



中央研究院
資訊科學研究所

Institute of Information Science, Academia Sinica • Taipei, Taiwan, ROC

TR-IIS-19-003

Calculating a backtracking algorithm:
an exercise in monadic program derivation

Shin-Cheng Mu



June 20, 2019

||

Technical Report No. TR-IIS-19-003

<http://www.iis.sinica.edu.tw/page/library/TechReport/tr2019/tr19.html>

Calculating a Backtracking Algorithm:

An Exercise in Monadic Program Derivation

SHIN-CHENG MU, Academia Sinica, Taiwan

Equational reasoning is among the most important tools that functional programming provides us. Curiously, relatively less attention has been paid to reasoning about monadic programs. In this report we derive a backtracking algorithm for problem specifications that use a monadic unfold to generate possible solutions, which are filtered using a *scanl*-like predicate. We develop theorems that convert a variation of *scanl* to a *foldr* that uses the state monad, as well as theorems constructing hylomorphism. The algorithm is used to solve the *n*-queens puzzle, our running example. The aim is to develop theorems and patterns useful for the derivation of monadic programs, focusing on the intricate interaction between state and non-determinism.

1 INTRODUCTION

Equational reasoning is among the many gifts that functional programming offers us. Functional programs preserve a rich set of mathematical properties, which not only helps to prove properties about programs in a relatively simple and elegant manner, but also aids the development of programs. One may refine a clear but inefficient specification, stepwise through equational reasoning, to an efficient program whose correctness may not be obvious without such a derivation.

It is misleading if one says that functional programming does not allow side effects. In fact, even a purely functional language may allow a variety of side effects – in a rigorous, mathematically manageable manner. Since the introduction of *monads* into the functional programming community [Moggi 1989; Wadler 1992], it has become the main framework in which effects are modelled. Various monads were developed for different effects, from general ones such as IO, state, non-determinism, exception, continuation, environment passing, to specific purposes such as parsing. Numerous research were also devoted to producing practical monadic programs.

It is also a wrong impression that impure programs are bound to be difficult to reason about. In fact, the laws of monads and their operators are sufficient to prove quite a number of useful properties about monadic programs. The validity of these properties, proved using only these laws, is independent from the particular implementation of the monad.

This report follows the trail of Hutton and Fulger [2008] and Gibbons and Hinze [2011], aiming to develop theorems and patterns that are useful for reasoning about monadic programs. We focus on two effects – non-determinism and state. In this report we consider problem specifications that use a monadic unfold to generate possible solutions, which are filtered using a *scanl*-like predicate. We develop theorems that convert a variation of *scanl* to a *foldr* that uses the state monad, as well as theorems constructing hylomorphism. The algorithm is used to solve the *n*-queens puzzle, our running example.

While the interaction between non-determinism and state is known to be intricate, when each non-deterministic branch has its own local state, we get a relatively well-behaved monad that provides a rich collection of properties to work with. The situation when the state is global and shared by all non-deterministic branches is much more complex, and is dealt with in a subsequent paper [Pauwels et al. 2019].

Author's address: Shin-Cheng Mu, Institute of Information Science, Academia Sinica, Taiwan, scm@iis.sinica.edu.tw.

2 MONAD AND EFFECT OPERATORS

A monad consists of a type constructor $m :: * \rightarrow *$ and two operators *return* and “bind” (\gg), often modelled by the following Haskell type class declaration:¹

```
class Monad m where
  return :: a -> m a
  (>>)   :: m a -> (a -> m b) -> m b .
```

They are supposed to satisfy the following *monad laws*:

$$\text{return } x \gg f = f \ x , \quad (1)$$

$$m \gg \text{return} = m , \quad (2)$$

$$(m \gg f) \gg g = m \gg (\lambda x \rightarrow f \ x \gg g) . \quad (3)$$

We also define $m_1 \gg m_2 = m_1 \gg \text{const } m_2$, which has type $(\gg) :: m \ a \rightarrow m \ b \rightarrow m \ b$. Kleisli composition, denoted by (\gg) , composes two monadic operations $a \rightarrow m \ b$ and $b \rightarrow m \ c$ into an operation $a \rightarrow m \ c$. The operator $(\$)$ applies a pure function to a monad.

$$(\gg) :: \text{Monad } m \Rightarrow (a \rightarrow m \ b) \rightarrow (b \rightarrow m \ c) \rightarrow a \rightarrow m \ c$$

$$(f \gg g) \ x = f \ x \gg g ,$$

$$(\$) :: \text{Monad } m \Rightarrow (a \rightarrow b) \rightarrow m \ a \rightarrow m \ b$$

$$f \ \$ \ n = n \gg (\text{return} \cdot f) .$$

The following properties can be proved from their definitions and the monad laws:

$$(f \cdot g) \ \$ \ m = f \ \$ \ (g \ \$ \ m) , \quad (4)$$

$$(f \ \$ \ m) \gg g = m \gg (g \cdot f) , \quad (5)$$

$$f \ \$ \ (m \gg k) = m \gg (\lambda x \rightarrow f \ \$ \ k \ x) , \ x \text{ not free in } f . \quad (6)$$

Effect and Effect Operators. Monads are used to model effects, and each effect comes with its collection of operators. For example, to model non-determinism we assume two operators \emptyset and (\square) , respectively modeling failure and choice. A state effect comes with operators *get* and *put*, which respectively reads from and writes to an unnamed state variable.

A program may involve more than one effect. In Haskell, the type class constraint `MonadPlus` in the type of a program denotes that the program may use \emptyset or (\square) , and possibly other effects, while `MonadState s` denotes that it may use *get* and *put*. Some theorems in this report, however, apply only to programs that, for example, use non-determinism and *no other effects*. In such cases we will note in text that the theorem applies only to programs “whose only effect is non-determinism.” The set of effects a program uses can always be statically inferred by syntax.

Total, Finite Programs. Like in other literature on program derivation, we assume a set-theoretic semantics in which functions are total. We thus have the following laws regarding branching:

$$f \ (\text{if } p \ \text{then } e_1 \ \text{else } e_2) = \text{if } p \ \text{then } f \ e_1 \ \text{else } f \ e_2 , \quad (7)$$

$$\text{if } p \ \text{then } (\lambda x \rightarrow e_1) \ \text{else } (\lambda x \rightarrow e_2) = \lambda x \rightarrow \text{if } p \ \text{then } e_1 \ \text{else } e_2 . \quad (8)$$

¹ This report uses type classes to be explicit about the effects a program uses. For example, programs using non-determinism are labelled with constraint `MonadPlus m`. The style of reasoning proposed in this report is not tied to type classes or Haskell, and we do not strictly follow the particularities of type classes in the current Haskell standard. For example, we overlook the particularities that a `Monad` must also be `Applicative`, `MonadPlus` be `Alternative`, and that functional dependency is needed in a number of places in this report.

Lists in this report are inductive types, and unfolds generate finite lists too. Non-deterministic choices are finitely branching. Given a concrete input, a function always expands to a finitely-sized expression consisting of syntax allowed by its type. We may therefore prove properties of a monadic program by structural induction over its syntax.

3 EXAMPLE: THE n -QUEENS PROBLEM

Reasoning about monadic programs gets more interesting when more than one effect is involved. Backtracking algorithms make good examples of programs that are stateful and non-deterministic, and the n -queens problem, also dealt with by Gibbons and Hinze [2011], is among the most well-known examples of backtracking.²

In this section we present a specification of the problem, before transforming it into the form $\text{unfoldM } p f \gg \text{filt } (\text{all ok} \cdot \text{scanl}_+ (\oplus) st)$ (whose components will be defined later), which is the general form of problems we will deal with in this report.

3.1 Non-Determinism

Since the n -queens problem will be specified by a non-deterministic program, we discuss non-determinism before presenting the specification. We assume two operators \emptyset and (\parallel) :

```
class Monad m => MonadPlus m where
   $\emptyset$  :: m a
   $(\parallel)$  :: m a → m a → m a .
```

The former denotes failure, while $m \parallel n$ denotes that the computation may yield either m or n . What laws they should satisfy, however, can be a tricky issue. As discussed by Kiselyov [2015], it eventually comes down to what we use the monad for. It is usually expected that (\parallel) and \emptyset form a monoid. That is, (\parallel) is associative, with \emptyset as its zero:

$$(m \parallel n) \parallel k = m \parallel (n \parallel k), \quad (9)$$

$$\emptyset \parallel m = m = m \parallel \emptyset. \quad (10)$$

It is also assumed that monadic bind distributes into (\parallel) from the end, while \emptyset is a left zero for (\gg) :

$$\text{left-distributivity} : (m_1 \parallel m_2) \gg f = (m_1 \gg f) \parallel (m_2 \gg f), \quad (11)$$

$$\text{left-zero} : \emptyset \gg f = \emptyset. \quad (12)$$

We will refer to the laws (9), (10), (11), (12) collectively as the *nondeterminism laws*. Other properties regarding \emptyset and (\parallel) will be introduced when needed.

The monadic function $\text{filt } p x$ returns x if $p x$ holds, and fails otherwise:

```
filt :: MonadPlus m => (a → Bool) → a → m a
filt p x = guard (p x) >> return x ,
```

where guard is a standard monadic function defined by:

```
guard :: MonadPlus m => Bool → m ()
guard b = if b then return () else  $\emptyset$  .
```

The following properties allow us to move guard around. Their proofs are given in Appendix A.

$$\text{guard } (p \wedge q) = \text{guard } p \gg \text{guard } q, \quad (13)$$

$$\text{guard } p \gg (f \$ m) = f \$ (\text{guard } p \gg m). \quad (14)$$

²Curiously, Gibbons and Hinze [2011] did not finish their derivation and stopped at a program that exhaustively generates all permutations and tests each of them. Perhaps it was sufficient to demonstrate their point.

<table style="width: 100%; border-collapse: collapse;"> <tr><td></td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr> <tr><td>0</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>Q</td><td>.</td><td>.</td></tr> <tr><td>1</td><td>.</td><td>.</td><td>Q</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td></tr> <tr><td>2</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>Q</td><td>.</td><td>.</td></tr> <tr><td>3</td><td>Q</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td></tr> <tr><td>4</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>Q</td><td>.</td></tr> <tr><td>5</td><td>.</td><td>Q</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td></tr> <tr><td>6</td><td>.</td><td>.</td><td>.</td><td>.</td><td>Q</td><td>.</td><td>.</td><td>.</td></tr> <tr><td>7</td><td>.</td><td>.</td><td>Q</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td></tr> </table> <p style="text-align: center;">(a)</p>		0	1	2	3	4	5	6	7	0	Q	.	.	1	.	.	Q	2	Q	.	.	3	Q	4	Q	.	5	.	Q	6	Q	.	.	.	7	.	.	Q	<table style="width: 100%; border-collapse: collapse;"> <tr><td></td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr> <tr><td>0</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>.</td><td>.</td><td>.</td></tr> <tr><td>1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>.</td><td>.</td><td>.</td><td>.</td></tr> <tr><td>2</td><td>2</td><td>3</td><td>4</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td></tr> <tr><td>3</td><td>3</td><td>4</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td></tr> <tr><td>4</td><td>4</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td></tr> <tr><td>5</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>12</td><td>.</td></tr> <tr><td>6</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>12</td><td>13</td></tr> <tr><td>7</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>12</td><td>13</td><td>14</td></tr> </table> <p style="text-align: center;">(b)</p>		0	1	2	3	4	5	6	7	0	0	1	2	3	4	.	.	.	1	1	2	3	4	2	2	3	4	3	3	4	4	4	5	12	.	6	12	13	7	12	13	14	<table style="width: 100%; border-collapse: collapse;"> <tr><td></td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr> <tr><td>0</td><td>0</td><td>-1</td><td>.</td><td>.</td><td>.</td><td>-5</td><td>-6</td><td>-7</td></tr> <tr><td>1</td><td>.</td><td>0</td><td>-1</td><td>.</td><td>.</td><td>.</td><td>-5</td><td>-6</td></tr> <tr><td>2</td><td>.</td><td>.</td><td>0</td><td>-1</td><td>.</td><td>.</td><td>.</td><td>-5</td></tr> <tr><td>3</td><td>.</td><td>.</td><td>.</td><td>0</td><td>.</td><td>.</td><td>.</td><td>.</td></tr> <tr><td>4</td><td>.</td><td>.</td><td>.</td><td>.</td><td>0</td><td>.</td><td>.</td><td>.</td></tr> <tr><td>5</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>0</td><td>.</td><td>.</td></tr> <tr><td>6</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>0</td><td>.</td></tr> <tr><td>7</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>.</td><td>0</td></tr> </table> <p style="text-align: center;">(c)</p>		0	1	2	3	4	5	6	7	0	0	-1	.	.	.	-5	-6	-7	1	.	0	-1	.	.	.	-5	-6	2	.	.	0	-1	.	.	.	-5	3	.	.	.	0	4	0	.	.	.	5	0	.	.	6	0	.	7	0
	0	1	2	3	4	5	6	7																																																																																																																																																																																																																																													
0	Q	.	.																																																																																																																																																																																																																																													
1	.	.	Q																																																																																																																																																																																																																																													
2	Q	.	.																																																																																																																																																																																																																																													
3	Q																																																																																																																																																																																																																																													
4	Q	.																																																																																																																																																																																																																																													
5	.	Q																																																																																																																																																																																																																																													
6	Q	.	.	.																																																																																																																																																																																																																																													
7	.	.	Q																																																																																																																																																																																																																																													
	0	1	2	3	4	5	6	7																																																																																																																																																																																																																																													
0	0	1	2	3	4	.	.	.																																																																																																																																																																																																																																													
1	1	2	3	4																																																																																																																																																																																																																																													
2	2	3	4																																																																																																																																																																																																																																													
3	3	4																																																																																																																																																																																																																																													
4	4																																																																																																																																																																																																																																													
5	12	.																																																																																																																																																																																																																																													
6	12	13																																																																																																																																																																																																																																													
7	12	13	14																																																																																																																																																																																																																																													
	0	1	2	3	4	5	6	7																																																																																																																																																																																																																																													
0	0	-1	.	.	.	-5	-6	-7																																																																																																																																																																																																																																													
1	.	0	-1	.	.	.	-5	-6																																																																																																																																																																																																																																													
2	.	.	0	-1	.	.	.	-5																																																																																																																																																																																																																																													
3	.	.	.	0																																																																																																																																																																																																																																													
4	0	.	.	.																																																																																																																																																																																																																																													
5	0	.	.																																																																																																																																																																																																																																													
6	0	.																																																																																																																																																																																																																																													
7	0																																																																																																																																																																																																																																													

Fig. 1. (a) This placement can be represented by $[3, 5, 7, 1, 6, 0, 2, 4]$. (b) Up diagonals. (c) Down diagonals.

$$\text{guard } p \gg m = m \gg (\lambda x \rightarrow \text{guard } p \gg \text{return } x), \text{ if } m \gg \emptyset = \emptyset. \quad (15)$$

3.2 Specification

The aim of the puzzle is to place n queens on a n by n chess board such that no two queens can attack each other. Given n , we number the rows and columns by $[0..n-1]$. Since all queens should be placed on distinct rows and distinct columns, a potential solution can be represented by a permutation xs of the list $[0..n-1]$, such that $xs !! i = j$ denotes that the queen on the i th column is placed on the j th row (see Figure 1(a)). In this representation queens cannot be put on the same row or column, and the problem is reduced to filtering, among permutations of $[0..n-1]$, those placements in which no two queens are put on the same diagonal. The specification can be written as a non-deterministic program:

```
queens :: MonadPlus m => Int -> m [Int]
queens n = perm [0..n-1] >> filt safe,
```

where `perm` non-deterministically computes a permutation of its input, and the pure function `safe :: [Int] -> Bool` determines whether no queens are on the same diagonal.

This specification of `queens` generates all the permutations, before checking them one by one, in two separate phases. We wish to fuse the two phases and produce a faster implementation. The overall idea is to define `perm` in terms of an unfold, transform `filt safe` into a fold, and fuse the two phases into a *hylomorphism* [Meijer et al. 1991]. During the fusion, some non-safe choices can be pruned off earlier, speeding up the computation.

Permutation. The monadic function `perm` can be written both as a fold or an unfold. For this problem we choose the latter. The function `select` non-deterministically splits a list into a pair containing one chosen element and the rest:

```
select :: MonadPlus m => [a] -> m (a, [a]) .
select [] = 0
select (x : xs) = return (x, xs) || ((id × (x:)) $ select xs),
```

where $(f \times g) (x, y) = (f x, g y)$. For example, `select [1, 2, 3]` yields one of $(1, [2, 3])$, $(2, [1, 3])$ and $(3, [1, 2])$. The function call `unfoldM p f y` generates a list $[a]$ from a seed $y :: b$. If $p y$ holds, the generation stops. Otherwise an element and a new seed is generated using f . It is like the usual `unfoldr` apart from that f , and thus the result, is monadic:

```
unfoldM :: Monad m => (b -> Bool) -> (b -> m (a, b)) -> b -> m [a]
unfoldM p f y | p y = return []
                | otherwise = f y >> λ(x, z) -> (x:) $ unfoldM p f z .
```

Given these definitions, *perm* can be defined by:

```
perm :: MonadPlus m => [a] -> m [a]
perm = unfoldM null select .
```

3.3 Safety Check in a *scanl*

We have yet to define *safe*. Representing a placement as a permutation allows an easy way to check whether two queens are put on the same diagonal. An 8 by 8 chess board has 15 *up diagonals* (those running between bottom-left and top-right). Let them be indexed by $[0..14]$ (see Figure 1(b)). If we apply *zipWith (+) [0..]* to a permutation, we get the indices of the up-diagonals where the chess pieces are placed. Similarly, there are 15 *down diagonals* (those running between top-left and bottom right). By applying *zipWith (-) [0..]* to a permutation, we get the indices of their down-diagonals (indexed by $[-7..7]$). See Figure 1(c). A placement is safe if the diagonals contain no duplicates:

```
ups, downs :: [Int] -> [Int]
ups  xs = zipWith (+) [0..] xs ,
downs xs = zipWith (-) [0..] xs ,
safe  :: [Int] -> Bool
safe xs = nodup (ups xs) ^& nodup (downs xs) ,
```

where *nodup* :: Eq a => [a] -> Bool determines whether there is no duplication in a list.

The eventual goal is to transform *filt safe* into a *foldr*, to be fused with *perm*, an unfold that generates a list from left to right. In order to do so, it helps if *safe* can be expressed in a computation that processes the list left-to-right, that is, a *foldl* or a *scanl*. To derive such a definition we use the standard trick – introducing accumulating parameters, and generalising *safe* to *safeAcc* below:

```
safeAcc :: (Int, [Int], [Int]) -> [Int] -> Bool
safeAcc (i, us, ds) xs = nodup us' ^& nodup ds' ^&
  all (notin us) us' ^& all (notin ds) ds' ,
  where us' = zipWith (+) [i..] xs
        ds' = zipWith (-) [i..] xs .
```

It is a generalisation because *safe* = *safeAcc* (0, [], []). By plain functional calculation, one may conclude that *safeAcc* can be defined using a variation of *scanl*:

```
safeAcc (i, us, ds) = all ok · scanl+ (⊕) (i, us, ds) ,
  where (i, us, ds) ⊕ x = (i + 1, (i + x : us), (i - x : ds))
        ok (i, (x : us), (y : ds)) = xnotin us ^& ynotin ds ,
```

where *all p* = *foldr* (∧) True · *map p* and *scanl+* is like the standard *scanl*, but applies *foldl* to all non-empty prefixes of a list. It can be specified by:

```
scanl+ :: (b -> a -> b) -> b -> [a] -> [b]
scanl+ (⊕) st = tail · scanl (⊕) st ,
```

and it also adopts an inductive definition:

```
scanl+ (⊕) st []      = []
scanl+ (⊕) st (x : xs) = (st ⊕ x) : scanl+ (⊕) (st ⊕ x) xs .
```

Operationally, *safeAcc* examines the list from left to right, while keeping a state (i, us, ds) , where *i* is the current position being examined, while *us* and *ds* are respectively indices of all the up and

down diagonals encountered so far. Indeed, in a function call $\text{scanl}_+ (\oplus) st$, the value st can be seen as a “state” that is explicitly carried around. This naturally leads to the idea: can we convert a scanl_+ to a monadic program that stores st in its state? This is the goal of the next section.

As a summary of this section, after defining *queens*, we have transformed it into the following form:

$$\text{unfoldM } p f \gg \text{filt } (\text{all } ok \cdot \text{scanl}_+ (\oplus) st) .$$

This is the form of problems we will consider for the rest of this report: problems whose solutions are generated by an monadic unfold, before being filtered by an *filt* that takes the result of a scanl_+ .

4 FROM PURE TO STATEFUL scanl

The aim of this section is to turn the filtering phase $\text{filt } (\text{all } ok \cdot \text{scanl}_+ (\oplus) st)$ into a *foldr*. For that we introduce a state monad to pass the state around.

The state effect provides two operators:

```
class Monad m => MonadState s m where
  get :: m s
  put :: s -> m () ,
```

where *get* retrieves the state, while *put* overwrites the state by the given value. They are supposed to satisfy the *state laws*:

$$\text{put-put} : \quad \text{put } st \gg \text{put } st' = \text{put } st' , \quad (16)$$

$$\text{put-get} : \quad \text{put } st \gg \text{get} = \text{put } st \gg \text{return } st , \quad (17)$$

$$\text{get-put} : \quad \text{get} \gg \text{put} = \text{return } () , \quad (18)$$

$$\text{get-get} : \quad \text{get} \gg (\lambda st \rightarrow \text{get} \gg k st) = \text{get} \gg (\lambda st \rightarrow k st) . \quad (19)$$

4.1 From scanl_+ to monadic *foldr*

Consider the following monadic variation of scanl :

```
scanlM :: MonadState s m => (s -> a -> s) -> s -> [a] -> m [s]
scanlM (\oplus) st xs = put st >> foldr (\otimes) (return []) xs
  where x \otimes n = get >> \lambda st -> let st' = st \oplus x
    in (st') :$ (put st' >> n) .
```

It behaves like scanl_+ , but stores the accumulated information in a monadic state, which is retrieved and stored in each step. The main body of the computation is implemented using a *foldr*.

To relate scanl_+ and scanlM , one would like to have $\text{return } (\text{scanl}_+ (\oplus) st xs) = \text{scanlM } (\oplus) st xs$. However, the lefthand side does not alter the state, while the righthand side does. One of the ways to make the equality hold is to manually backup and restore the state. Define

```
protect :: MonadState s m => m b -> m b
protect n = get >> \lambda ini -> n >> \lambda x -> put ini >> return x ,
```

We have

THEOREM 4.1. *For all $(\oplus) :: (s \rightarrow a \rightarrow s)$, $st :: s$, and $xs :: [a]$,*

$$\text{return } (\text{scanl}_+ (\oplus) st xs) = \text{protect } (\text{scanlM } (\oplus) st xs) .$$

PROOF. By induction on xs . We present the case $xs := x : xs$.

$$\begin{aligned}
& \text{protect } (\text{scanlM } (\oplus) \text{ st } (x : xs)) \\
= & \{ \text{expanding definitions, let } st' = st \oplus x \} \\
& \text{get } \approx \lambda ini \rightarrow \text{put } st \gg \text{get } \approx \lambda st \rightarrow \\
& ((st') : \$) (\text{put } st' \gg \text{foldr } (\otimes) (\text{return } []) xs) \approx \lambda r \rightarrow \\
& \text{put } ini \gg \text{return } r \\
= & \{ \text{by put-get (17)} \} \\
& \text{get } \approx \lambda ini \rightarrow \text{put } st \gg \\
& ((st') : \$) (\text{put } st' \gg \text{foldr } (\otimes) (\text{return } []) xs) \approx \lambda r \rightarrow \\
& \text{put } ini \gg \text{return } r \\
= & \{ \text{by (6)} \} \\
& (st') : \$ (\text{get } \approx \lambda ini \rightarrow \text{put } st \gg \text{put } st' \gg \\
& \quad \text{foldr } (\otimes) (\text{return } []) xs \approx \lambda r \rightarrow \\
& \quad \text{put } ini \gg \text{return } r) \\
= & \{ \text{by put-put (16)} \} \\
& (st') : \$ (\text{get } \approx \lambda ini \rightarrow \text{put } st' \gg \text{foldr } (\otimes) (\text{return } []) xs \\
& \quad \approx \lambda r \rightarrow \text{put } ini \gg \text{return } r) \\
= & \{ \text{definitions of scanlM and protect} \} \\
& (st') : \$ \text{protect } (\text{scanlM } (\oplus) st' xs) \\
= & \{ \text{induction} \} \\
& (st') : \$ \text{return } (\text{scanl}_+ (\oplus) st' xs) \\
= & \text{return } ((st \oplus x) : \text{scanl}_+ (\oplus) (st \oplus x) xs) \\
= & \text{return } (\text{scanl}_+ (\oplus) st (x : xs)) .
\end{aligned}$$

□

This proof is instructive due to the use of properties (16) and (17), and that (st') , being a pure function, can be easily moved around using (6).

We have learned that $\text{scanl}_+ (\oplus) st$ can be turned into $\text{scanlM } (\oplus) st$, defined in terms of a stateful *foldr*. In the definition, state is the only effect involved. The next task is to transform $\text{filt } (\text{scanl}_+ (\oplus) st)$ into a *foldr*. The operator *filt* is defined using non-determinism. Hence the transformation involves the interaction between two effects.

4.2 Right-Distributivity and Local State

We now digress a little to discuss one form of interaction between non-determinism and state. In this report, we wish that the following two additional properties are valid:

$$\text{right-distributivity} : m \approx (\lambda x \rightarrow f_1 x \parallel f_2 x) = (m \approx f_1) \parallel (m \approx f_2), \quad (20)$$

$$\text{right-zero} : m \gg \emptyset = \emptyset . \quad (21)$$

Note that the two properties hold for some monads with non-determinism, but not all. With some implementations of the monad, it is likely that in the lefthand side of (20), the effect of m happens once, while in the righthand side it happens twice. In (21), the m on the lefthand side may incur some effects that do not happen in the righthand side.

Having (20) and (21) leads to profound consequences on the semantics and implementation of monadic programs. To begin with, (20) implies that (\parallel) be commutative. To see that, let $m = m_1 \parallel m_2$ and $f_1 = f_2 = \text{return}$ in (20). Implementation of such non-deterministic monads have been studied by Kiselyov [2013].

When mixed with state, one consequence of (20) is that $get \gg (\lambda s \rightarrow f_1 s \parallel f_2 s) = (get \gg f_1 \parallel get \gg f_2)$. That is, f_1 and f_2 get the same state regardless of whether get is performed outside or inside the non-determinism branch. Similarly, (21) implies $put\ s \gg \emptyset = \emptyset$ – when a program fails, the changes it performed on the state can be discarded. These requirements imply that *each non-determinism branch has its own copy of the state*. Therefore, we will refer to (20) and (21) as *local state laws* in this report – even though they do not explicitly mention state operators at all!

One monad satisfying the local state laws is $M\ a = s \rightarrow [(a, s)]$, which is the same monad one gets by `StateT s (ListT Identity)` in the Monad Transformer Library [Gill and Kmett 2014]. With effect handling [Kiselyov and Ishii 2015; Wu et al. 2012], the monad meets the requirements if we run the handler for state before that for list.

The advantage of having the local state laws is that we get many useful properties, which make this stateful non-determinism monad preferred for program calculation and reasoning. Recall, for example, that (21) is the antecedent of (15). The result can be stronger: non-determinism commutes with all other effects if we have local state laws.

Definition 4.2. Let m and n be two monadic programs such that x does not occur free in m , and y does not occur free in n . We say m and n commute if

$$\begin{aligned} m \gg \lambda x \rightarrow n \gg \lambda y \rightarrow f\ x\ y &= \\ n \gg \lambda y \rightarrow m \gg \lambda x \rightarrow f\ x\ y. & \end{aligned} \quad (22)$$

We say that m commutes with effect δ if m commutes with any n whose only effects are δ , and that effects ϵ and δ commute if any m and n commute as long as their only effects are respectively ϵ and δ .

THEOREM 4.3. *If right-distributivity (20) and right-zero (21) hold in addition to the monad laws stated before, non-determinism commutes with any effect ϵ .*

PROOF. Let m be a monadic program whose only effect is non-determinism, and $stmt$ be any monadic program. The aim is to prove that m and $stmt$ commute. Induction on the structure of m .

CASE $m := return\ e$:

$$\begin{aligned} stmt \gg \lambda x \rightarrow return\ e \gg \lambda y \rightarrow f\ x\ y &= \\ = \{ \text{monad law (1)} \} & \\ stmt \gg \lambda x \rightarrow f\ x\ e &= \\ = \{ \text{monad law (1)} \} & \\ return\ e \gg \lambda y \rightarrow stmt \gg \lambda x \rightarrow f\ x\ y. & \end{aligned}$$

CASE $m := m_1 \parallel m_2$:

$$\begin{aligned} stmt \gg \lambda x \rightarrow (m_1 \parallel m_2) \gg \lambda y \rightarrow f\ x\ y &= \\ = \{ \text{by (11)} \} & \\ stmt \gg \lambda x \rightarrow (m_1 \gg f\ x) \parallel (m_2 \gg f\ x) &= \\ = \{ \text{by (20)} \} & \\ (stmt \gg \lambda x \rightarrow m_1 \gg f\ x) \parallel (stmt \gg \lambda x \rightarrow m_2 \gg f\ x) &= \\ = \{ \text{induction} \} & \\ (m_1 \gg \lambda y \rightarrow stmt \gg \lambda x \rightarrow f\ x\ y) \parallel (m_2 \gg \lambda y \rightarrow stmt \gg \lambda x \rightarrow f\ x\ y) &= \\ = \{ \text{by (11)} \} & \\ (m_1 \parallel m_2) \gg \lambda y \rightarrow stmt \gg \lambda x \rightarrow f\ x\ y. & \end{aligned}$$

CASE $m := \emptyset$:

$$\begin{aligned}
& stmt \gg \lambda x \rightarrow \emptyset \gg \lambda y \rightarrow f \ x \ y \\
= & \{ \text{by (12)} \} \\
& stmt \gg \lambda x \rightarrow \emptyset \\
= & \{ \text{by (21)} \} \\
& \emptyset \\
= & \{ \text{by (12)} \} \\
& \emptyset \gg \lambda y \rightarrow stmt \gg \lambda x \rightarrow f \ x \ y .
\end{aligned}$$

□

Note. We briefly justify proofs by induction on the syntax tree. Finite monadic programs can be represented by the free monad constructed out of *return* and the effect operators, which can be represented by an inductively defined data structure, and interpreted by effect handlers [Kiselyov and Ishii 2015; Kiselyov et al. 2013]. When we say two programs m_1 and m_2 are equal, we mean that they have the same denotation when interpreted by the effect handlers of the corresponding effects, for example, $hdNondet (hdState \ s \ m_1) = hdNondet (hdState \ s \ m_2)$, where *hdNondet* and *hdState* are respectively handlers for nondeterminism and state. Such equality can be proved by induction on some sub-expression in m_1 or m_2 , which are treated like any inductively defined data structure. A more complete treatment is a work in progress. (*End of Note*)

4.3 Filtering Using a Stateful, Non-Deterministic Fold

Having dealt with $scanl_+ (\oplus) \ st$ in Section 4.1, in this section we aim to turn a filter of the form $filt (all \ ok \cdot scanl_+ (\oplus) \ st)$ to a stateful and non-deterministic *foldr*.

We calculate, for all ok , (\oplus) , st , and xs :

$$\begin{aligned}
& filt (all \ ok \cdot scanl_+ (\oplus) \ st) \ xs \\
= & guard (all \ ok (scanl_+ (\oplus) \ st \ xs)) \gg return \ xs \\
= & return (scanl_+ (\oplus) \ st \ xs) \gg \lambda ys \rightarrow \\
& guard (all \ ok \ ys) \gg return \ xs \\
= & \{ \text{Theorem 4.1, definition of } protect, \text{ monad law} \} \\
& get \gg \lambda ini \rightarrow scanLM (\oplus) \ st \ xs \gg \lambda ys \rightarrow put \ ini \gg \\
& guard (all \ ok \ ys) \gg return \ xs \\
= & \{ \text{Theorem 4.3: non-determinism commutes with state} \} \\
& get \gg \lambda ini \rightarrow scanLM (\oplus) \ st \ xs \gg \lambda ys \rightarrow \\
& guard (all \ ok \ ys) \gg put \ ini \gg return \ xs \\
= & \{ \text{definition of } protect, \text{ monad laws} \} \\
& protect (scanLM (\oplus) \ st \ xs) \gg (guard \cdot all \ ok) \gg return \ xs .
\end{aligned}$$

Recall that $scanLM (\oplus) \ st \ xs = put \ st \gg foldr (\otimes) (return \ []) \ xs$. The following theorem fuses a monadic *foldr* with a *guard* that uses its result.

THEOREM 4.4. *Assume that state and non-determinism commute. Let (\otimes) be defined as that in $scanLM$ for any given $(\oplus) :: s \rightarrow a \rightarrow s$. We have that for all $ok :: s \rightarrow Bool$ and $xs :: [a]$:*

$$\begin{aligned}
& foldr (\otimes) (return \ []) \ xs \gg (guard \cdot all \ ok) \gg return \ xs = \\
& foldr (\odot) (return \ []) \ xs , \\
& \text{where } x \odot m = get \gg \lambda st \rightarrow guard (ok (st \oplus x)) \gg \\
& put (st \oplus x) \gg ((x:) \ \$) \ m .
\end{aligned}$$

PROOF. Unfortunately we cannot use a *foldr* fusion, since xs occurs free in $\lambda ys \rightarrow \text{guard } (all\ ok\ ys) \gg \text{return } xs$. Instead we use a simple induction on xs . For the case $xs := x : xs$:

$$\begin{aligned}
& (x \otimes \text{foldr } (\otimes) (\text{return } []) xs) \gg (\text{guard } \cdot \text{all ok}) \gg \text{return } (x : xs) \\
= & \{ \text{definition of } (\otimes) \} \\
& \text{get } \gg \lambda st \rightarrow \\
& (((st \oplus x):) \$ (\text{put } (st \oplus x) \gg \text{foldr } (\otimes) (\text{return } []) xs)) \gg \\
& (\text{guard } \cdot \text{all ok}) \gg \text{return } (x : xs) \\
= & \{ \text{monad laws, (5), and (6)} \} \\
& \text{get } \gg \lambda st \rightarrow \text{put } (st \oplus x) \gg \\
& \text{foldr } (\otimes) (\text{return } []) xs \gg \lambda ys \rightarrow \\
& \text{guard } (all\ ok\ (st \oplus x : ys)) \gg \text{return } (x : xs) \\
= & \{ \text{since } \text{guard } (p \wedge q) = \text{guard } q \gg \text{guard } p \} \\
& \text{get } \gg \lambda st \rightarrow \text{put } (st \oplus x) \gg \\
& \text{foldr } (\otimes) (\text{return } []) xs \gg \lambda ys \rightarrow \\
& \text{guard } (ok\ (st \oplus x)) \gg \text{guard } (all\ ok\ ys) \gg \\
& \text{return } (x : xs) \\
= & \{ \text{assumption: nondeterminism commutes with state} \} \\
& \text{get } \gg \lambda st \rightarrow \text{guard } (ok\ (st \oplus x)) \gg \text{put } (st \oplus x) \gg \\
& \text{foldr } (\otimes) (\text{return } []) xs \gg \lambda ys \rightarrow \\
& \text{guard } (all\ ok\ ys) \gg \text{return } (x : xs) \\
= & \{ \text{monad laws and definition of } (\$) \} \\
& \text{get } \gg \lambda st \rightarrow \text{guard } (ok\ (st \oplus x)) \gg \text{put } (st \oplus x) \gg \\
& (x:) \$ (\text{foldr } (\otimes) (\text{return } []) xs \gg \lambda ys \rightarrow \text{guard } (all\ ok\ ys) \gg \text{return } xs) \\
= & \{ \text{induction} \} \\
& \text{get } \gg \lambda st \rightarrow \text{guard } (ok\ (st \oplus x)) \gg \text{put } (st \oplus x) \gg \\
& (x:) \$ \text{foldr } (\odot) (\text{return } []) xs \\
= & \{ \text{definition of } (\odot) \} \\
& \text{foldr } (\odot) (\text{return } []) (x : xs) .
\end{aligned}$$

□

This proof is instructive due to extensive use of commutativity.

In summary, we now have this corollary performing $\text{filt } (all\ ok \cdot \text{scanl}_+ (\oplus) st)$ using a non-deterministic and stateful *foldr*:

COROLLARY 4.5. *Let (\odot) be defined as in Theorem 4.4. If state and non-determinism commute, we have:*

$$\begin{aligned}
& \text{filt } (all\ ok \cdot \text{scanl}_+ (\oplus) st) xs = \\
& \text{protect } (\text{put } st \gg \text{foldr } (\odot) (\text{return } []) xs) .
\end{aligned}$$

5 MONADIC HYLOMORPHISM

To recap what we have done, we started with a specification of the form $\text{unfoldM } p\ f\ z \gg \text{filt } (all\ ok \cdot \text{scanl}_+ (\oplus) st)$, where $f :: \text{MonadPlus } m \Rightarrow b \rightarrow m\ (a, b)$, and have shown that

$$\begin{aligned}
& \text{unfoldM } p\ f\ z \gg \text{filt } (all\ ok \cdot \text{scanl}_+ (\oplus) st) \\
= & \{ \text{Corollary 4.5, with } (\odot) \text{ defined as in Theorem 4.4} \} \\
& \text{unfoldM } p\ f\ z \gg \lambda xs \rightarrow \text{protect } (\text{put } st \gg \text{foldr } (\odot) (\text{return } []) xs)
\end{aligned}$$

$$= \{ \text{Theorem 4.3: nondeterminism commutes with state} \} \\ \text{protect } (\text{put } st \gg \text{unfoldM } p f z \gg \text{foldr } (\odot) (\text{return } [])) .$$

The final task is to fuse $\text{unfoldM } p f$ with $\text{foldr } (\odot) (\text{return } [])$.

5.1 Monadic Hylo-Fusion

In a pure setting, it is known that, provided that the unfolding phase terminates, $\text{foldr } (\otimes) e \cdot \text{unfoldr } p f$ is the unique solution of *hylo* in the equation below [Hinze et al. 2015]:

$$\begin{aligned} \text{hylo } y \mid p y &= e \\ \mid \text{otherwise} &= \text{let } f y = (x, z) \text{ in } x \otimes \text{hylo } z . \end{aligned}$$

Hylomorphisms with monadic folds and unfolds are a bit tricky. Pardo [2001] discussed hylomorphism for regular base functors, where the unfolding phase is monadic while the folding phase is pure. As for the case when both phases are monadic, he noted “the drawback ... is that they cannot be always transformed into a single function that avoids the construction of the intermediate data structure.”

For our purpose, we focus our attention on lists, and have a theorem fusing the monadic unfolding and folding phases under a side condition. Given $(\otimes) :: b \rightarrow m c \rightarrow m c$, $e :: c$, $p :: a \rightarrow \text{Bool}$, and $f :: a \rightarrow m (b, a)$ (where *Monad* m), consider the expression:

$$\text{unfoldM } p f \gg \text{foldr } (\otimes) (\text{return } e) :: \text{Monad } m \Rightarrow a \rightarrow m c .$$

The following theorem says that this combination of folding and unfolding can be fused into one, with some side conditions:

THEOREM 5.1. *Let $m :: * \rightarrow * \rightarrow *$ be in type class *Monad*. For all $(\otimes) :: a \rightarrow m c \rightarrow m c$, $e :: m c$, $p :: b \rightarrow \text{Bool}$, and $f :: b \rightarrow m (a, c)$, we have that $\text{unfoldM } p f \gg \text{foldr } (\otimes) e = \text{hyloM } (\otimes) e p f$, defined by:*

$$\begin{aligned} \text{hyloM } (\otimes) e p f y \mid p y &= e \\ \mid \text{otherwise} &= f y \gg \lambda(x, z) \rightarrow x \otimes \text{hyloM } (\otimes) e p f z , \end{aligned}$$

if the relation $(\neg \cdot p) ? \cdot \text{snd} \cdot (\ll) \cdot f$ is well-founded (see the note below) and, for all k , we have

$$n \gg ((x \otimes) \cdot k) = x \otimes (n \gg k) , \quad (23)$$

where n abbreviates $\text{unfoldM } p f z$.

The “well-foundedness” condition essentially says that f eventually terminates – details to be explained after the proof of this theorem. Condition (23) may look quite restrictive. In most cases the author have seen, however, we can actually prove that (23) holds for an entire class of n that includes $\text{unfoldM } p f z$. In the application of this report, for example, the only effect of $\text{unfoldM } p f z$ is non-determinism, and we will prove in Lemma 5.2 that (23) holds for all n whose only effect is non-determinism, for the particular operator we use in the n -queens problem.

We prove Theorem 5.1 below.

PROOF. We start with showing that $\text{unfoldM } p f \gg \text{foldr } (\otimes) e$ is a fixed-point of the recursive equations of *hyloM*. When $p y$ holds, it is immediate that

$$\text{return } [] \gg \text{foldr } (\otimes) e = e .$$

When $\neg (p y)$, we reason:

$$\begin{aligned} \text{unfoldM } p f y \gg \text{foldr } (\otimes) e \\ = \{ \text{definition of } \text{unfoldM}, \neg (p y) \} \end{aligned}$$

$$\begin{aligned}
& (f \ y \gg (\lambda(x, z) \rightarrow (x) \ \$ \ unfoldM \ p \ f \ z)) \gg \text{foldr} (\otimes) \ e \\
& = \quad \{ \text{monad law and } \text{foldr} \} \\
& \quad f \ y \gg (\lambda(x, z) \rightarrow \text{unfoldM} \ p \ f \ z \gg \lambda xs \rightarrow x \otimes \text{foldr} (\otimes) \ e \ xs) \\
& = \quad \{ \text{since } n \gg ((x \otimes) \cdot k) = x \otimes (n \gg k) \text{ where } n = \text{unfoldM} \ p \ f \ z \} \\
& \quad f \ y \gg (\lambda(x, z) \rightarrow x \otimes (\text{unfoldM} \ p \ f \ z \gg \text{foldr} (\otimes) \ e)).
\end{aligned}$$

Now that $\text{unfoldM} \ p \ f \ z \gg \text{foldr} (\otimes) \ e$ is a fixed-point, we may conclude that it equals $\text{hyloM} (\otimes) \ e \ p \ f$ if the latter has a unique fixed-point, which is guaranteed by the well-foundedness condition. See the note below. \square

Note. Let q be a predicate, $q?$ is a relation defined by $\{(x, x) \mid q \ x\}$. The parameter y in unfoldM is called the *seed* used to generate the list. The relation $(\neg \cdot p) ? \cdot \text{snd} \cdot (\gg) \cdot f$ maps one seed to the next seed (where (\gg) is (\gg) written reversed). If it is *well-founded*, intuitively speaking, the seed generation cannot go on forever and p will eventually hold. It is known that inductive types (those can be folded) and coinductive types (those can be unfolded) do not coincide in SET. To allow a fold to be composed after an unfold, typically one moves to a semantics based on complete partial orders. However, it was shown [Doornbos and Backhouse 1995] that, in Rel, when the relation generating seeds is well-founded, hylo-equations do have unique solutions. One may thus stay within a set-theoretic semantics. Such an approach is recently explored again [Hinze et al. 2015]. (*End of Note*)

Theorem 5.1 does not rely on the *local state laws* (20) and (21), and does not put restriction on e . To apply the theorem to our particular case, we have to show that its preconditions hold for our particular (\odot) – for that we will need (21) and perhaps also (20). In the lemma below we slightly generalise (\odot) in Theorem 4.4:

LEMMA 5.2. *Assume that (21) holds. Given $p::a \rightarrow s \rightarrow \text{Bool}$, $\text{next}::a \rightarrow s \rightarrow s$, and $\text{res}::a \rightarrow b \rightarrow b$, define (\odot) as below:*

$$\begin{aligned}
(\odot) & :: (\text{MonadPlus } m, \text{MonadState } s \ m) \Rightarrow a \rightarrow m \ b \rightarrow m \ b \\
x \odot m & = \text{get} \gg \lambda st \rightarrow \text{guard} (p \ x \ st) \gg \\
& \quad \text{put} (\text{next } x \ st) \gg (\text{res } x \ \$ \ m).
\end{aligned}$$

We have $n \gg ((x \odot) \cdot k) = x \odot (n \gg k)$, if n commutes with state.

PROOF. We reason:

$$\begin{aligned}
& n \gg ((x \odot) \cdot k) \\
& = n \gg \lambda y \rightarrow x \odot k \ y \\
& = \quad \{ \text{definition of } (\odot) \} \\
& \quad n \gg \lambda y \rightarrow \text{get} \gg \lambda st \rightarrow \\
& \quad \text{guard} (p \ x \ st) \gg \text{put} (\text{next } x \ st) \gg (\text{res } x \ \$ \ k \ y) \\
& = \quad \{ n \text{ commutes with state} \} \\
& \quad \text{get} \gg \lambda st \rightarrow n \gg \lambda y \rightarrow \\
& \quad \text{guard} (p \ x \ st) \gg \text{put} (\text{next } x \ st) \gg (\text{res } x \ \$ \ (k \ y)) \\
& = \quad \{ \text{by (15), since (21) holds} \} \\
& \quad \text{get} \gg \lambda st \rightarrow \text{guard} (p \ x \ st) \gg \\
& \quad n \gg \lambda y \rightarrow \text{put} (\text{next } x \ st) \gg (\text{res } x \ \$ \ (k \ y)) \\
& = \quad \{ n \text{ commutes with state} \} \\
& \quad \text{get} \gg \lambda st \rightarrow \text{guard} (p \ x \ st) \gg
\end{aligned}$$

$$\begin{aligned}
& \text{put } (\text{next } x \text{ st}) \gg n \gg \lambda y \rightarrow (\text{res } x \text{ } \$) (k y)) \\
= & \{ \text{properties of } (\$) \} \\
& \text{get } \gg \lambda st \rightarrow \text{guard } (p x st) \gg \\
& \text{put } (\text{next } x \text{ st}) \gg (\text{res } x \text{ } \$) n \gg k) \\
= & \{ \text{definition of } (\odot) \} \\
& x \odot (n \gg k) .
\end{aligned}$$

□

5.2 Summary, and Solving n -Queens

To conclude our derivation, a problem formulated as $\text{unfoldM } p f z \gg \text{filt } (\text{all } ok \cdot \text{scanl}_+ (\oplus) st)$ can be solved by a hylomorphism. Define:

$$\begin{aligned}
\text{solve} &:: (\text{MonadState } s m, \text{MonadPlus } m) \Rightarrow \\
& (b \rightarrow \text{Bool}) \rightarrow (b \rightarrow m (a, b)) \rightarrow (s \rightarrow \text{Bool}) \rightarrow (s \rightarrow a \rightarrow s) \rightarrow s \rightarrow b \rightarrow m [a] \\
\text{solve } p f ok (\oplus) st z &= \text{protect } (\text{put } st \gg \text{hyloM } (\odot) (\text{return } []) p f z) , \\
& \text{where } x \odot m = \text{get } \gg \lambda st \rightarrow \text{guard } (ok (st \oplus x)) \gg \\
& \quad \text{put } (st \oplus x) \gg ((x:) \$) m) .
\end{aligned}$$

COROLLARY 5.3. *Given $p :: b \rightarrow \text{Bool}$, $f :: (\text{MonadPlus } m, \text{MonadState } s m) \Rightarrow b \rightarrow m (a, b)$, $z :: b$, $ok :: s \rightarrow \text{Bool}$, $(\oplus) :: s \rightarrow a \rightarrow s$, $st :: s$, If the relation $(\neg \cdot p) ? \cdot \text{snd} \cdot (\approx\approx) \cdot f$ is well-founded, the local state laws hold in addition to the other laws, and $\text{unfoldM } p f z$ commutes with state, we have*

$$\begin{aligned}
\text{unfoldM } p f z \gg \text{filt } (\text{all } ok \cdot \text{scanl}_+ (\oplus) st) &= \\
\text{solve } p f ok (\oplus) st z . &
\end{aligned}$$

n -Queens Solved. Recall that

$$\begin{aligned}
\text{queens } n &= \text{perm } [0 \dots n - 1] \gg \text{filt } \text{safe} \\
&= \text{unfoldM } \text{null } \text{select } [0 \dots n - 1] \gg \text{filt } (\text{all } ok \cdot \text{scanl}_+ (\oplus) (0, [], [])) ,
\end{aligned}$$

where the auxiliary functions select , ok , (\oplus) are defined in Section 3. The function select cannot be applied forever since the length of the given list decreases after each call, and perm , using only non-determinism, commutes with state. Therefore, Corollary 5.3 applies, and we have $\text{queens } n = \text{solve } \text{null } \text{select } ok (\oplus) (0, [], []) [0 \dots n - 1]$. Expanding the definitions we get:

$$\begin{aligned}
\text{queens} &:: (\text{MonadPlus } m, \text{MonadState } (\text{Int}, [\text{Int}], [\text{Int}]) m) \Rightarrow \text{Int} \rightarrow m [\text{Int}] \\
\text{queens } n &= \text{protect } (\text{put } (0, [], []) \gg \text{queensBody } [0 \dots n - 1]) , \\
\text{queensBody} &:: (\text{MonadPlus } m, \text{MonadState } (\text{Int}, [\text{Int}], [\text{Int}]) m) \Rightarrow [\text{Int}] \rightarrow m [\text{Int}] \\
\text{queensBody } [] &= \text{return } [] \\
\text{queensBody } xs &= \text{select } xs \gg \lambda (x, ys) \rightarrow \\
& \quad \text{get } \gg \lambda st \rightarrow \text{guard } (ok (st \oplus x)) \gg \\
& \quad \text{put } (st \oplus x) \gg ((x:) \$) \text{queensBody } ys) , \\
& \text{where } (i, us, ds) \oplus x = (1 + i, (i + x) : us, (i - x) : ds) \\
& \quad ok (_, u : us, d : ds) = (u \notin us) \wedge (d \notin ds) .
\end{aligned}$$

This completes the derivation of our backtracking algorithm for the n -queens problem.

6 CONCLUSIONS AND RELATED WORK

This report is a case study of reasoning and derivation of monadic programs. To study the interaction between non-determinism and state, we construct backtracking algorithms solving problems that can be specified in the form $\text{unfoldM } f \ p \ \gg \ \text{assert } (\text{all ok} \cdot \text{scanl}_+ (\oplus) \text{ st})$. The derivation of the backtracking algorithm works by fusing the two phases into a monadic hylomorphism. It turns out that in derivations of programs using non-determinism and state, commutativity plays an important role. We assume in this report that the local state laws (right-distributivity and right-zero) hold. In this scenario we have nicer properties at hand, and commutativity holds more generally.

The local state laws imply that each non-deterministic branch has its own state. It is cheap to implement when the state can be represented by linked data structures, such as a tuple containing lists, as in the n -queens example. When the state contains blocked data, such as a large array, duplicating the state for each non-deterministic branch can be costly. Hence there is practical need for sharing one global state among non-deterministic branches. When a monad supports shared global state and non-determinism, commutativity of the two effects holds in limited cases. The behaviour of the monad is much less intuitive, and might be considered awkward sometimes. In a subsequent paper [Pauwels et al. 2019], we attempt to find out what algebraic laws we can expect and how to reason with programs when the state is global.

Affeldt et al. [2019] modelled a hierarchy of monadic effects in Coq. The formalisation was applied to verify a number of equational proofs of monadic programs, including some of the proofs in an earlier version of this report. A number of errors was found and reported to the author.

Acknowledgements. The author would like to thank Tyng-Ruey Chuang for examining a very early draft of this report; Jeremy Gibbons, who has been following the development of this research and keeping giving good advices; and Tom Schrijvers and Koen Pauwels, for nice cooperation on work following-up this report. Thanks also go to Reynald Affeldt, David Nowak and Takafumi Saikawa for verifying and finding errors in the proofs in an earlier version of this report. The author is solely responsible for any remaining errors, however.

REFERENCES

- Reynald Affeldt, David Nowak, and Takafumi Saikawa. 2019. A hierarchy of monadic effects for program verification using equational reasoning. In *Mathematics of Program Construction*, Graham Hutton (Ed.). Springer.
- Henk Doornbos and Roland C. Backhouse. 1995. Induction and recursion on datatypes. In *Mathematics of Program Construction (Lecture Notes in Computer Science)*, Bernhard Möller (Ed.). Springer, 242–256.
- Jeremy Gibbons and Ralf Hinze. 2011. Just do it: simple monadic equational reasoning. In *International Conference on Functional Programming*, Olivier Danvy (Ed.). ACM Press, 2–14.
- Andy Gill and Edward Kmett. 2014. The Monad Transformer Library. <https://hackage.haskell.org/package/mtl>.
- Ralf Hinze, Nicolas Wu, and Jeremy Gibbons. 2015. Conjugate hylomorphisms, or: the mother of all structured recursion schemes. In *Symposium on Principles of Programming Languages*, David Walker (Ed.). ACM Press, 527–538.
- Graham Hutton and Diana Fulger. 2008. Reasoning about effects: seeing the wood through the trees. In *Draft Proceedings of Trends in Functional Programming*, Peter Achten, Pieter Koopman, and Marco T. Morazán (Eds.).
- Oleg Kiselyov. 2013. How to restrict a monad without breaking it: the winding road to the Set monad. <http://okmij.org/ftp/Haskell/set-monad.html>.
- Oleg Kiselyov. 2015. Laws of MonadPlus. <http://okmij.org/ftp/Computation/monads.html#monadplus>.
- Oleg Kiselyov and Hiromi Ishii. 2015. Freer monads, more extensible effects. In *Symposium on Haskell*, John H Reppy (Ed.). ACM Press, 94–105.
- Oleg Kiselyov, Amr Sabry, and Cameron Swords. 2013. Extensible effects: an alternative to monad transformers. In *Symposium on Haskell*, Chung-chieh Shan (Ed.). ACM Press, 59–70.
- Erik Meijer, Maarten Fokkinga, and Ross Paterson. 1991. Functional programming with bananas, lenses, envelopes, and barbed wire. In *Functional Programming Languages and Computer Architecture (Lecture Notes in Computer Science)*, R. John Muir Hughes (Ed.). Springer-Verlag, 124–144.
- Eugenio Moggi. 1989. Computational lambda-calculus and monads. In *Logic in Computer Science*, Rohit Parikh (Ed.). IEEE Computer Society Press, 14–23.

- Alberto Pardo. 2001. Fusion of recursive programs with computational effects. *Theoretical Computer Science* 260, 1-2 (2001), 165–207.
- Koen Pauwels, Tom Schrijvers, and Shin-Cheng Mu. 2019. Handling local state with global state. In *Mathematics of Program Construction*, Graham Hutton (Ed.). Springer.
- Philip L. Wadler. 1992. Monads for functional programming. In *Program Design Calculi: Marktoberdorf Summer School*, Manfred Broy (Ed.), Springer-Verlag, 233–264.
- Nicolas Wu, Tom Schrijvers, and Ralf Hinze. 2012. Effect handlers in scope. In *Symposium on Haskell*, Janis Voigtländer (Ed.). ACM Press, 1–12.

A MISCELLANEOUS PROOFS

Proofs of (13) and (14).

PROOF. Proof of (13) relies only on property of **if** and conjunction:

$$\begin{aligned}
 & \text{guard } (p \wedge q) \\
 &= \text{if } p \wedge q \text{ then return } () \text{ else } \emptyset \\
 &= \text{if } p \text{ then (if } q \text{ then return } () \text{ else } \emptyset) \text{ else } \emptyset \\
 &= \text{if } p \text{ then guard } q \text{ else } \emptyset \\
 &= \text{guard } p \gg \text{guard } q .
 \end{aligned}$$

To prove (14), surprisingly, we need only distributivity and *not* (12):

$$\begin{aligned}
 & \text{guard } p \gg (f \ \$ \ m) \\
 &= \{ \text{definition of guard} \} \\
 & \quad (\text{if } p \text{ then return } () \text{ else } \emptyset) \gg (f \ \$ \ m) \\
 &= \{ \text{by (7)} \} \\
 & \quad \text{if } p \text{ then return } () \gg (f \ \$ \ m) \text{ else } \emptyset \gg \gg (f \ \$ \ m) \\
 &= \{ \text{by (3) and (1)} \} \\
 & \quad \text{if } p \text{ then } f \ \$ \ (\text{return } () \gg m) \text{ else } f \ \$ \ (\emptyset \gg m) \\
 &= \{ \text{by (7)} \} \\
 & \quad f \ \$ \ ((\text{if } p \text{ then return } () \text{ else } \emptyset) \gg m) \\
 &= \{ \text{definition of guard} \} \\
 & \quad f \ \$ \ (\text{guard } p \gg m) .
 \end{aligned}$$

□

Proof of (15).

PROOF. We reason:

$$\begin{aligned}
 & m \gg \lambda x \rightarrow \text{guard } p \gg \text{return } x \\
 &= \{ \text{definition of guard} \} \\
 & \quad m \gg \lambda x \rightarrow (\text{if } p \text{ then return } () \text{ else } \emptyset) \gg \text{return } x \\
 &= \{ \text{by (7), with } f \ n = m \gg \lambda x \rightarrow n \gg \text{return } x \} \\
 & \quad \text{if } p \text{ then } m \gg \lambda x \rightarrow \text{return } () \gg \text{return } x \\
 & \quad \quad \text{else } m \gg \lambda x \rightarrow \emptyset \gg \text{return } x \\
 &= \{ \text{since } \text{return } () \gg n = n \text{ and (12)} \} \\
 & \quad \text{if } p \text{ then } m \text{ else } m \gg \emptyset \\
 &= \{ \text{assumption: } m \gg \emptyset = \emptyset \} \\
 & \quad \text{if } p \text{ then } m \text{ else } \emptyset \\
 &= \{ \text{since } \text{return } () \gg n = n \text{ and (12)} \}
 \end{aligned}$$

if p **then** $\text{return } () \gg m$
 else $\emptyset \gg m$
= { by (7), with $f = (\gg m)$ }
 (if p **then** $\text{return } ()$ **else** \emptyset) $\gg m$
= { definition of *guard* }
 guard $p \gg m$.

□