of these phenomena are hard to deal with and in a complex program potentially unsolvable.

## 4.4 The Problem with Indexing

One could try solving the problem of existential types by indexing the program over a typing context. The level of the index is independent from the level of the structure, therefore the chain of reasoning from section 4.3 does not apply. The typing context needs to have the same structure as the program.

A central problem with this approach is that every call of  $\gg$  changes the structure of the program and therefore the context. These changes now have to be reflected on the type level, because the typing context has to reflect the programs shape. If  $\gg$  substitutes leaves differently, the changes to the context aren't simple substitutions, but depend on the stored value. As with increasing universe levels, this complications are increasingly hard to deal with and cannot be hidden from the user of the library.

## Chapter 5

# Scoped Algebras

Due to the deep-rooted problem with the higher order approach from chapter 4 it seemed reasonable to search for another formulation of scoped effects, which does not rely on existential types. Piróg et al. [Pir+18] presented a novel formulation for scoped operations and their algebras, which fulfils this requirement. Their approach does not describe the combination of multiple effects, but due to the different structure the approach seemed worth exploring nonetheless.

This chapter transfers the basic implementation from Piróg et al. to Agda, derives a different implementation of `fold`, based on the work by Fu and Selinger [FS18], for their monad to aid termination checking and presents an idea for modularisation of their algebras.

### 5.1 The Monad $E$

Piróg et al. describe a monad, which is suited for modelling operations with scopes [Pir+18]. The monad is the result of rewriting a slightly modified version of the monad from “Effect Handlers in Scope” i.e. the monad used in chapter 4. They separate the signature into one describing effects with scopes  $\Gamma$  and one describing the algebraic effects  $\Sigma$ . The monad  $E$  can be described as the fixpoint of the following equation, where the coend (the integral sign) denotes an existential types.

$$EA \cong A + \Sigma(EA) + \int^{X \in \mathcal{C}} \Gamma(EX) \times (EA)^X$$

This representation looks appropriate considering our earlier definition. An element of the monad is either a value of  $A$ , an operation without scopes, i.e. a functor applied to `Free F A` or an operation with scopes. Operations with scopes (e.g. `catch`) always quantified over some type to store subprograms over the same signature but with different local result type. Furthermore they provided a continuation, which transformed values of the internal result type to the result type of the whole program. [GAMMA] The following Agda data type represents the above monad.

```
data ProgE (Σ Γ : Container) (A : Set) : Set₁ where
  var : A → ProgE Σ Γ A
  op  : [ Σ ] (ProgE Σ Γ A) → ProgE Σ Γ A
  scp : {X : Set} → [ Γ ] (ProgE Σ Γ X) → (X → ProgE Σ Γ A) → ProgE Σ Γ A
```

Notice again that this definition requires  $X$  to be a smaller type than  $E$  i.e. it's not sufficient to model deep effects as explained in chapter 4. Piróg et al. also not size issues with this definition.

Piróg et al. rewrite this definition using a left Kan extension and derive the following equivalent monad without the existential type.

$$EA \cong A + \Sigma(EA) + \Gamma(E(EA))$$

An equivalent monad without the existential type is a promising candidate for modelling deep effects in Agda, because it avoids the size issues.

The monad models scopes using the double  $E$  layer. The outer layer corresponds to the part of program in scope. By evaluating it (i.e. the part of the program in scope) one obtains a value of type  $EA$ , the rest of the program producing a result of type  $A$ . This resulting program corresponds to the continuation in the higher order approach, which was a function mapping from the the result of the scoped program to the rest of the whole program.

## 5.2 The Prog Monad

In this section we will define the central monad for this approach. Because signatures are split into effects with and without scopes we will define effects as pairs of functors and therefore **Containers**.

```
record Effect : Set1 where
  field
    Ops Scps : Container
  open Effect public
```

The functions **ops** and **scps** combine the corresponding signatures of a **List** of **Effects**.

```
ops scps : List Effect → Container
ops = sum ∘ mapL Ops
scps = sum ∘ mapL Scps
```

Using these helper functions we can define a modular version of the monad by Piróg et al [Pir+18]. It's equivalent to the fixpoint and the Haskell definition from the paper (assuming that signatures are given by strictly positive functors).

```
data Prog (effs : List Effect) (A : Set) : Set where
  var : A → Prog effs A
  op : [ ops effs ] (Prog effs A) → Prog effs A
  scp : [ scps effs ] (Prog effs (Prog effs A)) → Prog effs A
```

Piróg et al. also derive algebras for the above monad, which correctly model scoped effects. To implement their recursion scheme we have to define  $\gg$  for **Prog effs A**. Notice that **Prog** is a truly nested or non-regular data type [BM98].

Defining recursive functions for these data types is more complicated. The “direct” implementations of **fmap** and  $\gg$  do not obviously terminate. Augmenting **Prog** with size annotations leads to problems when proving the monad laws<sup>1</sup>. Instead we will define a generic **fold**, which we can reuse for all functions traversing elements of **Prog effs A**.

### 5.2.1 Folds for Nested Data Types

Defining recursion schemes for complex recursive data types is a common problem. Fu and Selinger demonstrate a general construction for **fold**s for nested data types in Agda [FS18]. Following their construction and adapting it to arbitrary branching trees leads to a sufficiently strong **fold** to define all important functions for **Prog effs A**.

**Index Type** The first part of the construction by Fu and Selinger is to define the correct index type for the data structure. The index type describes the recursive structure of the data type i.e. how the type variables at each level are instantiated. For complex mutual recursive data types the index type takes the form of a branching tree. For **Prog effs** the one type variable is either instantiated with the value type *A* (**pure**) or some number of **Prog effs** layers applied to the current type variable (**op**, **scp**). Our index type therefore just counts the number of **Prog effs** layers. Natural numbers are sufficient.

Next Fu and Selinger define a type level function, which translates a value of the index type to its corresponding type. For **Prog effs A** this function just applies **Prog effs** *n* times to *A*. The operator  $\hat{\_}$  applies a function *n*-times to a given argument *x* i.e. it represents *n*-fold function application, usually denoted  $f^n(x)$ .

$$\begin{aligned} \hat{\_} &: \forall \{ \ell \} \{ C : \text{Set } \ell \} \rightarrow (C \rightarrow C) \rightarrow \mathbb{N} \rightarrow C \rightarrow C \\ (f \hat{\_} 0) \quad x &= x \\ (f \hat{\_} \text{succ } n) \quad x &= f((f \hat{\_} n) x) \end{aligned}$$

<sup>1</sup>As in chapter 4 the monad laws only hold for size  $\infty$ , but working with size  $\infty$  in proofs leads to termination problems. The **scp** constructor can produce an arbitrary number of **Prog effs** layers. This forces us to use our induction hypothesis on not obviously smaller terms, but the size annotation is assumed to be  $\infty$ .

**Recursion Scheme** Next we will define **fold** for  $\text{Prog } \text{effs } A$ . The fold produces an arbitrary  $\mathbb{N}$  indexed value. The type family  $P$  determines the result type at each index. The **fold** produces a value of type  $P n$  for a given value of type  $(\text{Prog } \text{effs } \wedge n) A$ . Furthermore the **fold** takes functions for processing substructures. As usual, the arguments of these function correspond to those of the constructors they processes with recursive occurrences of the type itself already processed. The cases are obtained by pattern matching on the index type and the value of type  $(\text{Prog } \text{effs } \wedge n) A$  i.e. the value of the type depending on the index.

```

fold : (P :  $\mathbb{N} \rightarrow \text{Set}$ )  $\rightarrow \forall n \rightarrow$ 
  (A  $\rightarrow P \text{ } 0$ )  $\rightarrow$ 
  ( $\forall \{n\} \rightarrow P n \rightarrow P (\text{succ } n)$ )  $\rightarrow$ 
  ( $\forall \{n\} \rightarrow \llbracket \text{ops } \text{effs} \rrbracket (P (\text{succ } n)) \rightarrow P (\text{succ } n)$ )  $\rightarrow$ 
  ( $\forall \{n\} \rightarrow \llbracket \text{scps } \text{effs} \rrbracket (P (\text{succ } (\text{succ } n))) \rightarrow P (\text{succ } n)$ )  $\rightarrow$ 
  ( $\text{Prog } \text{effs } \wedge n) A \rightarrow P n$ 
fold P 0 a v o s x = a x
fold P (succ n) a v o s (var x) = v ( fold P n a v o s x )
fold P (succ n) a v o s (op x) = o (map ( fold P (succ n) a v o s ) x)
fold P (succ n) a v o s (scp x) = s (map ( fold P (succ (succ n)) a v o s ) x)

```

Notices that for the **op** and **scp** constructors the recursive occurrences and potential additional values are determined by the **Container**. The functions therefore processor arbitrary **Container** extensions, which contain solutions for the corresponding index. When implementing those two cases we cannot apply **fold** directly to recursive occurrences, because those depend on the choice of **Container**. **map** for **Containers** exactly captures the correct behavior.

The **fold** function, based on the approach by Fu and Selinger, is similar to the one by Piróg et al. Piróg et al. derived their **fold** by deriving algebras for a second monad. In “Syntax and Semantics for Operations with Scopes” [Pir+18] they show that the two monads are equivalent and therefore transfer the **fold** from the second monad to the one used in their Haskell implementation. Following Fu and Selinger we derived essentially the same **fold** and implemented it directly i.e. without the use of  $\gg$ .

**Example** Using **fold** we can implement  $\gg$  for  $\text{Prog } \text{effs } A$ . The continuations  $k$  passed to  $\gg$  should just effect the inner most layer. Intuitively, when using **bind** on a value constructed with **scp** we traverse the outer layer and call **bind** on the inner one recursively. To implement  $\gg$  we fold over the first argument. We could fix the arbitrary  $n$  to be 1, but defining a version generic in  $n$  is useful for later proofs. The  $\mathbb{N}$  indexed type **bind-P** defines the type for the intermediate result at every layer.

```

bind-P :  $\forall A B \text{ effs} \rightarrow \mathbb{N} \rightarrow \text{Set}$ 
bind-P A B effs 0 = A
bind-P A B effs (succ n) =  $\text{Prog } \text{effs } \wedge (\text{succ } n) \$ B$ 

```

$\gg$  corresponds to variable substitution i.e. it replaces the values stored in **var** leaves with subtrees generated from these values. Calling  $k$  on a program with zero layers (a value of type  $A$ ) would produce a program with one layer. Therefore,  $\gg$  can only be called on programs with at least one layer. The lowest layer is extended with the result of  $k$ . For all numbers greater than zero we produce a program with the same structure but a different value type. For layer zero (i.e. values) we could either produce a value of type  $\text{Prog } \text{effs } B$  or leave the value of type  $A$  unchanged. In both cases we have to handle the lowest **var** constructors differently.

```

bind :  $\forall n \rightarrow (\text{Prog } \text{effs } \wedge \text{succ } n) A \rightarrow (A \rightarrow \text{Prog } \text{effs } B) \rightarrow$ 
  ( $\text{Prog } \text{effs } \wedge \text{succ } n) B$ 
bind {effs} {A} {B} n ma k = fold (bind-P A B effs) (succ n) id ( $\lambda$  where
  {0} x  $\rightarrow k x$ 
  {succ n} x  $\rightarrow \text{var } x$ 
  ) op scp ma

```

We left the values unchanged, therefore the **var** constructor at layer zero has to produce value of type  $\text{Prog } \text{effs } B$  by calling  $k$ . In all other cases we replace each constructor with itself to leave these parts unchanged.

Using  $\gg$  for a program with one layer and `var` as `return` we can define a monad instance for `Prog effs`. In contrast to Haskell this automatically defines a functor and an applicative instances, because these can be defined in terms of  $\gg$  and `return`<sup>2</sup>.

```
instance
  Prog-RawMonad : RawMonad (Prog effs)
  Prog-RawMonad = record { return = var ; _>>_ = bind 0 }
```

The record (which is used as a type class) is part of the Agda standard library. It is named `RawMonad`, because it does not enforce the monad laws. We will prove the laws in section 5.2.3 using a technique from section 5.2.2.

### 5.2.2 Induction Schemes for Nested Data Types

Following the examples by Fu and Selinger [FS18] we can generalize the `fold` from section 5.2.1 to a dependently type version, an induction principle. In the induction principle the result type/proposition `P` is generalized to a dependent type. Therefore the induction principle allows for proofs of predicates by induction without explicit recursion.

The types for the four functions, corresponding to the three constructors and the base case, also have to be generalized.

$$\text{ind} : (P : (n : \mathbb{N}) \rightarrow (\text{Prog effs} \wedge n) A \rightarrow \text{Set}) \rightarrow \forall n \rightarrow$$

In the base case the given value of type `A` is the handled value. Therefore the value is bound and passed to the proposition.

$$(\lambda x : A \rightarrow P \mathbf{0} x) \rightarrow$$

The `var` can be handled similar to the examples by Fu and Selinger. An additional hidden parameter `x` for the smaller, recursively handled value is introduced. Because `x` represents the recursively handled type its part of the smaller results type. Furthermore, the parameter is used to describe the currently handled value `var x`. `var x` is therefore part of the functions result type.

Under the Curry Howard corresponds this function (ignoring the index type) can be read as the proposition  $\forall x. P(x) \Rightarrow P(\text{var } x)$  i.e. the induction step for the constructor `var`.

$$(\forall \{n\} \rightarrow P n x \rightarrow P (\text{succ } n) (\text{var } x)) \rightarrow$$

Similar to `fold` dealing with `op` and `scp` is more complicated, because they represent arbitrarily branching nodes. Remember that a containers position function maps from a type of positions, which depends on the values shape, to the contained values. Hence, assuming the containers values corresponds to assuming a position function. Analogues to the `fold` the result for the recursively handled value is function, mapping from positions, for the assumed shape, to proofs for the proposition for the there contained values. The value for the position is obtained using the assumed position function  $\kappa$ . The currently handled value is constructed using `s` and  $\kappa$ . Notice that the each of the four parameters depends on all its predecessors.

$$\begin{aligned} &(\forall \{n\} s \{ \kappa \} \rightarrow ((p : \text{Pos} (\text{ops effs}) s) \rightarrow P (1 + n) (\kappa p)) \rightarrow P (\text{succ } n) (\text{op } (s, \kappa))) \rightarrow \\ &(\forall \{n\} s \{ \kappa \} \rightarrow ((p : \text{Pos} (\text{scps effs}) s) \rightarrow P (2 + n) (\kappa p)) \rightarrow P (\text{succ } n) (\text{scp } (s, \kappa))) \rightarrow \\ &(x : (\text{Prog effs} \wedge n) A) \rightarrow P n x \end{aligned}$$

The actual implementation of the induction principle is straight forward and similar to the one for `fold`. The composition with the position function corresponds to the call to `map`.

$$\begin{aligned} \text{ind } P \mathbf{0} a v o s x &= a x \\ \text{ind } P (\text{succ } n) a v o s (\text{var } x) &= v (\text{ind } P n a v o s x) \\ \text{ind } P (\text{succ } n) a v o s (\text{op } (c, \kappa)) &= o c (\text{ind } P (\text{succ } n) a v o s \circ \kappa) \\ \text{ind } P (\text{succ } n) a v o s (\text{scp } (c, \kappa)) &= s c (\text{ind } P (\text{succ } (\text{succ } n)) a v o s \circ \kappa) \end{aligned}$$

<sup>2</sup>We automatically obtain the functions  $\ll$ ,  $\ll\ll$ , `pure` and  $\gg$ .

### 5.2.3 Proving the Monad Laws

**Left Identity** First we will prove the left identity law. Because the value passed  $\gg$  constructed using `return` i.e. `var` both sides of the equality can be directly evaluated to  $k\ a$ .

$$\begin{aligned} \text{bind-ident}^! &: \forall \{A\ B : \text{Set}\} \{a\} \{k : A \rightarrow \text{Prog}\ \text{effs}\ B\} \rightarrow \\ &(\text{return}\ a \gg k) \equiv k\ a \\ \text{bind-ident}^! &= \text{refl} \end{aligned}$$

**Right Identity** When proving the right identity the value passed to  $\gg$  can be an arbitrarily complex program. Therefore the proposition is not “obvious” as it was the case with `bind-ident`<sup>!</sup>.

$$\text{bind-ident}^r : \{A : \text{Set}\} (ma : \text{Prog}\ \text{effs}\ A) \rightarrow (ma \gg \text{return}) \equiv ma$$

$\gg$  is recursive in its first argument, therefore we will prove the proposition by induction on  $ma$ . To use the induction scheme we have to define a proposition for every layer. Since  $\gg$  does not change values we simply produce a value of type  $\top$  at layer zero. For all other we proof the proposition for the appropriate `bind` i.e. the one called by `fold` to handle a value for the given  $n$ .

$$\text{bind-ident}^r \{ \text{effs} \} \{ A \} = \text{ind} (\lambda \{ 0 \_ \rightarrow \top ; (\text{succ}\ n) p \rightarrow \text{bind}\ n\ p\ \text{var} \equiv p \})$$

We call the induction scheme with the given value with one layer, therefore the initial  $n$  is `1`. The “proof” for values can be inferred, because for each value it’s just a value of the unit type.

$$1 \_$$

To proof that the proposition holds for values constructed using `var` we have to case split on the number of layers  $n$ . For `0` we have to proof that `var`  $x$  is equal to itself, because  $\gg$  leaves values unchanged. This proof forms the basis for our induction.

For the second case we are given a program  $x$  with `succ`  $n$  layers and an induction hypothesis  $IH$  that the proposition holds for a call to `bind`  $n$ . We have to prove that the proposition holds for `bind` (`succ`  $n$ ) and the new program `var`  $x$ . By applying the  $\gg$  rule for `var` (for  $n$  greater than zero) we can move `var` to the outside. The new proposition is `var` (`bind`  $n$ )  $\equiv$  `var`  $x$ . This proposition is equal to the induction hypothesis with `var` applied to both sides. Therefore we can proof it using congruence.

$$(\lambda \{ \{0\} \} (\text{tt}) \rightarrow \text{refl} ; \{ \text{succ}\ n \} IH \rightarrow \text{cong}\ \text{var}\ IH)$$

The proofs for the `op` and `scp` are identical and similar to the `var` case. For each shape  $s$  we are given a proof for each position of the given shape. We have to proof that the proposition holds for a new program constructed using either `op` or `scp`. For both constructors `bind`  $n$  calls itself recursively on the all contained values i.e. the results of the position function. Using congruence we can simplify the equality to the equality of the position functions. By invoking the axiom of extensionality we can prove the equality for each position. This equality is exactly the one given by the induction hypothesis.

$$\begin{aligned} &(\lambda\ s\ IH \rightarrow \text{cong}\ (\text{op} \circ (s\ \_))\ (\text{extensionality}\ IH)) \\ &(\lambda\ s\ IH \rightarrow \text{cong}\ (\text{scp} \circ (s\ \_))\ (\text{extensionality}\ IH)) \end{aligned}$$

**Associativity** The proof for associativity follows the same pattern as the one for the right identity.  $\gg$  is defined by recursion on its first argument. We therefore proof the proposition by induction on  $ma$ . In all cases the left-hand side reduces to the induction hypothesis in the same manner as before. Therefore these cases look identical.

$$\begin{aligned} \text{bind-assoc} &: \forall \{A\ B\ C\} \\ &(f : A \rightarrow \text{Prog}\ \text{effs}\ B) (g : B \rightarrow \text{Prog}\ \text{effs}\ C) (ma : \text{Prog}\ \text{effs}\ A) \rightarrow \\ &(ma \gg f \gg g) \equiv (ma \gg \lambda a \rightarrow f\ a \gg g) \\ \text{bind-assoc}\ f\ g &= \text{ind} \\ &(\lambda\ \text{where} \end{aligned}$$

$$\begin{aligned}
& 0 \ p \quad \rightarrow \top \\
& (\text{succ } n) \ p \rightarrow \text{bind } n \ (\text{bind } n \ p \ f) \ g \equiv \text{bind } n \ p \ \lambda a \rightarrow \text{bind } 0 \ (f \ a) \ g \\
& ) \ 1 \ - \\
& (\lambda \{ \{0\} \ - \rightarrow \text{refl} ; \{ \text{succ } n \} \ IH \rightarrow \text{cong var } IH \} ) \\
& (\lambda s \ IH \rightarrow \text{cong } (\text{op} \circ (s \ , \_)) \ (\text{extensionality } IH)) \\
& (\lambda s \ IH \rightarrow \text{cong } (\text{scp} \circ (s \ , \_)) \ (\text{extensionality } IH))
\end{aligned}$$

**Functor and Applicative Laws** The monad laws imply the functor and applicative laws. We can proof them without using explicit induction by rewriting equations involving  $\gg$  using the above law. These proofs are simpler than the ones explicitly involving the definition of  $\gg$  using **fold**. We can write them using the chain reasoning operators as described by Norell [Nor07].

$$\begin{aligned}
& \text{fmap-id} : \forall \{ \text{effs} \} \{ A \ B : \text{Set} \} \rightarrow (ma : \text{Prog effs } A) \rightarrow (\text{id} \ \<\$ \ ma) \equiv ma \\
& \text{fmap-id } ma = \text{begin} \\
& \quad (\text{id} \ \<\$ \ ma) \quad \equiv \langle \rangle \text{ -- definition of } \<\$ \rangle \\
& \quad (ma \gg \lambda a \rightarrow \text{var } (\text{id } a)) \equiv \langle \rangle \text{ -- definition of id and } \eta\text{-conversion} \\
& \quad (ma \gg \text{var}) \quad \equiv \langle \text{bind-ident}^r \ ma \rangle \\
& \quad ma \quad \blacksquare
\end{aligned}$$

## 5.3 Combining Effects

Similar to chapter 4 we reuse parts of the infrastructure from chapter 3. Each **Effect** consists of a pair of **Containers**, one representing scoped and one representing unscoped effects. Therefore, an **Effect** stack now stores pairs of containers, not containers directly. The type  $\_ \in \_$  together with **inj** and **prj** can be reused to model effect constraints.

Due to the component wise combination of **Effects**, a proof that an **Effect** is an element of an effect stack implies that an operations from one of the two signatures is part of the corresponding signature of the combined effect.

$$\begin{aligned}
& \text{opsInj} : e \in \text{effs} \rightarrow \text{Ops } e \in \text{map}^L \text{Ops } \text{effs} \\
& \text{opsInj } (\text{here refl}) = \text{here refl} \\
& \text{opsInj } (\text{there } p) = \text{there } (\text{opsInj } p) \\
& \text{scpsInj} : e \in \text{effs} \rightarrow \text{Scps } e \in \text{map}^L \text{Scps } \text{effs} \\
& \text{scpsInj } (\text{here refl}) = \text{here refl} \\
& \text{scpsInj } (\text{there } p) = \text{there } (\text{scpsInj } p)
\end{aligned}$$

Using the above proofs we can implement smart constructors/inject functions for scoped and unscoped operations without requiring other evidence.

$$\begin{aligned}
& \text{Op} : \{ e \in \text{effs} \} \rightarrow \llbracket \text{Ops } e \rrbracket (\text{Prog effs } A) \rightarrow \text{Prog effs } A \\
& \text{Op } \llbracket p \rrbracket = \text{op} \circ \text{inj } (\text{opsInj } p) \\
& \text{Scp} : \{ e \in \text{effs} \} \rightarrow \llbracket \text{Scps } e \rrbracket (\text{Prog effs } (\text{Prog effs } A)) \rightarrow \text{Prog effs } A \\
& \text{Scp } \llbracket p \rrbracket = \text{scp} \circ \text{inj } (\text{scpsInj } p)
\end{aligned}$$

To escape the monad after interpreting all effects we again add the **run** handler.

$$\begin{aligned}
& \text{run} : \text{Prog } \llbracket \rrbracket A \rightarrow A \\
& \text{run } (\text{var } x) = x
\end{aligned}$$

## 5.4 Nondet

As first example we will implement the nondeterminism effect. In section 5.4.1 we will implement the example by Piróg et al. to demonstrate that the **fold** definition from section 5.2.1 is sufficient. Section 5.4.2 will present an idea for modular effects and handlers.



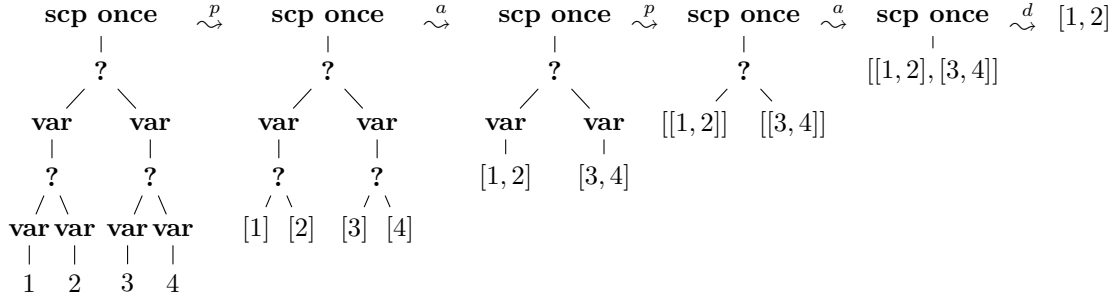


Figure 5.1: Interpretation of **once** (**var** 1 ? **var** 3)  $\gg \lambda x. \text{var } x ? \text{var } (x + 1)$

### 5.4.1 As Scoped Algebra

The signature for the two algebraic operations is the same as before. Furthermore we define a signature for the scoped operations **once**.

```
data Choices : Set where ???s : (Maybe CID) → Choices ; fails : Choices
data Onces : Set where onces : Onces
```

**Nondet<sup>P</sup>** corresponds to the data type from the example by Piróg et al. [Pir+18, sec. 6]. The effect has the unary, scoped operation **once** and the nullary and binary, algebraic operations **??** and **fail**.

```
NondetP : Effect
Ops NondetP = Choices ▷ λ{ (??? _ ) → Bool ; fails → ⊥ }
Scps NondetP = Onces ~> ⊤
```

A scoped algebra for an  $\mathbb{N}$  indexed carrier type  $C$  consists of three operations. **a** the *algebra* for the unscoped operations. **p** for *promoting* the carrier type when entering a scope. **d** for *demoting* the carrier type when leaving a scope and interpreting the syntax. Figure 5.4.1 demonstrates how the handler interprets **Nondet** syntax using the scoped algebra. It corresponds to an image for the other monad from “Syntax and Semantics for Operations with Scopes”, but represents programs using the **Prog** *effs* monad.

The indices for **d** and **a** are offset by one compared to the definition by Piróg et al. We won’t define our carrier data type in two stages as Piróg et al. but as an  $n$ -fold version of a simpler type. This change allows a simpler implementation using the **fold** from section 5.2.1, but should be insignificantly enough to present the similarities between the to recursion schemes.

```
record ScopedAlgebra (E : Effect) (C : ℕ → Set) : Set where
  constructor <_,_,_>
  field
    p : ∀ {n} → C n → C (1 + n)
    d : ∀ {n} → [ Scps E ] (C (2 + n)) → C (1 + n)
    a : ∀ {n} → [ Ops E ] (C (1 + n)) → C (1 + n)
  open ScopedAlgebra
```

Given a **ScopedAlgebra** for an **Effect** we can interpret its syntax. **fold<sup>P</sup>** corresponds to slightly modified version of the fold by Piróg et al. Their function works for an arbitrary  $n$  to allow recursion. Since, this recursion is abstracted in **fold** this is not needed. Furthermore they have to inject values explicitly into the carrier type. This happens implicitly due to the handling of the 0-th layer. Notice that the functions from the **ScopedAlgebra** correspond exactly to the ones expected by the **fold** from section 5.2.1. The values them self aren’t preprocessed and will just get promoted, hence **id** as passed as the first of the four functions.

```
foldP : ∀ {C : Set → ℕ → Set} → ScopedAlgebra e (C A) →
  Prog (e :: []) (C A 0) → C A 1
foldP {C = C} <p, d, a> = fold (C _ ) 1 id p
  (λ{ (inj1 s, κ) → a (s, κ) }) λ{ (inj1 s, κ) → d (s, κ) }
```

Just porting the algebra for **Nondet** by Piróg et al. yields a correct handler for the effect in isolation. The carrier type are iterated **Lists**.

The implementation of the scoped algebra is straight forward. The algebraic operations are handled as before and the promotion operation corresponds to the earlier handling of values. The demotion operation i.e. the handler for **once** has to produce an  $n$ -fold list, given an  $n + 1$ -fold list. Before applying the handler, the programs in the **var** nodes are the results for all possible continuations for the program in scope. The elements of the given list are the results of these programs. By acting just on the given list of lists the handler can separate between the results of the different branches in the scoped program.

```

NondetAlg : ScopedAlgebra NondetP (λ i → List ^ i $ A)
p NondetAlg = _ :: []
a NondetAlg (??s _, κ) = κ true ++ κ false
a NondetAlg (fails, κ) = []
d NondetAlg (onces, κ) with κ tt
... | [] = []
... | x :: _ = x

runNondetP : Prog (NondetP :: []) A → List A
runNondetP = foldP { C = λ A i → List ^ i $ A } NondetAlg

```

The carrier type can be thought of as the context for the computation. By having contexts of contexts it's possible to differentiate between the state of the computation in scope and the whole computation.

Lastly we will define a smartconstructor for the **once** operation. To capture the program  $p$  in scope, **pure** is mapped over it. The original program is now the outer **Prog** *effs* layer i.e. the first and second layers of the first term in figure 5.4.1. The original **var**  $x$  nodes are now **var**(**var**  $x$ ) nodes. Since  $\gg$  just effects the lowest layer it won't change the captured program and just act on it's results.

```

onceP : [ NondetP ∈ effs ] → Prog effs A → Prog effs A
onceP p = Scp (onces, λ _ → pure <$> p)

```

## 5.4.2 As Modular Handler

Piróg et al. just present handlers for single effects. This section presents an idea for adapting the handlers from the paper to modular ones.

As in the earlier chapters, when working with modular effects, the general approach is to execute the handlers for each effect one after another [Sch+19]. Each handler interprets the syntax for its effect and leaves the rest in place (or in case of non-orthogonal effects manipulates syntax of certain other effects). The carrier type for these handlers consists of the usual carrier type for these handlers, which is post composed with the type of the program without the interpreted syntax. For example, a handler for exceptions would produce values of type  $E \uplus A$ , therefore the modular handler produces value of type **Prog** *effs* ( $E \uplus A$ ).

In the context of scoped algebras, the  $\mathbb{N}$  indexed carrier type is usually the  $n$ -fold of some simpler type  $C$ . It seems reasonable to choose an  $n$ -fold of **Prog** *effs*  $\circ C$  as carrier type, because the structure of  $n$  layers of  $C$ s has to be preserved to reuse the non modular handler. Simply lifting the  $n$ -fold carrier type in the monad is not sufficient. The interleaved monad layers are needed to preserve non-interpreted syntax.

Consider the following implementation of modular handler for nondeterminism. This version of the nondeterminism effect does not support the **once** operation, because the semantics of the above definition is not the expected one when interacting with other effects. Similar to earlier chapter we introduce **patterns** to simplify the handler.

```

Nondet : Effect
Ops Nondet = Choices ▷ λ { (??s _) → Bool ; fails → ⊥ }
Scps Nondet = Void

pattern Other s κ = (inj2 s, κ)

```

```

pattern Choice cid  $\kappa$  = (inj1 (??s cid) ,  $\kappa$ )
pattern Fail          = (inj1 fails , _)

```

The new handler has the expected signature, which follows from the above described carrier type.

```

runNondet' : Prog (Nondet :: effs) A → Prog effs (Tree A)
runNondet' {effs} {A} = fold (λ i → (Prog effs ∘ Tree) ^ i $ A) 1 id

```

Values are now not only injected into the context, but also into the monad.

```
(pure ∘ leaf)
```

The algebraic operations are interpreted as before, except that all results are lifted into the monad. When an operation from a foreign effect is encountered the syntax is just reconstructed. The outer container coproduct is removed by interpreting the `Nondet` syntax, therefore `s` already has the correct type (note that `Other` hides the `inj2`). `κ` produces result for the positions of the given shape, because the recursion is handled by `fold`. Therefore the implementation is the same as in chapter 3 except that the recursion is hidden.

```

(λ where
  (Choice id  $\kappa$ ) → branch id <$>  $\kappa$  true <*>  $\kappa$  false
  Fail          → pure failed
  (Other s  $\kappa$ )  → op (s ,  $\kappa$ )

```

The interesting case is the one for scoped operations of foreign effects. Similar to the algebraic operations we have to reconstruct the scoped operation, but the position function has the wrong type. It produces values of type `Prog effs ∘ Tree ^ suc n $ A` but expected are values of type `Prog effs $ Prog effs ∘ Tree ^ n $ A`.

To remove the intermediate `Tree` layer we map the `functionhdl` over the result of the position function. `hdl` traverses the outer tree and recombines the inner trees under the monad i.e. by interleaving binds it orders the results. On a term level, we are given a list of possible continuations, which we execute on after another, appending their results.

```

) λ where
  (Other s  $\kappa$ ) → scp (s , λ p → hdl <$>  $\kappa$  p)
where
  hdl : ∀ {A} → Tree (Prog effs (Tree A)) → Prog effs (Tree A)
  hdl (branch cid l r) = branch cid <$> hdl l <*> hdl r
  hdl (leaf v)         = v -- no recursive call due to fold
  hdl failed           = var failed

```

In terms of Haskell typeclass the above implementation generalizes if `C` is a traversable monad, because `hdl` corresponds to `fmap join . sequence`. This is quite a strong condition, but it does not seem necessary, because we will see another example in section 5.6, which does not follow this pattern. Furthermore, the carrier types of effects are often simple data structures like products, coproducts, lists or trees, which are usually traversable and often monads. It's also unclear if a monad or just a notion of flattening is needed.

Notice that the `hdl` is similar to the handler function from chapter 4. Because the `fold` already interpreted parts of the program we do not call the handler recursively, but just join the results.

```

runNondet : Prog (Nondet :: effs) A → Prog effs (List A)
runNondet p = dfs empty <$> runNondet' p

```

```

fail : { Nondet ∈ effs } → Prog effs A
fail = Op (fails , λ())

```

```

_??_ : { Nondet ∈ effs } → Prog effs A → Prog effs A → Prog effs A
p ?? q = Op (??s nothing , (if_then p else q))

```

## 5.5 Exceptions

As our first example for a scoped effect in the modular setting we will take a look at exceptions. The syntax for `throw` is the same as before. Similar to chapter 4 `catch` has two sub-computations, the program in scope and the handler. The boilerplate code for the syntax is given below.

```

data Throws (E : Set) : Set where throws : (e : E) → Throws E
data Catchs : Set where catchs : Catchs
data CatchP (E : Set) : Set where
  mainP : CatchP E
  handleP : (e : E) → CatchP E

Exc : Set → Effect
Ops (Exc E) = Throws E ∼ ⊥
Scps (Exc E) = Catchs ∼ CatchP E

pattern Throw e = (inj1 (throws e) , _)
pattern Catch κ = (inj1 catchs , κ)

```

The first part of the handler is the same as in the higher order setting. To interpret the scoped operation `catch` we first execute scoped program in the `mainP` position. It produces either an exception or the result for the rest of the program. In the later case we just return the result. Notice that the recursive call was taken care of by the `fold`. In the other case we obtain an exception  $e$  with which we can obtain the result of the continuation in the `handleP` position i.e. handle the exception. The result of the exception handler is again wrapped in `⊔`. We pass the result along by either unwrapping the program or re-injecting the exception in the program using `pure`. The same function is used to traverse foreign scopes. Again the function corresponds to the handler from chapter 4, but without the recursive call.

```

runExc : Prog (Exc E :: effs) A → Prog effs (E ⊔ A)
runExc {E} {effs} {A} = fold (λ i → (Prog effs ∘ (E ⊔ _)) ^ i $ A) 1 id
  (pure ∘ inj2)
  ( λ where
    (Throw e) → pure (inj1 e)
    (Other s κ) → op (s , κ)
  ) λ where
    (Catch κ) → κ mainP ⋈ λ where
      (inj1 e) → κ (handleP e) ⋈ [ pure ∘ inj1 , id ]
      (inj2 x) → x
    (Other s κ) → scp (s , λ p → [ pure ∘ inj1 , id ] <$> κ p)

```

The smart constructors for the operations follow the known pattern.

```

throw : [ Exc E ∈ effs ] → E → Prog effs A
throw e = Op (throws e , λ())

_catch_ : [ Exc E ∈ effs ] → Prog effs A → (E → Prog effs A) → Prog effs A
p catch h = Scp $ catchs , λ where
  mainP → pure <$> p
  (handleP e) → pure <$> h e

```

## 5.6 State

To implement the sharing effect as described by Bunkenburg we also need to implement the `State` effect. The syntax is the same as before.

```

data States (S : Set) : Set where
  puts : (s : S) → States S
  gets : States S

```

```

State : Set → Effect
Ops (State S) = States S ▷ λ{ (puts s) → ⊤ ; gets → S }
Scps (State S) = Void

pattern Get κ = (inj1 gets , κ)
pattern Put s1 κ = (inj1 (puts s1) , κ)

```

When traversing a foreign scope we have to eliminate the intermediate context.  $\kappa$  produces a value of type  $\text{Prog } \text{effs} (S \times (S \rightarrow \text{Prog } \text{effs} \dots))$ . The lifted pair consists of the final state of the program in scope and the function mapping an initial state to the result of the corresponding result of the continuation. To remove the inner context we simply pass the state along, by applying the function to the given state using `eval`.

```

runState : Prog (State S :: effs) A → S → Prog effs (S × A)
runState {S} {effs} {A} = fold (λ i → (λ X → S → Prog effs (S × X)) ^ i $ A) 1 id
  (λ x s0 → pure (s0 , x))
  (λ where
    (Put s1 κ) _ → κ tt s1
    (Get κ) s0 → κ s0 s0
    (Other s κ) s0 → op (s , λ p → κ p s0)
  ) λ where
    (Other s κ) s0 → scp (s , λ p → eval <$> κ p s0)
  where
    eval : ∀ {A B} → A × (A → B) → B
    eval (a , f) = f a

evalState : Prog (State S :: effs) A → S → Prog effs A
evalState s0 p = π2 <$> runState s0 p

```

The operations are just the usual generic operations for the effect.

```

get : { S | State S ∈ effs } → Prog effs S
get = Op (gets , pure)

put : { S | State S ∈ effs } → S → Prog effs ⊤
put s = Op (puts s , pure)

```

## 5.7 Share

Lastly we will implement the sharing effect. The signature contains just the single, unary, scoped operation, `share` which creates new sharing scope.

```

data Shares : Set where shares : SID → Shares

Share : Effect
Ops Share = Void
Scps Share = Shares ~> ⊤

pattern ShareScp sid κ = (inj1 (shares sid) , κ)

```

In the handler the passed along choice id is handled similar to the initial state in the `State` effect. It's part of the iterated carrier type, which allows it to be changed between layers<sup>3</sup>. When handling a sharing scope the captured program is handled with the id of the stored in the shape of the scoping operation. The continuation is accessed via `>>=` and continuous with the outside i.e. the initial id. Scopes of foreign effects don't effect sharing. In contrast to `State`, the captured program does not influence the continuation, therefore both use the same, initial id.

<sup>3</sup>This is a general pattern with this approach. Handler arguments are turned into function arguments for the carrier type, because the recursion is done via `fold`. The same can be observed in a setting without algebraic effects and folding handlers [Sch+19].

```

runShare' : { Nondet ∈ effs } → Prog (Share :: effs) A → SID → ℕ → Prog effs A
runShare' { effs } { A } { p } = fold (λ i → ((λ X → SID → ℕ → Prog effs X) ^ i) A) 1 id
  (λ z _ → var z)
  (λ { (Other s pf) → case prj (opsInj p) (s, pf) of λ where
    nothing      sid n → op (s, λ p → pf p sid n)
    (just (fails , κ)) sid n → fail
    (just (??s _ , κ)) sid n → Op (??s (just (sid, n)) , λ p → κ p sid (suc n))
  }) λ where
  (ShareScp sid' κ) sid n → κ tt sid' 0 >> λ r → r sid n
  (Other s κ) sid n → scp (s, λ p → (λ k → k sid n) <> κ p sid n)

runShare : { Nondet ∈ effs } → Prog (Share :: effs) A → Prog effs A
runShare p = runShare' p (0, 0) 0

```

For simplicity the handler is initial invoked with choice id (0,0,0). This should not be a problem if the numbering of scopes starts with a higher ID, because after calling the **Share** handler no scopes are duplicated. If such a situation should arise the ID passed around by the handler can simply be made optional via **Maybe**, allowing no IDs for the outside choices.

The **Shareable** and **Normalform** infrastructure from chapter 3 can be reused to define the **Ágda** operator.

The program in the scope is again captured by mapping **pure** over it. The construction of scope ids follow again the implementation by Bunkenburg.

```

share⟨_⟩ : { Share ∈ effs } → SID → Prog effs A → Prog effs A
share⟨_⟩ { Scps } { Ops } sid p = Scp (shares sid , λ _ → pure <> p)

share : { State SID ∈ effs } → { Share ∈ effs } → { Shareable effs A } →
  Prog effs A → Prog effs (Prog effs A)
share { Ops } { Scps } p = do
  (i, j) ← get
  put (i + 1, j)
  let p' = do
    put (i, j + 1)
    x ← p
    x' ← shareArgs x
    put (i + 1, j)
    pure x'
  pure $ share⟨ i, j ⟩ p'

```

Using **Nondet**, **State** and **Share** we can again simulate call-time choice semantics. As expected, doubling a shared coin yields the results 0 and 2.

```

runCTC : { Normalform (State SID :: Share :: Nondet :: []) A B } →
  Prog (State SID :: Share :: Nondet :: []) A → List B
runCTC p = run $ runNondet $ runShare $ evalState (! p) (1, 1)

coin : { Nondet ∈ effs } → Prog effs ℕ
coin = pure 0 ?? pure 1

doubleCoin : { Nondet ∈ effs } → { Share ∈ effs } → { State SID ∈ effs } →
  Prog effs ℕ
doubleCoin = do c ← share coin
  ( c + c )

runDoubleCoin : runCTC doubleCoin ≡ 0 :: 2 :: []
runDoubleCoin = refl

```

In contrast to chapter 4 this approach can also model deep effects without involving universe levels. The definition of an effectful list as well as its typeclass instances from chapter 3 can be reused.

```

doubleHead : { Nondet ∈ effs } → { Share ∈ effs } → { State SID ∈ effs } →
  Prog effs ℕ

```

```

doubleHead = do  $mxs \leftarrow \text{share}$  (coin ::M []M)
               ( $\mid$  headM  $mxs$  + headM  $mxs$   $\mid$ )

runDoubleHead : runCTC doubleHead  $\equiv$  0 :: 2 :: []
runDoubleHead = refl

```

## Chapter 6

# Conclusion

### 6.1 Summary



# Bibliography

- [AAG03] Michael Gordon Abbott, Thorsten Altenkirch, and Neil Ghani. “Categories of Containers”. In: *Foundations of Software Science and Computational Structures, 6th International Conference, FOSSACS 2003 Held as Part of the Joint European Conference on Theory and Practice of Software, ETAPS 2003, Warsaw, Poland, April 7-11, 2003, Proceedings*. Ed. by Andrew D. Gordon. Vol. 2620. Lecture Notes in Computer Science. Springer, 2003, pp. 23–38. DOI: 10.1007/3-540-36576-1\_2. URL: [https://doi.org/10.1007/3-540-36576-1\\_2](https://doi.org/10.1007/3-540-36576-1_2).
- [Abe+05] Andreas Abel et al. “Verifying haskell programs using constructive type theory”. In: *Proceedings of the ACM SIGPLAN Workshop on Haskell, Haskell 2005, Tallinn, Estonia, September 30, 2005*. Ed. by Daan Leijen. ACM, 2005, pp. 62–73. DOI: 10.1145/1088348.1088355. URL: <https://doi.org/10.1145/1088348.1088355>.
- [Alt+15] Thorsten Altenkirch et al. “Indexed containers”. In: *J. Funct. Program.* 25 (2015). DOI: 10.1017/S095679681500009X. URL: <https://doi.org/10.1017/S095679681500009X>.
- [Bau18] Andrej Bauer. “What is algebraic about algebraic effects and handlers?”. In: *CoRR* abs/1807.05923 (2018). arXiv: 1807.05923. URL: <http://arxiv.org/abs/1807.05923>.
- [BM98] Richard S. Bird and Lambert G. L. T. Meertens. “Nested Datatypes”. In: *Mathematics of Program Construction, MPC’98, Marstrand, Sweden, June 15-17, 1998, Proceedings*. Ed. by Johan Jeuring. Vol. 1422. Lecture Notes in Computer Science. Springer, 1998, pp. 52–67. DOI: 10.1007/BFb0054285. URL: <https://doi.org/10.1007/BFb0054285>.
- [Bra13] Edwin C. Brady. “Programming and reasoning with algebraic effects and dependent types”. In: *ACM SIGPLAN International Conference on Functional Programming, ICFP’13, Boston, MA, USA - September 25 - 27, 2013*. Ed. by Greg Morrisett and Tarmo Uustalu. ACM, 2013, pp. 133–144. DOI: 10.1145/2500365.2500581. URL: <https://doi.org/10.1145/2500365.2500581>.
- [Bun19] Niels Bunkenburg. “Modeling Call-Time Choice as Effect using Scoped Free Monads”. MA thesis. Germany: Kiel University, 2019.
- [CDB19] Jan Christiansen, Sandra Dylus, and Niels Bunkenburg. “Verifying effectful Haskell programs in Coq”. In: *Proceedings of the 12th ACM SIGPLAN International Symposium on Haskell, Haskell@ICFP 2019, Berlin, Germany, August 18-23, 2019*. Ed. by Richard A. Eisenberg. ACM, 2019, pp. 125–138. DOI: 10.1145/3331545.3342592. URL: <https://doi.org/10.1145/3331545.3342592>.
- [DCT19] Sandra Dylus, Jan Christiansen, and Finn Teegen. “One Monad to Prove Them All”. In: *Art Sci. Eng. Program.* 3.3 (2019), p. 8. DOI: 10.22152/programming-journal.org/2019/3/8. URL: <https://doi.org/10.22152/programming-journal.org/2019/3/8>.
- [FKS09] Sebastian Fischer, Oleg Kiselyov, and Chung-chieh Shan. “Purely functional lazy non-deterministic programming”. In: *Proceeding of the 14th ACM SIGPLAN international conference on Functional programming, ICFP 2009, Edinburgh, Scotland, UK, August 31 - September 2, 2009*. Ed. by Graham Hutton and Andrew P. Tolmach. ACM, 2009, pp. 11–22. DOI: 10.1145/1596550.1596556. URL: <https://doi.org/10.1145/1596550.1596556>.
- [FS18] Peng Fu and Peter Selinger. “Dependently Typed Folds for Nested Data Types”. In: *CoRR* abs/1806.05230 (2018). arXiv: 1806.05230. URL: <http://arxiv.org/abs/1806.05230>.

- [HKM95] Michael Hanus, Herbert Kuchen, and Juan José Moreno-Navarro. *Curry: A Truly Functional Logic Language*. 1995.
- [Nor07] Ulf Norell. “Towards a practical programming language based on dependent type theory”. PhD thesis. SE-412 96 Göteborg, Sweden: Department of Computer Science and Engineering, Chalmers University of Technology, Sept. 2007.
- [Pir+18] Maciej Piróg et al. “Syntax and Semantics for Operations with Scopes”. In: *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*. Ed. by Anuj Dawar and Erich Grädel. ACM, 2018, pp. 809–818. DOI: 10.1145/3209108.3209166. URL: <https://doi.org/10.1145/3209108.3209166>.
- [PP02] Gordon D. Plotkin and John Power. “Notions of Computation Determine Monads”. In: *Foundations of Software Science and Computation Structures, 5th International Conference, FOSSACS 2002. Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2002 Grenoble, France, April 8-12, 2002, Proceedings*. Ed. by Mogens Nielsen and Uffe Engberg. Vol. 2303. Lecture Notes in Computer Science. Springer, 2002, pp. 342–356. DOI: 10.1007/3-540-45931-6\\_24. URL: [https://doi.org/10.1007/3-540-45931-6%5C\\_24](https://doi.org/10.1007/3-540-45931-6%5C_24).
- [PP09] Gordon D. Plotkin and Matija Pretnar. “Handlers of Algebraic Effects”. In: *Programming Languages and Systems, 18th European Symposium on Programming, ESOP 2009, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2009, York, UK, March 22-29, 2009. Proceedings*. Ed. by Giuseppe Castagna. Vol. 5502. Lecture Notes in Computer Science. Springer, 2009, pp. 80–94. DOI: 10.1007/978-3-642-00590-9\\_7. URL: [https://doi.org/10.1007/978-3-642-00590-9%5C\\_7](https://doi.org/10.1007/978-3-642-00590-9%5C_7).
- [Sch+19] Tom Schrijvers et al. “Monad transformers and modular algebraic effects: what binds them together”. In: *Proceedings of the 12th ACM SIGPLAN International Symposium on Haskell, Haskell@ICFP 2019, Berlin, Germany, August 18-23, 2019*. Ed. by Richard A. Eisenberg. ACM, 2019, pp. 98–113. DOI: 10.1145/3331545.3342595. URL: <https://doi.org/10.1145/3331545.3342595>.
- [Swi08] Wouter Swierstra. “Data types à la carte”. In: *J. Funct. Program.* 18.4 (2008), pp. 423–436. DOI: 10.1017/S0956796808006758. URL: <https://doi.org/10.1017/S0956796808006758>.
- [Uni13] The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. Institute for Advanced Study: <https://homotopytypetheory.org/book>, 2013.
- [Wad15] Philip Wadler. “Propositions as types”. In: *Commun. ACM* 58.12 (2015), pp. 75–84. DOI: 10.1145/2699407. URL: <https://doi.org/10.1145/2699407>.
- [WSH14] Nicolas Wu, Tom Schrijvers, and Ralf Hinze. “Effect handlers in scope”. In: *Proceedings of the 2014 ACM SIGPLAN symposium on Haskell, Gothenburg, Sweden, September 4-5, 2014*. Ed. by Wouter Swierstra. ACM, 2014, pp. 1–12. DOI: 10.1145/2633357.2633358. URL: <https://doi.org/10.1145/2633357.2633358>.