

Reversible Session-Based Concurrency in Haskell^{*}

Folkert de Vries¹ and Jorge A. Perez¹[0000–0002–1452–6180]

University of Groningen, The Netherlands,

Abstract. Under a reversible semantics, computation steps can be undone. For message-passing, concurrent programs, reversing computation steps is a challenging and delicate task; one typically aims at formal semantics which are *causally-consistent*. Prior work has addressed this challenge in the context of a process model of multiparty protocols (choreographies) following a so-called *monitors-as-memories* approach. In this paper, we describe our ongoing efforts aimed at implementing this operational semantics in Haskell.

^{*} F. de Vries is a BSc student.

Table of Contents

Reversible Session-Based Concurrency in Haskell	1
<i>Folkert de Vries and Jorge A. Perez</i>	
1 Introduction	4
2 The Main Idea	5
2.1 Process Calculi	5
2.2 Implementing the PPDP calculus	7
2.3 Multiparty Session Types	8
2.3.1 Global Types	9
2.3.2 Local Types	11
2.4 Reversibility	12
2.5 Abstraction passing is protocol delegation	14
3 Putting it all together	14
3.1 Running and Debugging Programs	16
3.2 Properties of Reversibility	16
4 Convenient Syntax with the Free Monad	17
5 Discussion	18
5.1 Benefits of pure functional programming	18
5.2 Concurrent Debuggers	19
6 Conclusion	20
7 Appendix	20
A Performing IO in Haskell	21
B Do-notation	22
C Monads	22
D Except	23
E State and StateT	24
F Factoring out recursion	25
G Fix	25
H Monad.Free	27

I	Guaranteeing well-formedness of Free	27
---	--	----

J	Scheduling code	29
---	---------------------------	----

1 Introduction

This thesis describes an implemetation of theoretical work in the area of concurrent programming. In particular it is concerned with using formal tools to check the correctness of message passing and allow for flexible error handling.

An example of a class of errors in message passing is lack of **progress**. Consider this example of a receive on an empty channel:

```
main = do
  channel <- Channel.new
  -- will block forever
  message <- Channel.receive channel
```

This snippet uses Haskell's do-notation. the <- is used to bind the result of an effectful computation - like receiveing from a channel. See also appendix B

No value will ever be sent on the channel, so the receive blocks forever: it can't make any progress.

Failing gracefully is also harder in a concurrent context, because failure may need to be communicated to other participants and joint action may be necesarry to clean up the failure.

Often, concurrent systems often perform a list of individual operations that are meant to be one whole. In the snippet below, there is a point where the money is subtracted from A but not yet added to B. If an error occurs at this point, the system should revert back to the initial state: Just failing silently makes the money disappear.

-- more convincing example

Moving back to the initial state is non-trivial. How can we be sure that we have cleaned up all of our actions and use minimal resources?

The framework presented in [1] sets out to solve both of these issues. However, so far this was purely a theoretical exercise. How well do the ideas presented translate to a programming context, and is the resulting system actually convenient to use? In answering these questions this bachelor's thesis will make the following contributions:

- We begin by analyzing the three core components of [1]:
 - A process calculus, multiparty session types and reversibility. At the same time we give the encoding of the formal definition into Haskell data types.
 - We define and implement a **process calculus** from its foundations. Later we use the **Free** monad to provide convenient syntax.

- Next we look at **multiparty session types** for the implemented calculus. The session types feature nested recursion and choice.
 - Finally we consider **reversibility** given the two previous concepts. In particular we look at the information that needs to be preserved when moving forward in order to move backward correctly.
- Next we combine our encodings of the core components to define forward and backward evaluation functions.

The structure looks as follows: section 2 introduces the three key foundations from the PPDP paper and how they can be encoded into Haskell data types. Section 3 shows how the data types can be used to implement forward and backward reduction and provides the other mechanics needed to evaluate the program. Section 4 provides a more convenient syntax for writing programs. The appendices A through J give background and extra examples for the Haskell concepts and terminology used in the paper.

2 The Main Idea

The PPDP paper builds a system that features three basic concepts: a process calculus, multiparty session types and reversibility. These three ideas are combined to create more robust concurrent programs.

The process calculus is a very low-level programming language that allows concurrent communication. Their flavor of multiparty session types dynamically check the communication a process performs against a protocol. Reversibility - backwards evaluation of our process calculus - gives the ability to recover from errors or to safely fail.

In this section we show how these three concepts are formally defined in PPDP and how they are implemented in our Haskell implementation.

2.1 Process Calculi

As said, a process calculus is like a minimal programming language that can model concurrent communication. We will start by considering a well-understood existing calculus - the pi calculus. Next we will look at how PPDP extends it and finally give an implementation as a Haskell data type.

The pi-calculus is to concurrent computation much like what the lambda calculus is for sequential computing : A simple model that is convenient for reasoning and constructing proofs. The pi-calculus is defined as

$P, Q, R ::= \bar{x}(y).P$	Send the value y over channel x , then run P
$ x(y).P$	Receive on channel x , bind the result to y , then run P
$ P Q$	Run P and Q simultaneously
$ (\nu x)P$	Create a new channel x and run P
$!P$	Repeatedly spawn copies of P
$ 0$	Terminate the process

With this syntax we can construct programs like so:

$$(\nu x)(\bar{x}(42).0 \mid x(y).0)$$

This program is read as “create a channel x and then in parallel send 42 over x then terminate, and receive a value on x and bind it to the name y then terminate.” The pi-calculus is much too low-level to write real programs in, but it can compute any computable function (because the lambda calculus can be encoded into it [2]) and lends itself well to proofs.

A pi-calculus term can be reduced when there is a send and a receive over the same channel in parallel.

$$\bar{x}(z).P \mid x(y).Q \rightarrow P|Q[z/y]$$

The PPDP paper makes a few generalizations to this calculus. The calculus used in PPDP is given by

$P, Q ::= u!(V).P$	Send the value V , then run P
$ u?(x).P$	Receive and bind the result to x , then run P
$ u \triangleleft \{l_i.P_i\}_{i \in I}$	Select an option, then broadcast the choice, then run P_i
$ u \triangleright \{l_i : P_i\}_{i \in I}$	Offer options, receive a choice by the selector, then run P_i
$ (P Q)$	Run P and Q simultaneously
$ X \mid \mu X.P$	Variable and function abstraction
$ Vu$	function application
$ (\nu n)$	name restriction: make n unused in a term
$ \mathbf{0}$	terminate

We still have sending, receiving and parallel, and allow recursion and termination. Channel creation has been removed for simplicity: we'll use only one globally available channel. This channel is implemented as a queue which means that sends are non-blocking.

The primary extension is choice: This is where instead of a value, a label is sent from a selector to an offerer. Both parties will pick the branch that the label corresponds to. Choice could be implemented as a combination of send/receive and if-then-else, but they are primitives here because each branch can have a different type (this will become clearer in section, 2.3.)

Finally, we allow the sending of thunks - functions that take `Unit` as their argument and return a process term (i.e. a piece of program that can be executed). The fact that we can send programs - and not just values - means that our calculus is a higher-order calculus. The sending of thunks provides “protocol delegation via abstraction passing”.

The definition of functions in the PPDP paper is a bit strange: there are two ways of recursion - on the process level and on the value level. In the implementation the former has been removed.

2.2 Implementing the PPDP calculus

The implementation uses an algebraic data type (union type/sum type) to encode all the constructors of the grammar. We use the `Fix` type to factor out recursion from the grammar. As mentioned we omit the process-level recursion.

```
type Participant = String
type Identifier = String

type Program value = Fix (ProgramF value)

data ProgramF value next
  -- communication primitives
  = Send
    { owner :: Participant
    , value :: value
    , continuation :: next
    }
  | Receive
    { owner :: Participant
    , variableName :: Identifier
    , continuation :: next
    }

  -- choice primitives
```

```

| Offer Participant (List (String, next))
| Select Participant (List (String, value, next))

-- other constructors
| Parallel next next
| Application Identifier value
| NoOp
deriving (Functor)

```

We also need values in our language. To write more interesting examples we extend the types of values that can be used from references, booleans and functions to also include integers, strings, and basic integer and logic operators.

```

data Value
= VBool Bool
| VInt Int
| VString String
| VUnit
| VIntOperator Value IntOperator Value
| VComparison Value Ordering Value
| VFunction Identifier (Program Value)
| VReference Identifier
| VLabel String

```

We can now write the send/receive example as

```

example =
  Fix
    ( Parallel
      (Fix (Send "me" (VInt 42) (Fix NoOp)))
      (Fix (Receive "you" "y" (Fix NoOp)))
    )

```

While the above is easily manipulatable with pattern matching and functions from the `Fix` module, it's impossible to write clear examples in this style. Longer expressions need ever more parentheses and in general there is too much syntactical clutter. We will get back to designing a better syntax for defining programs in section 4.

2.3 Multiparty Session Types

As programmers we would like our programs to work as we expect. With concurrent programs, fitting the whole program in one's head becomes increasingly difficult as the application becomes larger.

Most programmers are familiar with data types. Compilers use data types to typecheck programs. Programs that typecheck are statically guaranteed to not have certain classes of bugs. Type systems range from very loose (dynamic languages like javascript and python) to very restrictive (Coq, Agda, Idris).

In the late 90s, a similar tool was developed for “typing” and checking the interaction between concurrent processes: Session types. Session types provide three key properties:

- **Order** every participant has an ordered list of sends and receives that it must perform
- **Progress** every sent message is eventually received
- **Safety** sender and receiver always agree about the type of the sent value

Next we will look at how these types are defined and how we can check that our program implements its session type.

2.3.1 Global Types The simplest non-trivial concurrent program has two participants. In this case, the types of the two participants are exactly dual: if the one sends, the other must receive. However, for the multiparty (3 or more) use case, things aren’t so simple.

We need to define globally what transactions occur in our protocol.

```
simple :: GlobalType String String
simple = do
  message "carol" "bob" "Bool"
  message "alice" "carol" "int"
end
```

We can see immediately that **safety and progress are guaranteed**: we cannot construct a valid global type that breaks these guarantees: Every communication has a send and receive, and they both must agree on the type. A more realistic example that we’ll use as a running example is the three buyer protocol. In this protocol, Alice and Bob communicate with the Vendor about the purchase of some item:

$$\begin{aligned}
 G = & A \rightarrow V : \langle \text{title} \rangle. \quad V \rightarrow \{A, B\} : \langle \text{price} \rangle. \\
 & A \rightarrow B : \langle \text{share} \rangle. \quad B \rightarrow \{A, V\} : \langle \text{OK} \rangle. \\
 & B \rightarrow C : \langle \text{share} \rangle. \quad B \rightarrow C : \langle \{\{\diamond\}\} \rangle. \\
 & B \rightarrow V : \langle \text{address} \rangle. \quad V \rightarrow B : \langle \text{date} \rangle. \text{end}
 \end{aligned}$$

Near the end of the protocol, Bob has to leave and transfers the remainder of his protocol to Carol. She will also be sent the code - a **thunk process** $\{\{\diamond\}\}$ - to

complete Bob's protocol, and finish the protocol in his name by evaluating the sent thunk.

The full definition of global types in the Haskell implementation is given by

```
type GlobalType participant u =
    Free (GlobalTypeF participant u) Void

data GlobalTypeF participant u next
    = Transaction
      { from :: participant
      , to :: participant
      , tipe :: u
      , continuation :: next
      }
    | Choice
      { from :: participant
      , to :: participant
      , options :: Map String next
      }
    | End
    | RecursionPoint next
    | RecursionVariable
    | Weaken next
    deriving (Functor)
```

We can now see why choice is useful: it allows us to branch on the session type level. For instance, one branch can terminate the protocol, and the other can start from the beginning.

The final three constructors are required for supporting nested recursion and taken from [3]. A `RecursionPoint` is a point in the protocol that we can later jump back to. A `RecursionVariable` triggers jumping to a previously encountered `RecursionPoint`. By default it will jump to the closest and most-recently encountered `RecursionPoint`, but `WeakenRecursion` makes it jump one `RecursionPoint` higher, encountering 2 weakens will jump 2 levels higher etc.

Using `Monad.Free`, we can write the `ThreeBuyer` example type as

```
data MyParticipants = A | B | C | V
    deriving (Show, Eq, Ord, Enum, Bounded)

data MyType = Title | Price | Share | Ok | Thunk | Address | Date
    deriving (Show, Eq, Ord)

globalType :: GlobalType.GlobalType MyParticipants MyType
```

```

globalType = do
  message A V Title
  messages V [A, B] Price
  message A B Share
  messages B [A, V] Ok
  message B C Share
  message B C Thunk
  message B V Address
  message V B Date
end

```

2.3.2 Local Types A global type can contain inherent parallelism: the order of its steps is not fully defined. Checking for correctness against a global type is therefore quite hard. The solution is to project the global type onto its participants, creating a local type.

The local type is an ordered list of steps that the participant must execute to comply with the protocol. Thus the third property **Order** is satisfied for local types.

The projection is mostly straightforward, except for choice. Because we allow recursion, a branch of a choice may recurse back to the beginning. When this occurs, all participants have to jump back to the beginning, so every choice must be communicated to all participants.

$$\begin{aligned}
(p \rightarrow q : \langle U \rangle . G) \downarrow_r &= \begin{cases} q! \langle U \rangle . (G \downarrow_r) & \text{if } r = p \\ p? \langle U \rangle . (G \downarrow_r) & \text{if } r = q \\ (G \downarrow_r) & \text{if } r \neq q, r \neq p \end{cases} \\
(p \rightarrow q : \{l_i : G_i\}_{i \in I}) \downarrow_r &= \begin{cases} q \oplus \{l_i : (G_i \downarrow_r)\}_{i \in I} & \text{if } r = p \\ p \& \{l_i : G_i \downarrow_r\}_{i \in I} & \text{if } r = q \\ (G_1 \downarrow_r) & \text{if } r \neq q, r \neq p \text{ and} \\ & \forall i, j \in I. G_i \downarrow_r = G_j \downarrow_r \end{cases} \\
(p \rightarrow q : \{l_i : G_i\}_{i \in I}) \downarrow_r &= \begin{cases} q \oplus \{l_i : (G_i \downarrow_r)\}_{i \in I} & \text{if } r = p \\ p \& \{l_i : G_i \downarrow_r\}_{i \in I} & \text{if } r = q \\ r \oplus \{l_i : G_i \downarrow_r\}_{i \in I} & \text{if } r \neq q, r \neq p \\ q \& \{l_i : G_i \downarrow_r\}_{i \in I} & \text{if } r \neq q, r \neq p \end{cases} \\
(\mu X. G) \downarrow_r &= \begin{cases} \mu X. G \downarrow_r & \text{if } r \text{ occurs in } G \\ \text{end} & \text{otherwise} \end{cases} \\
X \downarrow_r = X & \quad \text{end} \downarrow_r = \text{end}
\end{aligned}$$

Fig. 1. Projection of a global type G onto a participant r .

NOTE: the above is still wrong. For offer, it must also send the choice to all other participants all participants that are not p or q must also be informed of the choice. How do we write this all down?

all choices need to be communicated to all participants because a choice may trigger recursion. The recursion jumps back in protocol to an earlier state and expects all participants to be at that state. Otherwise, If a choice is not communicated with everyone, the other participants cannot know that a jump has to be made

The solution we have chosen is that the offerer relays the decision to all the other participants

2.4 Reversibility

The third component of the system is reversibility. The idea here is that we can move back to previous program states, reversing forward steps.

Reversibility is useful in a concurrent setting when an error is encountered but the current state is invalid. In such a case the program should revert to its initial state, from which next steps can be considered (e.g. to retry or to log the failure).

The naive way to achieve reversal is to store a snapshot of the initial state, but the memory consumption of this method is a deal-breaker. For instance, the system may interact with a large database. Keeping many copies of the database around is inconvenient and may not even be physically possible.

A nicer approach is to keep track of our forward steps, and store just enough information to reverse those steps. Conceptually, we're leaving behind a trail of breadcrumbs so we can always find our way back.

The challenge, then, is to find the minimal amount of information that we need to store for every instruction. Broadly, we need to track information about two things: the type and the process.

For the type we define a new data type called **TypeContext**. It contains the actions that have been performed and for some stores a bit of extra information like the **owner**.

On the process level there are four things that we need to track:

1. Used variable names in receives

The rest of the program depends on the name that we assign to a received value. Therefore we need to restore the original name when we revert. Used variable names are stored on a stack that is popped when we revert a receive.

```

program = do
  decision <- H.receive
  H.send decision
  H.send decision

```

2. Unused branches

When a choice is made and then reverted, we want all our options to be available again. Currently the semantics aren't able to make a different choice, but it will in the future.

```

type Zipper a = (List a, a, List a)

data OtherOptions
  = OtherSelections (Zipper (String, Value, Program Value))
  | OtherOffers (Zipper (String, Program Value))

```

We need to store the selection that has been made. The zipper contains the taken path as its central `a`, and the options before and after as the lists on either side.

3. Function applications

When applying a function we lose information about the applied function and the argument. Therefore we store them in a map and associate them with a unique identifier. This identifier is given to the **Application** constructor so when stepping backward the function and the argument can be recovered.

```

Map Identifier (Value, Value)

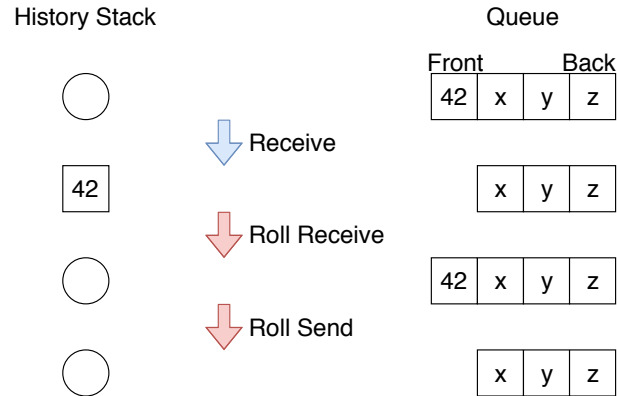
```

You might think that a stack would be a simpler solution, but a stack can give undesired behavior. Say that a participant is running in two locations, and the last-performed action at both locations is a function application. Now we want to undo both applications, but the order in which to undo them is undefined: we need both orders to work. When the application keeps track of exactly which function and argument it used the end result is always the same. Just using a stack could mix up the applications.

4. Messages on the channel

When a value is sent, the sender loses track of what has been sent. Therefore, reverting a send/receive pair must move the value from the receiver via the queue back to the sender. To this end, the queue holds on to received values: the value is popped from the queue but pushed onto the history stack. Now when the

receive is rolled, the value is moved back onto the queue, and when the send is rolled the value is moved from the head of the queue into the sender's process.



2.5 Abstraction passing is protocol delegation

Protocol delegation is where a participant can delegate (a part of) their protocol to be fulfilled by another participant. An example of where this idea is useful is a load balancing server: from the client's perspective, the server handles the request, but actually the load balancer delegates incoming requests to workers. The client does not need to be aware of this implementation detail.

To implement this idea, instructions need to keep track of whose protocol they should move forward. The **owner** field stores this information. Regardless of by whom an instruction is evaluated, the local type indexed by the **owner** field is the one that is checked against and changed.

3 Putting it all together

With all the definitions encoded, we can now define forward and backward evaluation of our system. Our aim is to implement

```
type Session a = StateT ExecutionState (Except Error) a

forward  :: Location -> Session ()
backward :: Location -> Session ()
```

Where

- **ExecutionState** stores the state of the world
- **Error** can be thrown when something fails

- `Location` defines places where code is ran concurrently (threads or machines)

We store all the information about a participant in a type called `Monitor`.

```
data Monitor value type =
  Monitor
    { _localType :: LocalTypeState type
    , _recursiveVariableNumber :: Int
    , _recursionPoints :: List (LocalType type)
    , _store :: Map Identifier value
    , _usedVariables :: List Binding
    , _applicationHistory :: Map Identifier (value, value)
    }
  deriving (Show, Eq)

data Binding =
  Binding
    { _visibleName :: Identifier
    , _internalName :: Identifier
    }
  deriving (Show, Eq)
```

The `TypeContext` and `LocalType` are stored as a tuple. Really, this gives a cursor into the local type, where everything to the left is the past and everything to the right is the future.

The next two fields are for keeping track of recursion in the local type. the `recursiveVariableNumber` is an index into the `recursionPoints` list: when a `RecursionVariable` is encountered we look at that index to find the new future local type.

Then follow two fields used for reversibility: the stack of used variable names and the store of function applications. Finally there is a variable store with the currently defined bindings.

With this data structure in place, we can define `ExecutionState`. It contains some counters for generating unique variable names, a monitor for every participant and a program for every location. Additionally every location has a default participant and a stack for unchosen branches.

```
data ExecutionState value =
  ExecutionState
    { variableCount :: Int
    , locationCount :: Int
    , applicationCount :: Int
    , participants :: Map Participant (Monitor value String)
```

```

    , locations :: Map Location
      (Participant , List OtherOptions , Program value)
    , queue :: Queue value
    , isFunction :: value -> Maybe (Identifier, Program value)
  }

```

The message queue is global and thus also lives in the `ExecutionState`. Finally we need a way of peeking into values, to see whether they are functions and if so, to extract their bodies for application.

3.1 Running and Debugging Programs

Finally, we want to be able to run our programs.

We use a simple round-robin scheduler that calls `forward` on the locations in order. There are two error cases that we need to handle:

- **blocked on receive**, either `InvalidQueueItem` or `EmptyQueue`: the process wants to perform a receive, but the expected item is not at the top of the queue yet. In this case we want to proceed evaluating the other locations so they can send the value that the erroring location expects
- **location terminates** with `Terminated`: the execution has reached a `NoOp`. In this case we don't want to schedule this location any more.

Otherwise we just continue until there are no active (non-terminated) locations left. For code see appendix [J](#)

3.2 Properties of Reversibility

The main property that reversing needs to preserve is *causal consistency*: the state that we reach when moving backward is a state that could have been reached by moving forward only.

The global type defines a partial order on all the communication steps. The relation of this partial order is causal dependency. Stepping backward may not undo an action until all its causally dependent actions are undone. This guarantee is baked into every part of the semantics. For instance, a send can only be undone when the receive is already undone, because there is a data dependency between the two actions (the sent value).

As such, we argue that *causal consistency* is preserved by our implementation.

4 Convenient Syntax with the Free Monad

The types we have defined for `Program`, `GlobalType` and `LocalType` form recursive tree structures. Because they are all new types, there is no easy way to traverse them. A common idiom is to factor out recursion using `Data.Fix` (see appendix F).

While a `Fixed` data type is easy to manipulate and traverse, it is even more messy to write. The program below implements “receive and bind the value to `result`, then send 42”:

```
program =
  Fix
    ( Receive
      { owner = "Alice"
      , variableName = "result"
      , continuation =
          Fix
            ( Send
              { owner = "Alice"
              , value = VInt 42
              , continuation = Fix NoOp
              }
            )
          }
    )
```

The syntax distracts from the goal of the program, the code is not clear at all. `Program` and `GlobalType` are types that we will write a lot manually, so fixing this issue is important.

Luckily, Haskell has a long tradition of embedded domain-specific languages. In particular we can use a cousin of `Fix`, the `Free` monad (appendix H) to get access to `do`-notation (appendix B). Concretely, the `do`-notation makes it possible instead of the above write

```
program = compile "Alice" $ do
  result <- receive
  send (VInt 42)
  terminate
```

Behind the scenes, the `do`-notation produces a value of type `HighLevelProgram` a using some helpers like `send` and `terminate`.

```
newtype HighLevelProgram a = HighLevelProgram
  (StateT (Participant, Int) (Free (ProgramF Value))) a)
```

```

    deriving
      ( Functor, Applicative, Monad
      , MonadState (Participant, Int)
      , MonadFree (ProgramF Value)
      )

send :: Value -> HighLevelProgram ()
send value = do
  (participant, _) <- State.get
  liftF (Send participant value ())

terminate :: HighLevelProgram a
terminate = liftF NoOp

-- similar for receive, select, etc.

```

The above snippet introduces a couple haskell concepts that we have not seen before and that require some background.

Functional languages can simulate mutable state using a type called the **State** (appendix E). **State** is an instance of monad (appendix C). In this case our piece of state is a pair (**Participant**, **Int**): the participant is the owner of the block, and the **Int** is a counter used to generate unique variable names. To combine **State** with **Free** (and to combine two monads in general) we need the **StateT** monad transformer (appendix E).

In the **send** helper we use the unit type **()** as a placeholder or hole. A continuation will need to fill the hole eventually but it's not available yet. When a **HighLevelProgram** is cast down into a **Program**, we want to be sure there are no remaining holes. In this particular case that means all branches must end in **terminate**. We use the fact that **terminate :: HighLevelProgram a** contains a free type variable **a** which can unify with **Void**, the type with no values. Thus **Free f Void** can contain no **Pure** because the **Pure** constructor needs a value of type **Void**, which don't exist. For more information see appendix I.

5 Discussion

5.1 Benefits of pure functional programming

It has consistently been the case that sticking closer to the formal model gives better code. The abilities that Haskell gives for directly specifying formal state-ments is invaluable. The main killer feature is algebraic data types (ADTs) also known as tagged unions or sum types.

Observe the formal definition and the Haskell data type for global types.

$$G, G' ::= p \rightarrow q : \langle U \rangle . G \mid p \rightarrow q : \{l_i : G_i\}_{i \in I} \mid \mu X . G \mid X \mid \text{end}$$

```
data GlobalTypeF u next =
  Transaction {..} | Choice {..} | R next | V | End | Wk next
```

They correspond directly. Moreover, we know that these are all the ways to construct a value of type `GlobalTypeF` and can exhaustively match on all the cases. Functional languages have had these features for a very long time. In recent years they have also made their way into non-functional languages (Rust, Swift, Kotlin).

Secondly, purity and immutability are very valuable in implementing and testing reversibility. The type system can actually guarantee that we have not forgotten to revert anything.

In a pure language, given functions $f :: a \rightarrow b$ and $g :: b \rightarrow a$ to prove that f and g are inverses it is enough to prove that $f \circ g = \text{identity} \ \&\& \ g \circ f = \text{identity}$. In an impure language, we can never be sure that the outside world is not mutated. Because we don't need to consider a context here, checking that reversibility works is as simple as comparing initial and final states for all transitions.

5.2 Concurrent Debuggers

As mentioned we initially also set out to investigate how useful PPDP semantics are for debugging concurrent programs. As it stands, there are two missing features

1. Modifying concurrent control flow

That is, a way to specify which thread will (try to) take a step forward next. The problem with concurrency is not so much technical: the primitives are available. What is needed is some way to step through a program one instruction at a time. The real challenge is providing a convenient mechanism for doing so, which brings us to

2. Convenient user interface

CaReDeb provides a command line interface. While CaReDeb is interesting from a technical point of view, its interface is not friendly. Additionally, the overhead of bringing the problem into CaReDeb's language is large: more time is probably spent translating than actually debugging.

We think that a good graphical interface is possible, but besides technical features a good user experience also needs user feedback. This means that we

need to look for users and concrete use cases. It would help if there were some concrete set of problems that could be extracted from code, compiled into a format/language that our debugger understands and then visually debugged. Performance can then be evaluated based on how well the debugger solves real-world problems.

6 Conclusion

we have given an encoding of the PPDP semantics in the Haskell programming language. By embedding the semantics we can now run and verify our example programs automatically and inspect them interactively.

We have seen that the PPDP semantics can be split into three core components: a process calculus, multiparty session types and reversibility. Additionally, all three of these are representable as recursive haskell data types. All other features of PPDP (the authors note decoupled rollbacks and abstraction passing, including delegation) can easily be integrated when these three types are established.

Relatedly, the implementation process has shown that sticking to the formal implementation leads to better code. There is less space for bugs to creep in. Furthermore, Haskell's mathematical nature means that the implementation inspired by the formal specification is easy (and often idiomatic) to express.

We have seen that Haskell allows for the definition of flexible embedded domain-specific languages, and makes it easy to transform between different representations of our programs using among others `Monad.Free`.

Finally, we've discussed how this implementation can be used for concurrent debugging.

With more focus on the user experience, a solid concurrent debugging can be built on the foundations presented here.

References

1. C. A. Mezzina and J. A. Pérez. Causally consistent reversible choreographies: a monitors-as-memories approach. In *Proceedings of the 19th International Symposium on Principles and Practice of Declarative Programming, Namur, Belgium, October 09 - 11, 2017*, pages 127–138, 2017.
2. R. Milner. Functions as processes. *Mathematical structures in computer science*, 2(2):119–141, 1992.
3. F. van Walree. Session types in cloud haskell. Master's thesis, 2017.

7 Appendix

Background information on Haskell syntax and concepts used in the thesis.

A Performing IO in Haskell

One of Haskell's key characteristics is that it is pure. This means that our computations can't have any observable effect to the outside world. Purity enables us to reason about our programs (referential transparency) and enables compiler optimizations.

But we use computers to solve problems, and we want to be able to observe the solution to our problems. Pure programs cannot produce observable results: The computer becomes very hot but we can't see our solutions.

So we perform a trick: we say that constructing our program is completely pure, but evaluating may produce side-effects like printing to the console or writing to a file. To separate this possibly effectful code from pure code we use the type system: side-effects are wrapped in the `IO` type.

```
-- print a string to the console
putStrLn :: String -> IO ()

-- read a line of input from the console
readLn :: IO String
```

A consequence of having no observable effects is that the compiler can reorder our code for faster execution (for instance by minimizing cache misses). But this will wreak havoc when performing IO: we want our IO actions to absolutely be ordered.

The trick we can pull here is to wrap the later actions in a function taking one argument, and piping the result of the first action into that function. The result is only available when the first action is done, so the first action is always performed before the rest: we have established a data-dependency between the first and the remaining actions that enforces the order.

The piping is done by the `>>=` operator. In the Haskell literature this function is referred to as `bind`, but I think the elm name `andThen` is more intuitive (at least for IO). A program that first reads a line and then prints it again can be written as

```
main =
    readLn >>= (\line -> putStrLn line)

andThen :: IO a -> (a -> IO b) -> IO b
andThen = (>>=)

main2 = do
    readLn `andThen` (\line -> putStrLn line)
```

The `putStrLn` can only be evaluated when `line` is available, so after `readLn` is done. More technically the `(>>=) :: IO a -> (a -> IO b) -> IO b` operator will first evaluate its first argument `IO a`, in this case `IO String` (that string is the line we have read). Then it “unwraps” that `IO String` to `String` to give it as an argument to `a -> IO b` (here `String -> IO ()`). Note that we can never (safely) go from `IO a -> a`. The unwrapping here is only valid because the final return type is still `IO something`.

When printing two lines, we can use a similar trick to force the order

```
main =  
    putStrLn "hello " >>= (\_ -> putStrLn "world")
```

Here we ignore the result of the first `putStrLn`, but the second `putStrLn` still depends on its return value. Thus it has to wait for the first `putStrLn` to finish before it can start.

B Do-notation

Writing nested functions in this way quickly becomes tedious. That is why special syntax is available: do-notation

```
main1 = do  
    line <- readLn  
    putStrLn line  
  
main2 = do  
    putStrLn "hello "  
    putStrLn "world"
```

do-notation is only syntactic sugar: it is translated by the compiler to the nested functions that we have seen above. The syntax is very convenient however. Additionally, we can use it for all types that implement `>>=`: all instances of the `Monad` typeclass.

C Monads

`Monad` is a Haskell typeclass (and a concept from a branch of mathematics called category theory). Typeclasses are sets of types that implement some functions, similar to interfaces or traits in other languages.

The monad typeclass defines two methods: `bind`/`andThen`/`>>=` which we have seen and `return :: Monad m => a -> m a`. The `Monad m =>` part of the signature constrains the function to only work on types that have a `Monad` instance.

I hope the above already gives some intuition about monad's main operator `>>=`: it forces order of evaluation. A second property is that `Monad` can merge contexts with `join :: Monad m => m (m a) -> m a`. A common example of `join` is `List.concat :: List (List a) -> List a`. A bit more illustrative is the implementation for `Maybe`

```
join :: Maybe (Maybe a) -> Maybe a
join value =
  case value of
    Nothing ->
      Nothing

    Just (Nothing) ->
      Nothing

    Just (Just x) ->
      Just x
```

If the outer context has failed (is `Nothing`), then the total computation has failed and there is no value of type `a` to give back. If the outer computation succeeded but the inner one failed, there is still no `a` and the only thing we can return is `Nothing`. Only if both the inner and the outer computations have succeeded can we give a result back.

In short

- `Monad` is a Haskell typeclass
- it has two main functions
 - `bind` or `andThen` or `>>= :: Monad m => m a -> (a -> m b) -> m b`
 - `return :: Monad m => a -> m a`
- `Monad` forces the order of operations and can flatten wrappers
- `Monad` allows us to use `do`-notation
- `IO` is an instance of `Monad`

Much material on the web about monads is about establishing the general idea, but really the exact meaning of `>>=` can be very different for every instance. Next we'll look at some of the types used in the code for this thesis.

D Except

`Except` is very similar to `Either`:

```
data Either a b
  = Left a
  | Right b
```

We use this type to throw and track errors in a pure way.

```
throwError :: e -> Except e a

data Error
  = QueueEmpty
  | ...

popQueue :: List a -> Except Error (a, List a)
popQueue queue =
  case queue of
    [] ->
      Except.throwError QueueEmpty

    x : xs ->
      return ( x, xs )
```

Except and Either have a `Monad` instance. In this context `return` means a non-error value, and `>>=` allows us to chain multiple operations that can fail, stopping when an error occurs.

E State and StateT

`State` is a wrapper around a function of type `s -> (a, s)`

```
newtype State s a = State { unState :: s -> (a, s) }
```

It is used to give the illusion of mutable state, while remaining completely pure. Intuitively, we can compose functions of this kind.

```
f :: s -> (a, s)
g ::      a -> s -> (b, s)
-- implies
h :: s ->      (b, s)
```

And this is exactly what monadic `bind` for state does.

```
andThen :: State s a -> (a -> State s b) -> State s b
andThen (State first) tagger =
  State $ \s ->
    let (value, newState) = first s
    in State second = tagger value
```



```

        in
            second newState

new :: a -> State s a
new value = State (\s -> (value, s))

instance Monad (State s) where
    (>>=) = andThen
    return = new

```

When we want to combine monads, for instance to have both state and error reporting, we must use monad transformers. The transformer is needed because monads don't naturally combine: `m1 (m2 a)` may not have a law-abiding monad instance.

```

newtype StateT s m a = StateT { runStateT :: s -> m (a, s) }

instance MonadTrans (StateT s) where
    lift :: (Monad m) => m a -> StateT s m a
    lift m = StateT $ \s -> do
        a <- m
        return (a, s)

instance (Monad m) => Monad (StateT s m) where
    return a = StateT $ \s -> return (a, s)

```

The `MonadTrans` typeclass defines the `lift` function that wraps a monadic value into the transformer. Next we define an instance because we can say “given a monad `m`, `StateT s m` is a law-abiding monad.

F Factoring out recursion

A commonly used idiom in our code is to factor out recursion from a data structure, using the `Fix` and `Monad.Free` types. Both require the data type to be an instance of `Functor`: The type is of the shape `f a` - like `List a` or `Maybe a`, and there exists a mapping function `fmap :: (a -> b) -> (f a -> f b)`.

`Fix` requires the data type to have a natural leaf: a constructor that does not contain an `a`. `Free` on the other hand lets us choose some other type for the leaves.

G Fix

The `Fix` data type is the fixed point type.

```
data Fix f = Fix (f (Fix f))
```

It allows us to express a type of the shape `f (f (f (f (...)))` concisely. For the values of this type to be finite, the `f` must have a constructor that does not recurse to be a leaf. Take for instance this simple expression language

```
data Expr
  = Literal Int
  | Add Expr Expr
```

`Literal` is the only constructor that can occur as a leaf, and `Add` is the only node. Using `Fix` We can equivalently write

```
data ExprF next
  = Literal Int
  | Add next next

simple :: Fix ExprF
simple = Fix (Literal 42)

complex :: Fix ExprF
complex =
  Fix (Add (Fix (Literal 40)) (Fix (Literal 2)))
```

By decoupling the recursion from the content, we can write functions that deal with only one level of the tree and apply them to the full tree. For instance evaluation of the above expression can be written as

```
evaluate :: Fix ExprF -> Int
evaluate =
  Fix.cata $ \expr ->
    case expr of
      Literal v ->
        v

      Add a b ->
        a + b
```

The `cata` function - a catamorphism also known as a fold or reduce - applies evaluate from the bottom up. In the code we write, we only need to make local decisions and don't have to write the plumbing to get the recursion right.

H Monad.Free

The Free monad is very similar to `Fix`, but allows us to use a different type for the leaves, and enables us to use do-notation. Writing expressions with `Fix` can be quite messy, free monads allow us to write examples much more succinctly.

Free is defined as

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

and as the name suggests `Monad.Free` has a `Monad` instance.

This then makes it possible to define a functor that represents instructions, define some helpers and then use do-notation to write our actual programs.

```
data StackF a next
  = Push a next
  | Pop (a -> next)
  | End
  deriving (Functor)

type Stack a = Free StackF a

program :: Stack Int
program = do
  push 5
  push 4
  a <- pop
  b <- pop
  push (a + b)

push :: a -> Stack a ()
push v = liftFree (Push v ())

pop :: Stack a a
pop = liftFree (Pop identity)
```

I Guaranteeing well-formedness of Free

We use the free monad to build up programs and global types. A problem with the free monad is that the built-up tree can still contain “holes” because of the `Pure _` branch of `Free`. That is fine while constructing the tree, but when

evaluating it we want all Pures to be gone. There are two ways of enforcing this constraint using the type systems.

We observe that only our leaves have a free type variable. For instance for `HighLevelProgram`, only `terminate` (via `NoOp`) can have type `HighLevelProgram a` where the `a` is unbound. That means that `terminate` will unify with anything: `HighLevelProgram String`, `HighLevelProgram Int`, etc.

```
terminate :: HighLevelProgram a
terminate = HighLevelProgram (liftF NoOp)
```

There are now two ways forward:

Solution 1: Rank2Types and Universal Quantification

Now if we enforce that our whole program unifies with anything, that implies that all Pures are gone from the structure. Normally, type signatures are valid if there is at least one valid unification for every type variable (i.e. existential quantification). But with the language extension `ExplicitForAll` we can mark type variables as universally quantified: they need to unify with all types. In this case we also need `Rank2Types` because of the position where we want to use `forall`.

```
{-# LANGUAGE Rank2Types #-}
{-# LANGUAGE ExplicitForAll #-}

compile :: Participant -> (forall a. HighLevelProgram a) -> Program Value
compile participant (HighLevelProgram program) = ...
```

Solution 2: Data.Void

The second solution is to use `Data.Void`. `Void` is the data type with zero values, which means there is no valid way of creating a value of type `Void`. Thus a `Free f Void` cannot have any Pures, because they need a value of type `Void` and there are none.

```
import Data.Void (Void)

compile :: Participant -> HighLevelProgram Void -> Program Value
compile participant (HighLevelProgram program) = ...
```

Tradeoffs

In the codebase we went with solution 2 because it produces clearer error messages and doesn't introduce extra language extensions to the project.

J Scheduling code

```
data Progress = Progress | NoProgress deriving (Eq, Show)

round :: List Location -> ExecutionState Value
      -> Either Error ( List (Location, Progress)
                      , ExecutionState Value
                      )

round locations state =
  foldM helper [] locations
    |> flip State.runStateT state
    |> Except.runExcept
  where helper :: List (Location, Progress) -> Location
        -> Session Value (List (Location, Progress))
        helper accum location = do
          state <- State.get

          let evaluated =
              State.runStateT (forward location) state
              |> Except.runExcept

          case evaluated of
            Right ( _, s ) -> do
              State.put s
              return $ ( location, Progress ) : accum

            Left (QueueError origin (InvalidQueueItem message)) ->
              -- blocked on receive, try moving others forward
              return $ ( location, NoProgress ) : accum

            Left (QueueError origin EmptyQueue) ->
              -- blocked on receive, try moving others forward
              return $ ( location, NoProgress ) : accum

            Left Terminated ->
              return accum

            Left err ->
              -- other errors are raised
              Except.throwError err

untilError :: ExecutionState Value
           -> Either Error (ExecutionState Value)
untilError state@ExecutionState{ locations } =
```

```

    helper (Map.keys locations) state
where helper locations state = do
    ( locationProgress, newState ) <-
        Interpreter.round locations state

    let isProgress =
        any
            (\(_, progress) -> progress == Progress)
            locationProgress

    if null locationProgress then
        -- no active locations
        Right state

    else if then
        helper (List.map fst locationProgress) newState

    else
        error $ "DEADLOCK\n" ++ show state

```