ABSTRACT

Static type systems are the most common form of program verification. In their most basic form, type systems guarantee that a computation always returns a value of some type. The work on monads and effect systems extends type systems to guarantee properties about *effectful computations* that perform side-effects like non-termination, I/O operations or exceptions.

In this thesis we extend type systems to guarantee properties about *context-dependent computations*. Such computations are increasingly common in modern software. For example, applications accessing data need to guarantee that the right data is available and distributed systems need to guarantee that resources are available on specific nodes.

We develop three *coeffect* type systems that are capable of capturing different context-dependent properties. All three systems are based on the unifying semantic structure called *indexed comonads*, but they use it differently.

Our *flat coeffect calculus* tracks one annotation about the entire context. It can be used to keep a set of required resources or a set of supported platforms. Our *structural coeffect calculus* tracks one annotation for each variable. It can be used to track liveness of variables or number of past values needed in data-flow computations. Finally, our *coeffect meta-language* embeds contextual values directly into a language. It can be used to guarantee security properties of computations by using tainting.

CONTENTS

1 INTRODUCTION

Some intro

1.1 HOW LAMBDA WORKS

The key difference - how lambda works

Effect systems, introduced by Gifford and Lucassen [24], track *effects* of computations, such as memory access or message-based communication [30]. Their approach augments typing judgments with effect information: $\Gamma \vdash e : \tau, F$. Wadler and Thiemann explain how this shapes effect analysis of lambda abstraction [70]:

> *In the rule for abstraction, the effect is empty because evaluation immediately returns the function, with no side effects. The effect on the function arrow is the same as the effect for the function body, because applying the function will have the same side effects as evaluating the body.*

In contrast to the static analysis of *effects*, the analysis of *context-dependence* does not match this pattern. In the systems we consider, lambda abstraction places requirements on both the *call-site* (latent requirements) and the *declaration-site* (immediate requirements), resulting in different syntactic properties. We informally discuss three examples first that demonstrate how contextual requirements propagate. Section ? then unifies these in a single calculus.

Also [55]

> *We will define an effect as a producer effect if all computations with that effect can be thunked as "pure" computations for a domain-specific notion of purity.*

Demonstrate using distributed computations
Demonstrate using dataflow/liveness
Perhaps mention LINQ as a motivation for cross-compilation.. [35]

1.2 ASSOCIATING WITH CONTEXT

-> Type providers make this important

1.3 FLAT COEFFECT SYSTEM

resources?

1.4 STRUCTURAL COEFFECT SYSTEM

The *flat coeffect system* presented in the previous sections has a number of uses, but often we need to track context-dependence in a more fine-grained

way. To track neededness or security, we need to associate information with individual *variables* of the context.

At the same time, we want to avoid developing multiple variants of coeffect systems – indeed, our motivation is to develop a *single unified mechanism* for tracking context-dependence. In this section, we present a more powerful *structural coeffect calculus*, which is a generalization of the flat calculus.

1.4.1 *Motivation: Tracking array accesses*

Similarly to the flat version, the *structural coeffect calculus* works with contexts and functions annotated with a coeffectt tags, written $C^r\Gamma$ and $C^r\tau_1 \to \tau_2$, respectively, but we use richer tag structure.

As an example, consider a language that allows us to get a value of a variable (representing some changing data-source) x versions back using the syntax $a_{[x]}$. To track information about individual variables, we use a product-like operation $\times$ on tags to mirrors the product structure of variables. For example:

$$C^{5\times 10}(a : \mathsf{D}_{\mathsf{nat}}, b : \mathsf{D}_{\mathsf{nat}}) \vdash a_{[5]} + b_{[10]} : \mathsf{nat}$$

The coeffect tag 5×10 corresponds to the free-variable context a, b, denoting that we need at most 5 and 10 past values of a and b. If we substitute c for both a and b, we need another operation to combine multiple tags associated with a single variable:

$$C^{5\ \mathsf{max}\ 10}(c : \mathsf{D}_{\mathsf{nat}}) \vdash c_{[5]} + c_{[10]} : \mathsf{nat}$$

In this example, the operation max would be the *max* function and so $5\ \mathsf{max}\ 10 = 10$. Before looking at the formal definition, consider the typing of let bindings:

$$\textbf{let}\ c = \textbf{if}\ \mathsf{test}()\ \textbf{then}\ a\ \textbf{else}\ b$$
$$a_{[15]} + c_{[10]}$$

The expression has free variables a and b (we ignore test, which is not a data source). It defines c, which may be assigned either a or b. The variable a may be used directly (second line) or indirectly via c.

The expression assigned to c uses variables a and b, so its typing context is $C^{0\times 0}(a, b)$. The value 0 is the unit of max and it denotes empty coeffect. The typing context of the body is $C^{15\times 10}(a, c)$.

To combine the tags, we take the coeffect associated with c and apply it to the tags of the context in which c was defined using the max operation. This is then combined with the remaining tags from the body yielding the overall context: $C^{15\times(10\ \mathsf{max}\ (0\times 0))}(a, (a, b))$. Using a simple normalization mechanism (described later), this can be further reduced to $C^{(15\ \mathsf{max}\ 10)\times 10}(a, b)$. This gives us the required information – we need at most $max(15, 10)$ past values of a and at most 10 past values of b.

1.5 CONTRIBUTIONS

2 PATHWAYS TO COEFFECTS

There are many different directions from which the concept of *coeffects* can be approached and, indeed, discovered. In the previous chapter, we motivated it by practical applications, but coeffects also naturally arise as an extension to a number of programming language theories. Thanks to the Curry-Howard-Lambek correspondence, we can approach coeffects from the perspective of type theory, logic and also category theory. This chapter gives an overview of the most important directions.

We start by revisiting practical applications and existing language features that are related to coeffects (Section 2.1), then we look at coeffects as the dual of effect systems (Section 2.2) and extend the duality to category theory, looking at the categorical dual of monads known as *comonads* (Section 2.3). Finally we look at logically inspired type systems that are closely related to our structural coeffects (Section 2.4).

This chapter serves two purposes. Firstly, it provides a high-level overview of the related work, although technical details are often postponed until later. Secondly it recasts existing ideas in a way that naturally leads to the coeffect systems developed later in the thesis. For this reason, we are not always faithful to the referenced work – sometimes we focus on aspects that the authors consider unimportant or present the work differently than originally intended. The reason is to fulfil the second goal of the chapter. When we do so, this is explicitly said in the text.

2.1 THROUGH APPLICATIONS

The general theme of this thesis is improving programming languages to better support writing *context-dependent* (or *context-aware*) computations. With current trends in the computing industry such as mobile and ubiquitous computing, this is becoming an important topic. In software engineering and programming community, a number of authors have addressed this problem from different perspectives. Hirschfeld et al. propose *Context-Oriented Programming* (COP) as a methodology [29], and the subject has also been addressed in mobile computations [7, 17]. In programming languages, Costanza [13] develops a domain-specific LISP-like language ContextL and Bardram [5] proposes a Java framework for COP.

We approach the problem from a different perspective, building on the tradition of statically-typed functional programming languages and their theories. However, even in this field, there is a number of calculi or language features that can be viewed as context-dependent.

2.1.1 *Motivation for flat coeffects*

In a number of systems, the execution environment provides some additional data, resources or information about the execution context, but are independent of the variables used by the program. We look at implicit parameters and rebindable resources (that both provide additional identifiers that can be accessed similarly to variables, but follow different scoping rules), distributed programming, cross-compilation and data-flow.

IMPLICIT PARAMETERS In Haskell, implicit parameters [32] are a special kind of variables that may behave as dynamically scoped. This means, if a function uses parameter ?p, then the caller of the function must define ?p and set its value. Implicit parameters can be used to parameterise a computation (involving a chain of function calls) without passing parameters explicitly as additional arguments of all involved functions. A simple language with implicit parameters has an expression ?p to read a parameter value and an expression[1] **letdyn** ?p = e_1 **in** e_2 that sets a parameter ?p to the value of e_1 and evaluates e_2 in a context containing ?p

An interesting question arises when we use implicit parameters in a nested function. The following function does some pre-processing and then returns a function that builds a formatted string based on two implicit parameters ?width and ?size:

```
let format = λstr →
  let lines = formatLines str ?width in
  (λrest → append lines rest ?width ?size)
```

The body of the outer function accesses the parameter ?width, so it certainly requires a context {?width : int}. The nested function (returned as a result) uses the parameter ?width, but in addition also uses ?size. Where should the parameters of the nested function come from?

In a purely dynamically scoped system, they would have to be defined when the user invokes the nested function. However, in Haskell, implicit parameters behave as a combination of lexical and dynamic scoping. This means that the nested function can capture the value of ?width and require just ?size In Haskell, this corresponds to the following type:

```
(?width :: Int) ⇒ String → ((?size :: Int) ⇒ String → string)
```

As a result, the function can be called as follows:

```
let formatHello =
  ( letdyn ?width = 5 in
    format "Hello") in
letdyn ?size = 10 in formatHello "world"
```

This way of assigning type to format and calling it is not the only possible, though. We could also say that the outer function requires both of the implicit parameters and the result is a (pure) function with no context requirements. This interaction between implicit parameters and lambda abstraction demonstrates one of the key aspects of coeffects and will be discussed later. Implicit parameters will also sever as one of our examples in Chapter Y.

TYPE CLASSES Implicit parameters are closely related to *type classes* [69]. In Haskell, type classes provide a principled form of ad-hoc polymorphism (overloading). When a code uses an overloaded operation (e.g. comparison or numeric operators) a constraint is placed on the context in which the operation is used. For example:

```
twoTimes :: Num α ⇒ α → α
twoTimes x = x + x
```

The constraint Num a on the function type arises from the use of the + operator. From the implementation perspective, the type class constraint means

1 Haskell uses **let** ?p = e_1 **in** e_2, but we use a different keyword to avoid confusion.

that the function takes a hidden parameter – a dictionary that provides the operation $+ :: \alpha \to \alpha \to \alpha$. Thus, the type $\mathsf{Num}\ \alpha \Rightarrow \alpha \to \alpha$ can be viewed as $(\mathsf{Num}_\alpha \times \alpha) \to \alpha$. Implicit parameters work in exactly the same way – they are passed around as hidden parameters.

The implementation of type classes and implicit parameters shows two important points about context-dependent properties. First, they are associated with some *scope*, such as the body of a function. Second, they are associated with the input. To call a function that takes an implicit parameter or has a type-class constraint, the caller needs to pass a (hidden) parameter together with the function inputs.

REBINDABLE RESOURCES The need for parameters that do not strictly follow static scoping rules also arises in distributed computing. This problem has been addressed, for example, by Bierman et al. and Sewell et al. [8, 49]. To quote the first work: *"Dynamic binding is required in various guises, for example when a marshalled value is received from the network, containing identifiers that must be rebound to local resources."*

This situation arises when marshalling and transferring function values. A function may depend on a local resource (e.g. a database available only on the server) and also resources that are available on the target node (e.g. current time). In the following example, the construct **access** Res represents access to a re-bindable resource named Res:

```
let recentEvents = λ() →
  let db = access News in
  query db "SELECT * WHERE Date > %1" (access Clock)
```

When recentEvents is created on a server and sent to a client, a remote reference to the database (available only on the server) must be captured. If the client device supports a clock, then Clock can be locally *rebound*, e.g., to accommodate time-zone changes. Otherwise, the date and time needs to be obtained from the server too.

The use of re-bindable resources creates a context requirement similar to the one arising from the use of implicit parameters. For function values, such context-requirements can be satisfied in different ways – resources must be available either at the declaration site (i.e. when a function is created) or at the call site (i.e. when a function is called).

DISTRIBUTED COMPUTING AND MULTI-TARGETTING An increasing number of programming languages is capable of running across multiple different platforms or execution environments. Functional programming languages that can be compiled to JavaScript (to target web and mobile clients) include, among others, F#, Haskell and OCaml [64].

Links [12], F# libraries [53, 43], ML5 and QWeSST [37, 48] and Hop [33] go further and allow a single source program to be compiled to multiple target runtimes. This posses additional challenges – it is necessary to track where each part of computation runs and statically guarantee that it will be possible to compile code to the required target platform (safe *multi-targetting*).

We demonstrate the problem by looking at input validation. In distributed applications that communicate over unsecured HTTP channel, user input needs to be validated interactively on the client-side (to provide immediate response) and then again on the server-side (to guarantee safety). For example:

```
let validateInput = λname →
  name ≠ "" && forall isLetter name

let displayProduct = λname →
  if validateInput name then displayProductPage name
  else displayErrorPage ()
```

The function validateInput can be compiled to both JavaScript (for client-side) and native code (for server-side). However, displayProduct uses other functionality (generating web pages) that is only available on the server-side, so it can only be compiled to native code.

In Links [12], functions can be annotated as client-side, server-side and database-side. F# WebTools [43] adds functions that support multiple targets (mixed-side). However, these are single-purpose language features and they are not extensible. For example, in modern mobile development it is also important to track minimal supported version of runtime[2].

Requirements on the execution environment can be viewed as contextual properties, but could be also presented as effects (use of some API required only in certain environment is a computational effect). We discuss the difference in Section X. Furthermore, the theoretical foundations of distributed languages like ML5 [37] suggest that a contextual treatment is more appropriate. We return to ML5 when discussing semantics in Section 2.3.3.

SAFE LOCKING In the previous examples, the context provides additional values or functions that may be accessed at runtime. However, it may also track *permissions* to perform some operation. This is done in the type system for safe locking of Flanagan and Abadi [20].

The system prevents race conditions (by only allowing access to mutable state under a lock) and avoids deadlocks (by imposing strict partial order on locks). The following program uses a mutable state under a lock:

```
newlock l : ρ in
let state = ref_ρ 10 in
sync l (!state)
```

The declaration **newlock** creates a lock l protecting memory region ρ. We can than allocate mutable variables in that memory region (second line). An access to mutable variable is only allowed in scope that is protected by a lock. This is done using the **sync** keyword, which locks a lock and evaluates an expression in a context that contains permission to access memory region of the lock (ρ in the above example).

The type system for safe locking associates the list of permission with the variable context. It uses judgements of a form $\Gamma, m \vdash e : \alpha$ specifying that an expression has a type in context Γ, given permissions (a list of locked regions) m. However, the treatment of lambda abstraction differs from the one for implicit parameters or rebindable resources. In the system for locking, code inside lambda function cannot use permissions from the scope where the function is declared. This is a necessary requirement – a lambda function created under a lock cannot access protected memory, because it will be executed later. We discuss how this restriction fits into our general coeffect framework in Section X.Y.

2 Android Developer guide [16] demonstrates how difficult it is to solve the problem without language support.

DATA-FLOW LANGUAGES The examples discussed so far are all – to some extent – similar. They attach additional information (implicit parameters, dictionaries) or restrictions (on execution environment) to the context where code evaluates. By *context*, we mean, most importantly, the values of variables and declarations that are in scope. The examples so far add more information to the context, but do not operate on the variable values.

Data-flow languages provide a different example. Lucid [66] is a declarative data-flow language designed by Wadge and Ashcroft. In Lucid, variables represent streams and programs are written as transformations over streams. A function application *square*(a) represents a stream of squares calculated from the stream of values a.

The data-flow approach has been successfully used in domains such as development of real-time embedded application where many *synchronous languages* [6] build on the data-flow paradigm. The following example is inspired by the Lustre [25] language and implements program to count the number of edges on a Boolean stream:

```
let edge = false fby (input && not (prev input))

let edgeCount =
  0 fby ( if edge then prev edgeCount
          else prev edgeCount )
```

The construct **prev** x returns a stream consisting of previous values of the stream x. The second value of **prev** x is first value of x (and the first value is undefined). The construct y **fby** x returns a stream whose first element is the first element of y and the remaining elements are values of x. Note that in Lucid, the constants such as false and 0 are constant streams. Formally, the construct are defined as follows (writing x_n for n-th element of a stream x):

$$(\textbf{prev}\ x)_n = \begin{cases} nil & \text{if } n = 0 \\ x_{n-1} & \text{if } n > 0 \end{cases} \qquad (y\ \textbf{fby}\ x)_n = \begin{cases} y_0 & \text{if } n = 0 \\ x_n & \text{if } n > 0 \end{cases}$$

When reading data-flow programs, we do not need to think about variables in terms of streams – we can see them as simple values. However, the operations **fby** and **prev** cannot operate on plain values – they require additional *context* which provides past values of variables (for **prev**) and information about the current location in the stream (for **fby**).

In this case, the context is not simply an additional (hidden) parameter. It completely changes how variables must be represented. We may want to capture various *contextual properties* of Lucid programs. For example, how many past elements need to be cached when we evaluate the stream.

To understand the nature of the context, we later look at the semantics of Lucid. This can be captured using a number of mathematical structures. Wadge [65] originally proposed to use monads, while Uustalu and Vene later used comonads [59].

2.1.2 *Motivation for structural coeffects*

We now turn our attention to system where additional contextual information are associated not with the context as a whole (or program scope), but with individual variables. We start by looking simple static analysis – variable *liveness*. Then we revisit data-flow computations and look at applications in security and software updating.

LIVENESS ANALYSIS *Live variable analysis* (LVA) [3] is a standard technique in compiler theory. It detects whether a free variable of an expression may be used by a program later (it is *live*) or whether it is definitely not needed (it is *dead*). As an optimization, compiler can remove bindings to dead variables as the result is never accessed. Wadler [67] describes the property of a variable that is dead as the *absence* of a variable.

In this thesis, we first use a restricted (and not practically useful) form of liveness analysis to introduce the theory of indexed comonads (Section X) and then use liveness analysis as one of the motivations for structural coeffects. Consider the following two simple functions:

$$\textbf{let}\ \mathsf{constant42} = \lambda \mathsf{x} \rightarrow 42$$

$$\textbf{let}\ \mathsf{constant} = \lambda \mathsf{value} \rightarrow \lambda \mathsf{x} \rightarrow \mathsf{value}$$

In liveness analysis, we annotate the context with a value specifying whether the variables in scope are *live* or *dead*. If we associate just a single value with the entire context, then the liveness analysis is very limited – it can say that the context of the expression 42 in the first function is dead, because no variables are accessed.

A useful liveness analysis needs to consider individual variables. For example, in the body of the second function (value), two variables are in scope. The variable value is accessed and thus is *live*, but the variable x is dead.

Static analyses can be classified as either *forward* or *backward* (depending on how they propagate information) and as either *must* or *may* (depending on what properties they guarantee). Liveness is a *backward* analysis – this means that the requirements propagates from variables to their declaration sites. The distinction between *must* and *may* is apparent when we look at an example with conditionals:

$$\begin{array}{l}\textbf{let}\ \mathsf{defaultArg}\ = \lambda \mathsf{cond} \rightarrow \lambda \mathsf{input} \rightarrow \\ \quad \textbf{if}\ \mathsf{cond}\ \textbf{then}\ 42\ \textbf{else}\ \mathsf{input}\end{array}$$

The liveness analysis is a *may* analysis meaning that it marks variable as live when it *may* be used and as dead if it is *definitely* not used. This means that the variable input is *live* in the example above. A *must* analysis would mark the variable only if it was used in both of the branches (this is sometimes called *neededness*).

The distinction between *may* and *must* analyses demonstrates the importance of interaction between contextual properties and certain language constructs such as conditionals.

DATA-FLOW LANGUAGES (REVISITED) When discussing data-flow languages in the previous section, we said that the context provides past values of variables. This can be viewed as a flat contextual property (the context needs to keep all past values), but we can also view it as a structural property. Consider the following example:

$$\textbf{let}\ \mathsf{offsetZip} = 0\ \textbf{fby}\ (\mathsf{left} + \textbf{prev}\ \mathsf{right})$$

The value offsetZip adds values of left with previous values of right. To evaluate a current value of the stream, we need the current value of left and one past value of right.

As mentioned earlier, a static analysis for data-flow computations could calculate how many past values must be cached. This can be done as a *flat* coeffect analysis that produces just a single number for each function.

However, we can design a more precise *structural* analysis and track the number of required elements for individual variables.

TAINTING AND PROVENANCE Tainting is a mechanism where variables coming from potentially untrusted sources are marked (*tainted*) and the use of such variables is disallowed in contexts where untrusted input can cause security issues or other problems. Tainting can be done dynamically as a runtime mark (e.g. in the Perl language) or statically using a type system. Tainting can be viewed as a special case of *provenance tracking*, known from database systems [11], where values are annotated with more detailed information about their source.

Statically typed systems that based on tainting have been use to prevent cross-site scripting attacks [62] and a well known attack known as SQL injection [27, 26]. In the latter chase, we want to check that SQL commands cannot be directly constructed from, potentially dangerous, inputs provided by the user. Consider the type checking of the following expression in a context containing variables `id` and `msg`:

```
let name = query ("SELECT Name WHERE Id = " + id) in
msg + name
```

In this example, `id` must not come directly from a user input, because `query` requires untainted string. Otherwise, the attacker could specify values such as `"1; DROP TABLE Users"`. The variable `msg` may or may not be tainted, because it is not used in protected context (i.e. to construct an SQL query).

In runtime checking, all (string) values need to be wrapped in an object that stores Boolean flag (for tainting) or more complex data (for provenance). In static checking, the information need to be associated with the variables in the variable context. We use tainting as a motivating example for *structural* coeffects in Section X.

SECURITY AND CORE DEPENDENCY CALCULUS The checking of tainting is a special case of checking of the *non-interference* property in *secure information flow*. Here, the aim is to guarantee that sensitive information (such as credit card number) cannot be leaked to contexts with low secrecy (e.g. sent via an unsecured network channel). Volpano et al. [63] provide the first (provably) sound type system that guarantees non-inference and Sabelfeld et al. [47] survey more recent work. The checking of information flows has been also integrated (as a single-purpose extension) in the FlowCaml [50] language. Finally, Russo et al. and Swamy et al. [46, 52] show that the properties can be checked using a monadic library.

Systems for secure information flow typically define a lattice of security classes $(\mathcal{S}, \leqslant)$ where $\mathcal{S}$ is a finite set of classes and an ordering. For example a set $\{L, H\}$ represents low and high secrecy, respectively with $L \leqslant H$ meaning that low security values can be treated as high security (but not the other way round).

An important aspect of secure information flow is called *implicit flows*. Consider the following example which may assign a new value to z:

```
if x > 0 then z := y
```

If the value of y is high-secure, then z becomes high-secure after the assignment (this is an *explicit* flow). However, if x is high-secure, then the value of z becomes high-secure, regardless of the security level of y, because the fact

whether an assignment is performed or not performed leaks information in its own (this is an *implicit* flow).

Abadi et al. realized that there is a number of analyses similar to secure information flow and proposed to unify them using a single model called Dependency Core Calculus (DCC) [1]. It captures other cases where some information about expression relies on properties of variables in the context where it executes. The DCC captures, for example, *binding time analysis* [56], which detects which parts of programs can be partially evaluated (do not depend on user input) and *program slicing* [57] that identifies parts of programs that contribute to the output of an expression.

2.1.3 *Beyond passive contexts*

In the systems discussed so far, the context provides additional data (resources, implicit parameters, historical values) or meta-data (security, provenance). However, it is impossible to write a function that modifies the context. We use the term *passive* context for such applications.

However, there is a number of systems where the context may be changed – not just be evaluating certain code block in a different scope (e.g. by wrapping it in prev in data-flow), but also by calling a function that, for example, acquires new capabilities. While this thesis focuses on systems with passive context, we quickly look at the most important examples of the *active* variant.

CALCULUS OF CAPABILITIES Crary et al. [14] introduced the Calculus of Capabilities to provide a sound system with region-based memory management for low-level code that can be easily compiled to assembly language. They build on the work of Tofte and Talpin [58] who developed an *effect system* (discussed in Section 2.3.2) that uses lexically scoped *memory regions* to provide an efficient and controlled memory management.

In the work of Tofte and Talpin, the context is *passive*. They extend a simple functional language with the **letrgn** construct that defines a new memory region, evaluates an expression (possibly) using memory in that region and then deallocates the memory of the region:

$$
\begin{aligned}
&\textbf{let}\ \mathsf{calculate} = \lambda \mathsf{input} \rightarrow \\
&\quad \textbf{letrgn}\ \rho\ \textbf{in} \\
&\quad \textbf{let}\ \mathsf{x} = \textbf{ref}_{\rho}\, \mathsf{input}\ \textbf{in}\ !\mathsf{x}
\end{aligned}
$$

The memory region ρ is a part of the context, but only in the scope of the body of **letrgn**. It is only available to the last line which allocates a memory cell in the region and reads it (before the region is deallocated). There is no way to allocate a region inside a function and pass it back to the caller.

Calculus of capabilities differs in two ways. First, it allows explicit allocation and deallocation of memory regions (and so region lifetimes do not follow strict LIFO ordering). Second, it uses continuation-passing style. We ignore the latter aspect and so the following example:

$$
\begin{aligned}
&\textbf{let}\ \mathsf{calculate} = \lambda \mathsf{input} \rightarrow \\
&\quad \textbf{letrgn}\ \rho\ \textbf{in} \\
&\quad \textbf{let}\ \mathsf{x} = \textbf{ref}_{\rho}\, \mathsf{input}\ \textbf{in}\ \mathsf{x}
\end{aligned}
$$

The example is almost identical to the previous one, except that it does not return the value of reference x. Instead, it returns the reference, which is

located in a newly allocated region. Together with the value, the function returns a *capability* to access the region ρ.

This is where systems with active context differ. To type check such programs, we do not only need to know what context is required to call `calculate`. We also need to know what effects it has on the context when it evaluates and the current context meeds to be appropriately adjusted after a function call. We briefly consider this problem in Section X.

SOFTWARE UPDATING Dynamic software updating (DSU) [22, 28] is the ability to update programs at runtime without stopping them. The Proteus system developed by Stoyle et al. [51] investigates what language support is needed to enable safe dynamic software updating in C-like languages. The system is based on the idea of capabilities.

The system distinguishes between *concrete* uses and *abstract* uses of a value. When a value is used concretely, the program examines its representation (and so it is not safe to change the representation during an update). An abstract use of a value does not need to examine the representation and so updating the value does not break the program.

The Proteus system uses capabilities to restrict what types may be used concretely after any point in the program. All other types, not listed in the capability, can be dynamically updated as this will not change concrete representation of types accessed later in the evaluation.

Similarly to Capability Calculus, capabilities in DSU can be changed by a function call. For example, calling a function that may update certain types makes it impossible to use those types concretely following the function call. This means that DSU uses the context *actively* and not just *passively*.

THESIS PERSPECTIVE As demonstrated in this section, there is a huge number of systems and applications that exhibit a form of context-dependence. The range includes different static analyses (liveness, provenance), well-known programming language features (implicit parameters and type classes) as well as features not widely available (e.g. for distributed programming).

It is impossible to cover all of these topics in a single coherent thesis and so we focus on two key aspects:

- **Flat vs. structural.** We look at both flat coeffects (single value for entire context) and structural coeffects (single value per variable). We use liveness, implicit parameters and data-flow to introduce flat coeffects (Section X) and liveness, refined data-flow and tainting to talk about structural coeffects (Section Y).
- **Analysis vs. restriction.** Some of the discussed examples can be viewed as static analyses that obtain some information about programs (i.e. the number of required past values in data-flow). Other examples provide type system that rules out certain invalid programs (e.g. safe locking). We cover this topic when discussing *partial coeffects* in Section Z.
- **May vs. must analysis.** When discussing liveness, we observed that we can obtain two different analyses depending on how conditionals are treated. We discuss this topic in Section X.

Although we also looked at examples of *active* contextual computations (where developers can write functions that modify the context), we do not consider these applications, to keep the material presented in this thesis focused. We briefly discuss them as future work in Section X.

$$\text{(var)}\frac{x : \alpha \in \Gamma}{\Gamma \vdash x : \alpha, \emptyset} \qquad \text{(write)}\frac{\Gamma \vdash e : \alpha, \sigma \quad l : \mathsf{ref}_\rho\ \alpha \in \Gamma}{\Gamma \vdash l \leftarrow e : \mathsf{unit}, \sigma \cup \{\mathsf{write}(\rho)\}}$$

$$\text{(fun)}\frac{\Gamma, x : \alpha_1 \vdash e : \beta, \sigma}{\Gamma \vdash \lambda x.e : \alpha \xrightarrow{\sigma} \beta, \emptyset} \qquad \text{(app)}\frac{\Gamma \vdash e_1 : \alpha \xrightarrow{\sigma_1} \beta, \sigma_2 \quad \Gamma \vdash e_2 : \alpha, \sigma_3}{\Gamma \vdash e_1\ e_2 : \beta, \sigma_1 \cup \sigma_2 \cup \sigma_3}$$

Figure 1: Simple effect system

2.2 THROUGH TYPE AND EFFECT SYSTEMS

Introduced by Gifford and Lucassen [24, 34], type and effect systems have been designed to track effectful operations performed by computations. Examples include tracking of reading and writing from and to memory locations [54], communication in message-passing systems [30] and atomicity in concurrent applications [21].

Type and effect systems are usually specified judgements of the form $\Gamma \vdash e : \alpha, \sigma$, meaning that the expression e has a type α in (free-variable) context Γ and additionally may have effects described by σ. Effect systems are typically added to a language that already supports effectful operations as a way of increasing the safety – the type and effect system provides stronger guarantees than a plain type system. Filinsky [19] refers to this approach as *descriptive*[3].

SIMPLE EFFECT SYSTEM The structure of a simple effect system is demonstrated in Figure 1. The example shows typing rules for a simply typed lambda calculus with an additional (effectful) operation $l \leftarrow e$ that writes the value of e to a mutable location l. The type of locations ($\mathsf{ref}_\rho\ \alpha$) is annotated with a *memory region* ρ of the location l. The effects tracked by the type and effect system over-approximate the actual effects and memory regions provide a convenient way to build such over-approximation. The effects are represented as a set of effectful actions that an expression may perform and the effectful action (*write*) adds a primitive effect $\mathsf{write}(\rho)$.

The remaining rules are shared by a majority of effect systems. Variable access (*var*) has no effects, application (*app*) combines the effects of both expressions, together with the latent effects of the function to be applied. Finally, lambda abstraction (*fun*) is a pure computation that turns the *actual* effects of the body into *latent* effects of the created function.

SIMPLE COEFFECT SYSTEM When writing the judgements of coeffect systems, we want to emphasize the fact that coeffect systems talk about *context* rather than *results*. For this reason, we write the judgements in the form $\Gamma@\sigma \vdash e : \alpha$, associating the additional information with the context (left-hand side) of the judgement rather than with the result (right-hand side) as in $\Gamma \vdash e : \alpha, \sigma$. This change alone would not be very interesting – we simply used different syntax to write a predicate with four arguments. As already mentioned, the key difference follows from the lambda abstraction rule.

The language in Figure 2 extends simple lambda calculus with resources and with a construct **access** e that obtains the resource specified by the expression e. Most of the typing rules correspond to those of effect systems.

3 In contrast to *prescriptive* effect systems that implement computational effects in a pure language – such as monads in Haskell

$$\text{(var)}\frac{x : \alpha \in \Gamma}{\Gamma@\emptyset \vdash x : \alpha} \qquad \text{(access)}\frac{\Gamma@\sigma \vdash e : \mathsf{res}_\rho\ \alpha}{\Gamma@\sigma_1 \cup \{\mathsf{access}(\rho)\} \vdash \textbf{access}\ e : \alpha}$$

$$\text{(fun)}\frac{\Gamma, x : \alpha@\sigma_1 \cup \sigma_2 \vdash e : \beta}{\Gamma@\sigma_1 \vdash \lambda x.e : \alpha \xrightarrow{\sigma_2} \beta} \qquad \text{(app)}\frac{\Gamma \vdash e_1 : \alpha \xrightarrow{\sigma_1} \beta, \sigma_2 \quad \Gamma \vdash e_2 : \alpha, \sigma_3}{\Gamma \vdash e_1\ e_2 : \beta, \sigma_1 \cup \sigma_2 \cup \sigma_3}$$

Figure 2: Simple effect system

Variable access (*var*) has no context requirements, application (*app*) combines context requirements of the two sub-expressions and latent context-requirements of the function.

The (*fun*) rule is different – the resources requirements of the body $\sigma_1 \cup \sigma_2$ are split between the *immediate context-requirements* associated with the current context $\Gamma@\sigma_1$ and the *latent context-requirements* of the function.

As demonstrated by examples in the Chapter 1, this means that the resource can be captured when a function is declared (e.g. when it is constructed on the server-side where database access is available), or when a function is called (e.g. when a function created on server-side requires access to current time-zone, it can use the resource available on the client-side).

2.3 THROUGH LANGUAGE SEMANTICS

Another pathway to coeffects leads through the semantics of effectful and context-dependent computations. In a pioneering work, Moggi [36] showed that effects (including partiality, exceptions, non-determinism and I/O) can be modelled uisng the category theoretic notion of *monad*.

When using monads, we distinguish effect-free values α from programs, or computations $M\alpha$. The *monad* M abstracts the *notion of computation* and provides a way of constructing and composing effectful computations:

Definition 1. *A* monad *over a category* $\mathcal{C}$ *is a triple* $(M, \mathsf{unit}, \mathsf{bind})$ *where:*

- M *is a mapping on objects (types)* $M : \mathcal{C} \to \mathcal{C}$
- unit *is a mapping* $\alpha \to M\alpha$
- bind *is a mapping* $(\alpha \to M\beta) \to (M\alpha \to M\beta)$

such that, for all $f : \alpha \to M\beta, g : \beta \to M\gamma$*:*

$$\mathsf{bind}\ \mathsf{unit} = \mathsf{id} \qquad \textit{(left identity)}$$
$$\mathsf{bind}\ f \circ \mathsf{unit} = f \qquad \textit{(right identity)}$$
$$\mathsf{bind}\ (\mathsf{bind}\ g \circ f) = (\mathsf{bind}\ f) \circ (\mathsf{bind}\ g) \qquad \textit{(associativity)}$$

Without providing much details, we note that well known examples of monads include the partiality monad ($M\alpha = \alpha + \bot$) also corresponding to the `Maybe` type in Haskell, list monad ($M\alpha = \mu\gamma.1 + (\alpha \times \gamma)$) and other. In programming language semantics, monads can be used in two distinct ways.

2.3.1 *Effectful languages and meta-languages*

Moggi uses monads to define two formal systems. In the first formal system, a monad is used to model the *language* itself. This means that the semantics of a language is given in terms of a one specific monad and the semantics

can be used to reason about programs in that language. To quote *"When reasoning about programs one has only one monad, because the programming language is fixed, and the main aim is to prove properties of programs"* [36, p. 5].

In the second formal system, monads are added to the programming language as type constructors, together with additional constructs corresponding to monadic bind and unit. A single program can use multiple monads, but the key benefit is the ability to reason about multiple languages. To quote *"When reasoning about programming languages one has different monads, one for each programming language, and the main aim is to study how they relate to each other"* [36, p. 5].

In this thesis, we generally follow the first approach – this means that we work with an existing programming language (without needing to add additional constructs corresponding to the primitives of our semantics). To explain the difference in greater detail, the following two sections show a minimal example of both formal systems. We follow Moggi and start with language where judgements have the form $x : \alpha \vdash e : \beta$ with exactly one variable[4].

LANGUAGE SEMANTICS When using monads to provide semantics of a language, we do not need to extend the language in any way – we assume that the language already contains the effectful primitives (such as the assignment operator $x \leftarrow e$ or other). A judgement of the form $x : \alpha \vdash e : \beta$ is interpreted as a morphism $\alpha \to M\beta$, meaning that any expression is interpreted as an effectful computation. The semantics of variable access (x) and the application of a primitive function f is interpreted as follows:

$$\begin{aligned} [\![x : \alpha \vdash x : \alpha]\!] &= \mathsf{unit}_M \\ [\![x : \alpha \vdash f\ e : \gamma]\!] &= (\mathsf{bind}_M\ f) \circ [\![e]\!] \end{aligned}$$

Variable access is an effect-free computation, that returns the value of the variable, wrapped using unit_M. In the second rule, we assume that e is an expression using the variable x and producing a value of type β and that f is a (primitive) function $\beta \to M\gamma$. The semantics lifts the function f using bind_M to a function $M\beta \to M\gamma$ which is compatible with the interpretation of the expression e.

META-LANGUAGE INTERPRETATION When designing meta-language based on monads, we need to extend the lambda calculus with additional type(s) and expressions that correspond to monadic primitives:

$$\begin{aligned} \alpha, \beta, \gamma &:= \tau \mid \alpha \to \beta \mid M\alpha \\ e &:= x \mid f\ e \mid \mathbf{return}_M\ e \mid \mathbf{let}_M\ x \Leftarrow e_1\ \mathbf{in}\ e_2 \end{aligned}$$

The types consist of primitive type (τ), function type and a type constructor that represents monadic computations. This means that the expressions in the language can create both effect-free values, such as α and computations $M\alpha$. The additional expression $\mathbf{return}_M$ is used to create a monadic computation (with no actual effects) from a value and $\mathbf{let}_M$ is used to sequence effectful computations. In the semantics, monads are not needed to inter-

4 This simplifies the examples as we do not need *strong* monad, but that is an orthogonal issue to the distinction between language semantics and meta-language.

pret variable access and application, they are only used in the semantics of additional (monadic) constructs:

$$\begin{aligned}
[\![x : \alpha \vdash x : \alpha]\!] &= \mathsf{id} \\
[\![x : \alpha \vdash f\ e : \beta]\!] &= f \circ [\![e]\!] \\
[\![x : \alpha \vdash \mathbf{return}_M\ e : M\beta]\!] &= \mathsf{unit}_M \circ [\![e]\!] \\
[\![x : \alpha \vdash \mathbf{let}_M\ y \Leftarrow e_1\ \mathbf{in}\ e_2 : M\beta]\!] &= \mathsf{bind}_M\ [\![e_2]\!] \circ [\![e_1]\!]
\end{aligned}$$

In this system, the interpretation of variable access becomes a simple identity function and application is just composition. Monadic computations are constructed explicitly using $\mathbf{return}_M$ (interpreted as unit_M) and they are also sequenced explicitly using the $\mathbf{let}_M$ construct. As noted by Moggi, the first formal system can be easily translated to the latter by inserting appropriate monadic constructs.

Moggi regards the meta-language system as more fundamental, because *"its models are more general"*. Indeed, this is a valid and reasonable perspective. Yet, we follow the first style, precisely because it is *less general* – our aim is to develop concrete context-aware programming languages (together with their type theory and semantics) rather than to build a general framework for reasoning about languages with context-dependent properties.

2.3.2 *Marriage of effects and monads*

The work on effect systems and monads both tackle the same problem – representing and tracking of computational effects. The two lines of research have been joined by Wadler and Thiemann [70]. This requires extending the categorical structure. A monadic computation $\alpha \to M\beta$ means that the computation has *some* effects while the judgement $\Gamma \vdash e : \alpha, \sigma$ specifies *what* effects the computation has.

To solve this mismatch, Wadler and Thiemann use a *family* of monads $M^\sigma\alpha$ with an annotation that specifies the effects that may be performed by the computation. In their system, an effectful function $\alpha \xrightarrow{\sigma} \beta$ is modelled as a pure function returning monadic computation $\alpha \to M^\sigma\beta$. Similarly, the semantics of a judgement $x : \alpha \vdash e : \beta, \sigma$ can be given as a function $\alpha \to M^\sigma\beta$. The precise nature of the family of monads has been later called *indexed monads* (e.g. by Tate [55]) and further developed by Atkey [4] in his work on *parameterized monads*.

THESIS PERSPECTIVE The key takeaway for this thesis from the outlined line of research is that, if we want to develop a language with type system that captures context-dependent properties of programs more precisely, the semantics of the language also needs to be a more fine-grained structure (akin to indexed monads). While monads have been used to model effects, an existing research links context-dependence with *comonads* – the categorical dual of monads.

2.3.3 *Context-dependent languages and meta-languages*

The theoretical parts of this thesis extend the work of Uustalu and Vene who use comonads to give the semantics of data-flow computations [61] and more generally, notions of *context-dependent computations* [60]. The computations discussed in the latter work include streams, arrays and containers – this is a more diverse set of examples, but they all mostly represent forms

of collections. Ahman et al. [2] discuss the relation between comonads and *containers* in more details.

The utility of comonads has been explored by a number of authors before. Brookes and Geva [10] use *computational* comonads for intensional semantics[5]. In functional programming, Kieburtz [31] proposed to use comonads for stream programming, but also handling of I/O and interoperability.

Biermann and de Paiva used comonads to model the necessity modality $\Box$ in intuitionistic modal S4 [9], linking programming languages derived from modal logics to comonads. One such language has been reconstructed by Pfenning and Davies [45]. Nanevski et al. extend this work to Contextual Modal Type Theory (CMTT) [39], which again shows the importance of comonads for *context-dependent* computations.

While Uustalu and Vene use comonads to define the *language semantics* (the first style of Moggi), Nanevski, Pfenning and Davies use comonads as part of meta-language, in the form of $\Box$ modality, to reason about context-dependent computations (the second style of Moggi). Before looking at the details, we use the following definition of comonad:

Definition 2. *A* comonad *over a category* $\mathcal{C}$ *is a triple* $(C, \mathsf{counit}, \mathsf{cobind})$ *where:*

- C *is a mapping on objects (types)* $C : \mathcal{C} \to \mathcal{C}$
- counit *is a mapping* $C\alpha \to \alpha$
- cobind *is a mapping* $(C\alpha \to \beta) \to (C\alpha \to C\beta)$

such that, for all $f : \alpha \to M\beta, g : \beta \to M\gamma$*:*

$$\mathsf{cobind}\ \mathsf{counit} = \mathsf{id} \qquad \textit{(left identity)}$$

$$\mathsf{counit} \circ \mathsf{cobind}\ f = f \qquad \textit{(right identity)}$$

$$\mathsf{cobind}\ (\mathsf{cobind}\ g \circ f) = (\mathsf{cobind}\ f) \circ (\mathsf{cobind}\ g) \qquad \textit{(associativity)}$$

The definition is similar to monad with "reversed arrows". Intuitively, the counit operation extracts a value α from a value that carries additional context $C\alpha$. The cobind operation turns a context-dependent function $C\alpha \to \beta$ into a function that takes a value with context, applies the context-dependent function to value(s) in the context and then propagates the context. The next section makes this intuitive definition more concrete. More detailed discussion about comonads can be found in Orchard's PhD thesis [42].

LANGUAGE SEMANTICS To demonstrate the approach of Uustalu and Vene, we consider the non-empty list comonad $C\alpha = \mu\gamma.\alpha + (\alpha \times \gamma)$. A value of the type is either the last element α or an element followed by another non-empty list $\alpha \times \gamma$. Note that the list must be non-empty – otherwise counit would not be a complete function (it would be undefined on empty list). In the following, we write $(l_1, \ldots, l_n)$ for a list of n elements:

$$\begin{aligned} \mathsf{counit}\ (l_1, \ldots, l_n) &= l_1 \\ \mathsf{cobind}\ f\ (l_1, \ldots, l_n) &= (f(l_1, \ldots, l_n), f(l_2, \ldots, l_n), \ldots, f(l_n)) \end{aligned}$$

The counit operation returns the current (first) element of the (non-empty) list. The cobind operation creates a new list by applying the context-dependent function f to the entire list, to the suffix of the list, to the suffix of the suffix and so on.

In causal data-flow, we can interpret the list as a list consisting of past values, with the current value in the head. Then, the cobind operation calcu-

5 The structure of computational comonad has been also used by the author of this thesis to abstract evaluation order of monadic computations [44].

$$\text{(eval)}\frac{\Gamma \vdash e : C^{\emptyset}\alpha}{\Gamma \vdash !e : \alpha} \qquad \text{(letbox)}\frac{\Gamma \vdash e_1 : C^{\Phi,\Psi}\alpha \quad \Gamma, x : C^{\Phi}\alpha \vdash e_2 : \beta}{\Gamma \vdash \textbf{let box } x = e_1 \textbf{ in } e_2 : C^{\Psi}\beta}$$

Figure 3: Typing for a comonadic language with contextual staged computations

lates the current value of the output based on the current and all past values of the input; the second element is calculated based on all past values and the last element is calculated based just on the initial input (l_n). In addition to the operations of comonad, the model also uses some operations that are specific to causal data-flow:

$$\mathsf{prev}\ (l_1, \ldots, l_n) \quad = \quad (l_2, \ldots, l_n)$$

The operation drops the first element from the list. In the data-flow interpretation, this means that it returns the previous state of a value.

Now, consider a simple data-flow language with single-variable contexts, variables, primitive built-in functions and a construct **prev** e that returns the previous value of the computation e. We omit the typing rules, but they are simple – assuming e has a type α, the expression **prev** e has also type α. The fact that the language models data-flow and values are lists (of past values) is a matter of semantics, which is defined as follows:

$$\begin{aligned} [\![x : \alpha \vdash x : \alpha]\!] &= \mathsf{counit}_C \\ [\![x : \alpha \vdash f\ e : \gamma]\!] &= f \circ (\mathsf{cobind}_C\ [\![e]\!]) \\ [\![x : \alpha \vdash \textbf{prev}\ e : \gamma]\!] &= \mathsf{prev} \circ (\mathsf{cobind}_C\ [\![e]\!]) \end{aligned}$$

The semantics follows that of effectful computations using monads. A variable access is interpreted using counit_C (obtain the value and ignore additional available context); composition uses cobind_C to propagate the context to the function f and **prev** is interpreted using the primitive prev (which takes a list and returns a list).

For example, the judgement $x : \alpha \vdash \textbf{prev}\ (\textbf{prev}\ x) : \alpha$ represents an expression that expects context with variable x and returns a stream of values before the previous one. The semantics of the term expresses this behaviour: $(\mathsf{prev} \circ \mathsf{prev} \circ (\mathsf{cobind}_C\ \mathsf{counit}_C))$. Note that the first operation is simply an identity function thanks to the comonad laws discussed earlier.

In the outline presented here, we ignored lambda abstraction. Similarly to monadic semantics, where lambda abstraction requires *strong* monad, the comonadic semantics also requires additional structure called *symmetric (semi)monoidal* comonads. This structure is responsible for the splitting of context-requirements in lambda abstraction. We return to this topic when discussing flat coeffect system later in the thesis.

META-LANGUAGE INTERPRETATION To briefly demonstrate the approach that employs comonads as part of a meta-language, we look at an example inspired by the work of Pfenning, Davies and Nanevski et al. We do not attempt to provide precise overview of their work. The main purpose of our discussion is to provide a different intuition behind comonads, and to give an example of a language that includes comonad as a type constructor, together with language primitives corresponding to comonadic operations[6].

6 In fact, Pfenning and Davies [45, 39] never mention comonads explicitly. This is done in later work by Gabbay et al. [23], but the connection between the language and comonads is not as direct as in case of monadic or comonadic semantics covered in the last few pages.

In languages inspired by modal logics, types can have the form $\Box\alpha$. In the work of Pfenning and Davies, this means a term that is provable with no assumptions. In distributed programming language ML5, Murphy et al. [37, 38] use the $\Box\alpha$ type to mean *mobile code*, that is code that can be evaluated at any node of a distributed system (the evaluation corresponds to the axiom $\Box\alpha \to \alpha$). Finally, Davies and Pfenning [15] consider staged computations and interpret $\Box\alpha$ as a type of (unevaluated) expressions of type α.

In Contextual Modal Type Theory, the modality $\Box$ is further annotated. To keep the syntax consistent with earlier examples, we use $C^{\Psi}\alpha$ for a type $\Box\alpha$ with an annotation Ψ. The type is a comonadic counterpart to the *indexed monads* used by Wadler and Thiemann when linking monads and effect systems and, indeed, it gives rise to a language that tracks context-dependence of computations in a type system.

In staged computation, the type $C^{\Psi}\alpha$ represents an expression that requires the context Ψ (i.e. the expression is an open term that requires variables Ψ). The Figure 3 shows two typing rules for such language. The rules directly correspond to the two operations of a comonad and can be interpreted as follows:

- (*eval*) corresponds to $\mathsf{counit} : C^{\emptyset}\alpha \to \alpha$. It means that we can evaluate a closed (unevaluated) term and obtain a value. Note that the rule requires a specific context annotation. It is not possible to evaluate an open term.
- (*letbox*) corresponds to $\mathsf{cobind} : (C^{\Psi}\alpha \to \beta) \to C^{\Psi,\Phi}\alpha \to C^{\Phi}\beta$. It means that given a term which requires variable context Ψ, Φ (expression e_1) and a function that turns a term needing Ψ into an evaluated value (expression e_2), we can construct a term that requires just Φ.

The fact that the (*eval*) rule requires a specific context is an interesting relaxation from ordinary comonads where counit needs to be defined for all values. Here, the indexed counit operation needs to be defined only on values annotated with $\emptyset$.

The annotated cobind operation that corresponds to (*letbox*) is in details introduced in Chapter X. An interesting aspect is that it propagates the context-requirements "backwards". The input expression (second parameter) requires a combination of contexts that are required by the two components – those required by the input of the function (first argument) and those required by the resulting expression (result). This is another key aspect that distinguishes coeffects from effect systems.

THESIS PERSPECTIVE As mentioned earlier, we are interested in designing context-dependent languages and so we use comonads as *language semantics*. Uustalu and Vene present a semantics of context-dependent computations in terms of comonads. We provide the rest of the story known from the marriage of monads and effects. We develop coeffect calculus with a type system that tracks the context requirements more precisely (by annotating the types) and we add indexing to comonads and link the two by giving a formal semantics.

The *meta-language* approach of Pfenning, Davies and Nanevski et al. is closely related to our work. Most importantly, Contextual Modal Type Theory (CMTT) uses indexed $\Box$ modality which seems to correspond to indexed comonads (in a similar way in which effect systems correspond to indexed

$$\text{(exchange)}\frac{\Gamma, x : \alpha, y : \beta \vdash e : \gamma}{\Gamma, y : \beta, x : \alpha \vdash e : \gamma} \qquad \text{(weakening)}\frac{\Gamma, \Delta \vdash e : \gamma}{\Gamma, x : \alpha, \Delta \vdash e : \gamma}$$

$$\text{(contraction)}\frac{\Gamma, x : \alpha, y : \alpha, \Delta \vdash e : \gamma}{\Gamma, x : \alpha, \Delta \vdash e[y \leftarrow x] : \gamma}$$

Figure 4: Exchange, weakening and contraction typing rules

monads). The relation between CMTT and comonads has been suggested by Gabbay et al. [23], but the meta-language employed by CMTT does not directly correspond to comonadic operations. For example, our let box typing rule from Figure 3 is not a primitive of CMTT and would correspond to $\mathsf{box}(\Psi, \mathsf{letbox}(e_1, x, e_2))$. Nevertheless, the indexing in CMTT provides a useful hint for adding indexing to the work of Uustalu and Vene.

2.4 THROUGH SUB-STRUCTURAL AND BUNCHED LOGICS

In the coeffect system for tracking resource usage outlined earlier, we associated additional contextual information (set of available resources) with the variable context of the typing judgement: $\Gamma@\sigma \vdash e : \alpha$. In other words, our work focuses on "what is happening on the left hand side of $\vdash$".

In the case of resources, the additional information about the context are simply added to the variable context (as a products), but we will later look at contextual properties that affect how variables are represented. More importantly, *structural coeffects* link additional information to individual variables in the context, rather than the context as a whole.

In this section, we look at type systems that reconsider Γ in a number of ways. First of all, sub-structural type systems [71] restrict the use of variables in the language. Most famously linear type systems introduced by Wadler [68] can guarantee that variable is used exactly once. This has interesting implications for memory management and I/O.

In bunched typing developed by O'Hearn [40], the variable context is a tree formed by multiple different constructors (e.g. one that allows sharing and one that does not). Most importantly, bunched typing has contributed to the development of separation logic [41] (starting a fruitful line of research in software verification), but it is also interesting on its own.

SUB-STRUCTURAL TYPE SYSTEMS Traditionally, Γ is viewed as a set of assumptions and typing rules admit (or explicitly include) three operations that manipulate the variable contexts which are shown in Figure 4. The (*exchange*) rule allows us to reorder variables (which is implicit, when assumptions are treated as set); (*weakening*) makes it possible to discard an assumption – this has the implication that a variable may be declared but never used. Finally, (*contraction*) makes it possible to use a single variable multiple times (by joining multiple variables into a single one using substitution).

In sub-structural type systems, the assumptions are typically treated as a list. As a result, they have to be manipulated explicitly. Different systems allow different subset of the rules. For example, *affine* systems allows exchange and weakening, leading to a system where variable may be used at most once; in *linear* systems, only exchange is permitted and so every variable has to be used exactly once.

$$\text{(exchange1)}\frac{\Gamma(\Delta, \Sigma) \vdash e : \alpha}{\Gamma(\Sigma, \Delta) \vdash e : \alpha} \qquad \text{(weakening)}\frac{\Gamma(\Delta) \vdash e : \alpha}{\Gamma(\Delta; \Sigma) \vdash e : \alpha}$$

$$\text{(exchange2)}\frac{\Gamma(\Delta; \Sigma) \vdash e : \alpha}{\Gamma(\Sigma; \Delta) \vdash e : \alpha} \qquad \text{(contraction)}\frac{\Gamma(\Delta; \Sigma) \vdash e : \alpha}{\Gamma(\Delta) \vdash e[\Sigma \leftarrow \Delta] : \alpha}$$

Figure 5: Exchange, weakening and contraction rules for bunched typing

When tracking context-dependent properties associated with individual variables, we need to be more explicit in how variables are used. Sub-structural type systems provide a way to do this. Even when we allow all three operations, we can track which variables are used and how (and use that to track additional contextual information about variables).

BUNCHED TYPE SYSTEMS Bunched typing makes one more refinement to how Γ is treated. Rather than having a list of assumptions, the context becomes a tree that contains variable typings (or special identity values) in the leaves and has multiple different types of nodes. The context can be defined, for example, as follows:

$$\Gamma, \Delta, \Sigma := x : \alpha \mid I \mid \Gamma, \Gamma \mid 1 \mid \Gamma; \Gamma$$

The values I and 1 represent two kinds of "empty" contexts. More interestingly, non-empty variable contexts may be constructed using two distinct constructors – Γ, Γ and $\Gamma; \Gamma$ – that have different properties. In particular, weakening and contraction is only allowed for the ; constructor, while exchange is allowed for both.

The structural rules for bunched typing are shown in Figure 5. The syntax $\Gamma(\Delta)$ is used to mean an assumption tree that contains Δ as a sub-tree and so, for example, (*exchange1*) can switch the order of contexts anywhere in the tree. The remaining rules are similar to the rules of linear logic.

One important note about bunched typing is that it requires a different interpretation. The omission of weakening and contraction in linear logic means that variable can be used exactly once. In bunched typing, variables may still be duplicated, but only using the ";" separator. The type system can be interpreted as specifying whether a variable may be shared between the body of a function and the context where a function is declared. The system introduces two distinct function types $\alpha \to \beta$ and $\alpha \twoheadrightarrow \beta$ (corresponding to ";" and "," respectively). The key property is that only the first kind of functions can share variables with the context where a function is declared, while the second restricts such sharing. We do not attempt to give a detailed description here as it is not immediately to coeffects – for more information, refer to O'Hearn's introduction [40].

THESIS PERSPECTIVE Our work can be viewed as annotating bunches. Such annotations then specify additional information about the context – or, more specifically, about the sub-tree of the context. Although this is not the exact definition used in Chapter X, we could define contexts as follows:

$$\Gamma, \Delta, \Sigma := x : \alpha \mid 1 \mid \Gamma, \Gamma \mid \Gamma@\sigma$$

Now we can not only annotate an entire context with some information (as in the simple coeffect system for tracking resources that used judgements of a form $\Gamma@\sigma \vdash e : \alpha$). We can also annotate individual components. For

example, a context containing variables x, y, z where only x is used could be written as $(x : \alpha @ \mathsf{used}), ((y : \alpha, z : \alpha) @ \mathsf{unused})$.

For the purpose of this introduction, we ignore important aspects such as how are nested annotations interpreted. The main goal is to show that coeffects can be easily viewed as an extension to the work on bunched logic. Aside from this principal connection, *structural coeffects* also use some of the proof techniques from the work on bunched logics, because they also use tree-like structure of variable contexts.

2.5 SUMMARY

This chapter presented four different pathways leading to the idea of coeffects. We also introduced the most important related work, although presenting related work was not the main goal of the chapter. The main goal was to show the idea of coeffects as a logical follow up to a number of research directions. For this reason, we highlighted only certain aspects of related work – the remaining aspects as well as important technical details are covered in later chapters.

The first pathway looks at applications and systems that involve notion of *context*. The two coeffect calculi we present aim to unify some of these systems. The second pathway follows as a dualization of well-known effect systems. However, this is not simply a syntactic transformation, because coeffect systems treat lambda abstraction differently. The third pathway follows by extending comonadic semantics of context-dependent computations with indexing and building a type system analogous to effect system from the "marriage of effects and monads". Finally, the fourth pathway starts with sub-structural type systems. Coeffect systems naturally arise by annotating bunches in bunched logics with additional information.

3 FLAT COEFFECT LANGUAGE

TODO: Change this

Understanding how programs affect their environment is a well studied area: *effect systems* [54] provide a static analysis of effects and *monads* [36] provide a unified semantics to different notions of effect. Wadler and Thiemann unify the two approaches [70], *indexing* a monad with effect information, and showing that the propagation of effects in an effect system matches the semantic propagation of effects in the monadic approach.

No such unified mechanism exists for tracking the context requirements. We use the term *coeffect* for such contextual program properties. Notions of context have been previously captured using comonads [60] (the dual of monads) and by languages derived from modal logic [45, 39], but these approaches do not capture many useful examples which motivate our work. We build mainly on the former comonadic direction (§3.3) and discuss the modal logic approach later (§3.5).

We extend a simply typed lambda calculus with a coeffect system based on comonads, replicating the successful approach of effect systems and monads.

EXAMPLES OF COEFFECTS. We present three examples that do not fit the traditional approach of *effect systems* and have not been considered using the *modal logic* perspective, but can be captured as *coeffect systems* (§3.1) – the tracking of implicit dynamically-scoped parameters (or resources), analysis of variable liveness, and tracking the number of required past values in dataflow computations.

COEFFECT CALCULUS. Informed by the examples, we identify a general algebraic structure for coeffects. From this, we define a general *coeffect calculus* that unifies the motivating examples (§3.2) and discuss its syntactic properties (§3.4).

INDEXED COMONADS. Our categorical semantics (§3.3) extends the work of Uustalu and Vene [60]. By adding annotations, we generalize comonads to *indexed comonads*, which capture notions of computation not captured by ordinary comonads.

3.1 MOTIVATION

Effect systems, introduced by Gifford and Lucassen [24], track *effects* of computations, such as memory access or message-based communication [30]. Their approach augments typing judgments with effect information: $\Gamma \vdash e : \tau, F$. Wadler and Thiemann explain how this shapes effect analysis of lambda abstraction [70]:

> *In the rule for abstraction, the effect is empty because evaluation immediately returns the function, with no side effects. The effect on the function arrow is the same as the effect for the function body, because applying the function will have the same side effects as evaluating the body.*

$$(var)\ \frac{x : \tau \in \Gamma}{C^{\emptyset}\Gamma \vdash x : \tau} \qquad (app)\ \frac{C^{r}\Gamma \vdash e_1 : C^{t}\tau_1 \to \tau_2 \quad C^{s}\Gamma \vdash e_2 : \tau_1}{C^{r \cup s \cup t}\Gamma \vdash e_1\ e_2 : \tau_2}$$

$$(access)\ \frac{}{C^{\{?a\}}\Gamma \vdash ?a : \rho} \qquad (abs)\ \frac{C^{r \cup s}(\Gamma, x : \tau_1) \vdash e : \tau_2}{C^{r}\Gamma \vdash \lambda x.e : C^{s}\tau_1 \to \tau_2}$$

Figure 6: Selected coeffect rules for implicit parameters

In contrast to the static analysis of *effects*, the analysis of *context-dependence* does not match this pattern. In the systems we consider, lambda abstraction places requirements on both the *call-site* (latent requirements) and the *declaration-site* (immediate requirements), resulting in different syntactic properties. We informally discuss three examples first that demonstrate how contextual requirements propagate. Section (§3.2) then unifies these in a single calculus.

We write coeffect judgements $C^{s}\Gamma \vdash e : \tau$ where the coeffect annotation s associates context requirements with the free-variable context Γ. Function types have the form $C^{s}\tau_1 \to \tau_2$ associating *latent* coeffects s with the parameter. The $C^{s}\Gamma$ syntax and $C^{s}\tau$ types are a result of the indexed comonadic semantics (§3.3).

3.1.1 *Implicit parameters and resources.*

Implicit parameters [32] are *dynamically-scoped* variables. They can be used to parameterize a computation without propagating arguments explicitly through a chain of calls and are part of the context in which expressions evaluate. As correctly expected [32], they can be modelled by comonads. Rebindable resources in distributed computations follow a similar pattern, but we discuss implicit parameters for simplicity.

The following function prints a number using implicit parameters ?culture (determining the decimal mark) and ?format (the number of decimal places):

$$\lambda n.\mathsf{printNumber}\ n\ ?\mathsf{culture}\ ?\mathsf{format}$$

Figure 6 shows a type-and-coeffect system tracking the set of an expression's implicit parameters. For simplicity here, all implicit parameters have type ρ.

Context requirements are created in (*access*), while (*var*) requires no implicit parameters; (*app*) combines requirements of both sub-expressions as well as the latent requirements of the function. The (*abs*) rule is where the example differs from effect systems. Function bodies can access the union of the parameters (or resources) available at the declaration-site ($C^{r}\Gamma$) and at the call-site ($C^{s}\tau_1$). Two of the nine permissible judgements for the above example are:

$$\begin{aligned} C^{\emptyset}\Gamma &\vdash (\ldots) : C^{\{?\mathsf{culture},?\mathsf{format}\}}\mathsf{int} \to \mathsf{string} \\ C^{\{?\mathsf{culture},?\mathsf{format}\}}\Gamma &\vdash (\ldots) : C^{\{?\mathsf{format}\}}\mathsf{int} \to \mathsf{string} \end{aligned}$$

The coeffect system infers multiple, i. e. non-principal, coeffects for functions. Different judgments are desirable depending on how a function is used. In the first case, both parameters have to be provided by the caller. In the second, both are available at declaration-site, but ?format may be rebound (precise meaning is provided by the monoidal structure on the product comonad in §3.3).

Implicit parameters can be captured by the *reader* monad, where parameters are associated with the function codomain $M^{\emptyset}(\mathsf{int} \to M^{\{?\mathsf{culture},?\mathsf{format}\}}\mathsf{string})$, modelling only the first case. Whilst the reader monad can be extended to model rebinding, the next example cannot be structured by *any* monad.

3.1.2 *Liveness analysis.*

Liveness analysis detects whether a free variable of an expression may be used (*live*) or whether it is definitely not needed (*dead*). A compiler can remove bindings to dead variables as the result is never used.

We start with a restricted analysis and briefly mention how to make it practical later (§3.5). The restricted form is interesting theoretically as it gives rise to the indexed Maybe comonad (§3.3), which is a basic but instructive example.

A coeffect system in Fig. 7 detects whether all variables are dead ($C^{D}\Gamma$) or whether at least one variable is live ($C^{L}\Gamma$). Variable access (*var*) is annotated with L and constant access with D. That is, if $c \in \mathbb{N}$ then $C^{D}\Gamma \vdash c : \mathsf{int}$. A dead context may be marked as live by letting $D \sqsubseteq L$ and adding subcoeffecting (§3.2).

The (*app*) rule is best understood by discussing its semantics. Consider first *sequential composition* of (semantic) functions g, f annotated with r, s. The argument of $g \circ f$ is live only when arguments of both f and g are live. The coeffect semantics captures the additional behaviour that f is not evaluated when g ignores its input (regardless of the evaluation order of the underlying language). We write $r \sqcap s$ for a conjunction (returning L iff $r = s = L$). Secondly, a *pointwise composition* passes the same argument to g and h. The parameter is live if either the parameter of g or h is live ($r \sqcup s$). Application combines the two operations, so the context Γ is live if it is needed by e_1 *or* by the function value *and* by e_2.

An (*abs*) rule (not shown) compatible with the structure in Fig. 6 combines the context annotations using $\sqcap$. Thus, if the body uses some variables, both the function argument and the context of the declaration-site are marked as live.

Liveness cannot be modelled using monads as $\tau_1 \to M^{r}\tau_2$. In call-by-value languages, the argument τ_1 is always evaluated. Using indexed comonads (§3.3), we model liveness as $C^{r}\tau_1 \to \tau_2$ where C^{r} is the parametric type $\mathsf{Maybe}\ \tau = \tau + 1$ (which contains a value τ when $r = L$ and does not contain value when $r = D$).

3.1.3 *Efficient dataflow.*

Dataflow languages (e. g. [66]) declaratively describe computations over streams. In *causal* data flow, program may access past values – in this setting, a function $\tau_1 \to \tau_2$ becomes a function from a list of historical values $[\tau_1] \to \tau_2$. A coeffect system here tracks how many past values to cache.

Figure 8 annotates contexts with an integer specifying the maximum number of required past values. The current value is always present, so (*var*) is annotated with 0. The expression **prev** e gets the previous value of stream e and requires one additional past value (*prev*); e. g. **prev** (**prev** e) requires 2 past values.

The (*app*) rule follows the same intuition as for liveness. Sequential composition adds the tags (the first function needs $n + p$ past values to produce p past inputs for the second function); passing the context to two subcomputations requires the maximum number of the elements required by the two subcomputations. The (*abs*) rule for data-flow needs a distinct operator – *min* – therefore, the declaration-site and call-site must each provide at least

$$(\textit{var})\ \frac{x : \tau \in \Gamma}{C^{L}\Gamma \vdash x : \tau} \qquad (\textit{app})\ \frac{C^{s}\Gamma \vdash e_2 : \tau_1 \qquad C^{r}\Gamma \vdash e_1 : C^{t}\tau_1 \to \tau_2}{C^{r \sqcup (s \sqcap t)}\Gamma \vdash e_1\ e_2 : \tau_2}$$

Figure 7: Selected coeffect rules for liveness analysis

$$(var)\ \frac{x : \tau \in \Gamma}{C^0\Gamma \vdash x : \tau} \qquad (app)\ \frac{C^m\Gamma \vdash e_1 : C^p\tau_1 \to \tau_2 \qquad C^n\Gamma \vdash e_2 : \tau_1}{C^{max(m,n+p)}\Gamma \vdash e_1\ e_2 : \tau_2}$$

$$(prev)\ \frac{C^n\Gamma \vdash e : \tau}{C^{n+1}\Gamma \vdash \mathbf{prev}\ e : \tau} \qquad (abs)\ \frac{C^{min(m,n)}(\Gamma, x : \tau_1) \vdash e : \tau_2}{C^m\Gamma \vdash \lambda x.e : C^n\tau_1 \to \tau_2}$$

Figure 8: Selected coeffect rules for causal data flow

the number of past values required by the function body (the body may use variables coming from the declaration-site as well as the argument).

The soundness follows from our categorical model (§3.3). Uustalu and Vene [60] model causal dataflow computations using a non-empty list comonad $\mathsf{NeList}\ \tau = \tau \times (\mathsf{NeList}\ \tau + 1)$. However, such model leads to (inefficient) unbounded lists of past elements. The above static analysis provides an approximation of the number of required past elements and so we use just fixed-length lists.

3.2 GENERALIZED COEFFECT CALCULUS

The previous three examples exhibit a number of commonalities. We capture these in the *coeffect calculus*. We do not overly restrict the calculus to make it open for notions of context-dependent computations not discussed above.

The syntax of our calculus is that of the simply-typed lambda calculus (where v ranges over variables, T over base types, and r over coeffect annotations):

$$e ::= v \mid \lambda v.e \mid e_1\ e_2 \qquad \tau ::= \mathsf{T} \mid \tau_1 \to \tau_2 \mid C^r\tau$$

The type $C^r\tau$ captures values of type τ in a context specified by the annotation r. This type appears only on the left-hand side of a function arrow $C^r\tau_1 \to \tau_2$. In the semantics, C^r corresponds to some data type (e. g. list or Maybe). Extensions such as explicit *let*-binding are discussed later (§3.4).

The coeffect tags r, that were demonstrated in the previous section, can be generalized to a structure with three binary operators and a particular element.

Definition 3. *A* coeffect algebra $(S, \oplus, \vee, \wedge, e)$ *is a set* S *with an element* $e \in S$*, a semi-lattice* $(S, \vee)$*, a monoid* $(S, \oplus, e)$*, and a binary* $\wedge$*. That is,* $\forall r, s, t \in S$*:*

$$r \oplus (s \oplus t) = (r \oplus s) \oplus t \qquad e \oplus r = r = r \oplus e \qquad \text{(monoid)}$$

$$r \vee s = s \vee r \qquad r \vee (s \vee t) = (r \vee s) \vee t \qquad r \vee r = r \qquad \text{(semi-lattice)}$$

The generalized coeffect calculus captures the three motivating examples (§3.1), where some operators of the coeffect algebra may coincide.

The $\oplus$ operator represents *sequential* composition; guided by the categorical model (§3.3), we require it to form a monoid with e. The operator $\vee$ corresponds to merging of context-requirements in *pointwise composition* and the semi-lattice $(S, \vee)$ defines a partial order: $r \leqslant s$ when $r \vee s = s$. This ordering implies a sub-coeffecting rule. The coeffect e is often the top or bottom of the lattice.

The $\wedge$ operator corresponds to splitting requirements of a function body. The operator is unrestricted in the general system. A number of additional laws holds for *some* coeffects systems, e. g. semi-lattice structure of $\wedge$ and a form of distributivity. Quite possibly, they should hold for all coeffect systems. We start with as few laws as possible so as not to limit possible uses of the calculus. We consider constrained variants that provide useful syntactic properties later (§3.4).

$$(var)\ \frac{x : \tau \in \Gamma}{C^{e}\Gamma \vdash x : \tau} \qquad (app)\ \frac{C^{r}\Gamma \vdash e_1 : C^{s}\tau_1 \to \tau_2 \qquad C^{t}\Gamma \vdash e_2 : \tau_1}{C^{r \vee (s \oplus t)}\Gamma \vdash e_1\ e_2 : \tau_2}$$

$$(sub)\ \frac{C^{s}\Gamma \vdash e : \tau}{C^{r}\Gamma \vdash e : \tau}\ (s \leqslant r) \qquad (abs)\ \frac{C^{r \wedge s}(\Gamma, x : \tau_1) \vdash e : \tau_2}{C^{r}\Gamma \vdash \lambda x.e : C^{s}\tau_1 \to \tau_2}$$

Figure 9: Type and coeffect system for the coeffect calculus

IMPLICIT PARAMETERS use sets of names $S = \mathcal{P}(\mathsf{Id})$ as tags with union $\cup$ for all three operators. Variable access is annotated with $e = \emptyset$ and $\leqslant$ is subset ordering.

LIVENESS uses a two point lattice $S = \{D, L\}$ where $D \sqsubseteq L$. Variables are annotated with the top element $e = L$ and constants with bottom D. The $\vee$ operation is $\sqcup$ (join) and $\wedge$ and $\oplus$ are both $\sqcap$ (meet).

DATAFLOW tags are natural numbers $S = \mathbb{N}$ and operations $\vee, \wedge$ and $\oplus$ correspond to *max*, *min* and $+$, respectively. Variable access is annotated with $e = 0$ and the order $\leqslant$ is the standard ordering of natural numbers.

3.2.1 *Coeffect typing rules.*

Figure 9 shows the rules of the coeffect calculus, given some coeffect algebra $(S, \oplus, \vee, \wedge, e)$. The context required by a variable access (*var*) is annotated with e. The sub-coeffecting rule (*sub*) allows the contextual requirements of an expression to be generalized.

The (*abs*) rule checks the body of the function in a context $r \wedge s$, which is a combination of the coeffects available in the context r where the function is defined and in a context provided by the caller of the function. Note that none of the judgements create a *value* of type $C^{r}\tau$. This type appears only immediately to the left of an arrow $C^{r}\tau_1 \to \tau_2$.

In function application (*app*), context requirements of both expressions and the function are combined as previously: the pointwise composition $\vee$ is used to combine the coeffects of the expression representing a function r and the coeffects of the argument, sequentially composed with the coeffects of the function $s \oplus t$.

For space reasons, we omit recursion. We note that this would require adding effect variables and extending the coeffect algebra with a fixed point operation.

3.3 COEFFECT SEMANTICS USING INDEXED COMONADS

The approach of *categorical semantics* interprets terms as morphisms in some category. For typed calculi, typing judgments $x_1 : \tau_1 \ldots x_n : \tau_n \vdash e : \tau$ are usually mapped to morphisms $[\![\tau_1]\!] \times \ldots \times [\![\tau_n]\!] \to [\![\tau]\!]$. Moggi showed the semantics of various effectful computations can be captured generally using the (*strong*) *monad* structure [36]. Dually, Uustalu and Vene showed that (*monoidal*) *comonads* capture various kinds of context-dependent computation [60].

We extend Uustalu and Vene's approach to give a semantics for the coeffect calculus by generalising comonads to *indexed comonads*. We emphasise semantic intuition and abbreviate the categorical foundations for space reasons.

INDEXED COMONADS. Uustalu and Vene's approach interprets well-typed terms as morphisms $C(\tau_1 \times \ldots \times \tau_n) \to \tau$, where C encodes contexts and

has a comonad structure [60]. Indexed comonads comprise a *family* of object mappings C^r indexed by a coeffect r describing the contextual requirements satisfied by the encoded context. We interpret judgments $C^r(x_1 : \tau_1, \ldots, x_n : \tau_n) \vdash e : \tau$ as morphisms $C^r([\![\tau_1]\!] \times \ldots \times [\![\tau_n]\!]) \to [\![\tau]\!]$.

The indexed comonad structure provides a notion of composition for computations with different contextual requirements.

Definition 4. *Given a monoid* $(S, \oplus, e)$ *with binary operator* $\oplus$ *and unit* e*, an* indexed comonad *over a category* $\mathcal{C}$ *comprises a family of object mappings* C^r *where for all* $r \in S$ *and* $A \in \mathrm{obj}(\mathcal{C})$ *then* $C^r A \in \mathrm{obj}(\mathcal{C})$ *and:*

- *a natural transformation* $\varepsilon_A : C^e A \to A$*, called the* counit*;*
- *a family of mappings* $(-)^\dagger_{r,s}$ *from morphisms* $C^r A \to B$ *to morphisms* $C^{r \oplus s} A \to C^s B$ *in* $\mathcal{C}$*, natural in* A, B*, called* coextend*;*

such that for all $f : C^r \tau_1 \to \tau_2$ *and* $g : C^s \tau_2 \to \tau_3$ *the following equations hold:*

$$\varepsilon \circ f^\dagger_{r,e} = f \qquad (\varepsilon)^\dagger_{e,r} = \mathsf{id} \qquad (g \circ f^\dagger_{r,s})^\dagger_{(r \oplus s),t} = g^\dagger_{s,t} \circ f^\dagger_{r,(s \oplus t)}$$

The *coextend* operation gives rise to an associative composition operation for computations with contextual requirements (with *counit* as the identity):

$$\hat{\circ} : (C^r \tau_1 \to \tau_2) \to (C^s \tau_2 \to \tau_3) \to (C^{r \oplus s} \tau_1 \to \tau_3) \qquad g \,\hat{\circ}\, f = g \circ f^\dagger_{r,s}$$

The composition $\hat{\circ}$ best expresses the intention of indexed comonads: contextual requirements of the composed functions are combined. The properties of the composition follow from the indexed comonad laws and the monoid $(S, \oplus, e)$.

EXAMPLE Indexed comonad are analogous to comonads (in coKleisli form), but with the additional monoidal structure on indices. Indeed, comonads are a special case of indexed comonads with a trivial singleton monoid, e. g., $(\{1\}, *, 1)$ with $1 * 1 = 1$ where C^1 is the underlying functor of the comonad and ε and $(-)^\dagger_{1,1}$ are the usual comonad operations. However, as demonstrated next, not all indexed comonads are derived from ordinary comonads.

EXAMPLE The *indexed partiality comonad* encodes free-variable contexts of a computation which are either *live* or *dead* (i. e., have *liveness* coeffects) with the monoid $(\{D, L\}, \sqcap, L)$, where $C^L A = A$ encodes live contexts and $C^D A = 1$ encodes dead contexts, where 1 is the unit type inhabited by a single value $()$. The *counit* operation $\varepsilon : C^L A \to A$ is defined $\varepsilon\, x = x$ and *coextend*, for all $f : C^r A \to B$, and thus $f^\dagger_{r,s} : C^{r \sqcap s} A \to C^s B$, is defined:

$$f^\dagger_{D,D} x = () \qquad f^\dagger_{D,L} x = f() \qquad f^\dagger_{L,D} x = () \qquad f^\dagger_{L,L} x = f\, x$$

The indexed family C^r here is analogous to the non-indexed Maybe (or *option*) data type $\mathsf{Maybe}\ A = A + 1$. This type does not permit a comonad structure since $\varepsilon : \mathsf{Maybe}\ A \to A$ is undefined at $(\mathsf{inr}\,())$. For the indexed comonad, ε need only be defined for $C^L A = A$. Thus, indexed comonads capture a broader range of contextual notions of computation than comonads.

Moreover, indexed comonads are not restricted by the *shape preservation* property of comonads [**?**]: that a coextended function cannot change the *shape* of the context. For example, in the second case above $f^\dagger_{D,L} : C^D A \to C^L B$ where the shape changes from 1 (empty context) to B (available context).

$$
\begin{aligned}
[\![C^r\Gamma \vdash \lambda x.e : C^s\tau_1 \to \tau_2]\!] &= \mathit{curry}\,([\![C^{r\wedge s}(\Gamma, x:\tau_1) \vdash e : \tau_2]\!] \circ m_{r,s}) \\
[\![C^{r\vee(s\oplus t)}\Gamma \vdash e_1\ e_2 : \tau]\!] &= (\mathit{uncurry}\,[\![C^r\Gamma \vdash e_1 : C^s\tau_1 \to \tau_2]\!]) \circ \\
&\qquad (\mathrm{id} \times [\![C^t\Gamma \vdash e_2 : \tau_1]\!]^\dagger_{t,s}) \circ n_{r,s\oplus t} \circ C^{r\vee(s\oplus t)}\Delta \\
[\![C^e\Gamma \vdash x_i : \tau_i]\!] &= \pi_i \circ \varepsilon
\end{aligned}
$$

Figure 10: Categorical semantics for the coeffect calculus

3.3.1 *Monoidal indexed comonads.*

Indexed comonads provide a semantics to sequential composition, but additional structure is needed for the semantics of the full coeffect calculus. Uustalu and Vene [60] additionally require a (*lax semi-*) *monoidal comonad* structure, which provides a monoidal operation $m : CA \times CB \to C(A \times B)$ for merging contexts (used in the semantics of abstraction).

The semantics of the coeffect calculus requires an indexed lax semi-monoidal structure for combining contexts *as well as* an indexed *colax* monoidal structure for *splitting* contexts. These are provided by two families of morphisms (given a coeffect algebra with $\vee$ and $\wedge$):

- $m_{r,s} : C^rA \times C^sB \to C^{(r\wedge s)}(A \times B)$ natural in A, B;
- $n_{r,s} : C^{(r\vee s)}(A \times B) \to C^rA \times C^sB$ natural in A, B;

The $m_{r,s}$ operation merges contextual computations with tags combined by $\wedge$ (greatest lower-bound), elucidating the behaviour of $m_{r,s}$: that merging may result in the loss of some parts of the contexts r and s.

The $n_{r,s}$ operation splits context-dependent computations and thus the contextual requirements. To obtain coeffects r and s, the input needs to provide *at least* r and s, so the tags are combined using the $\vee$ (least upper-bound).

For the sake of brevity, we elide the indexed versions of the laws required by Uustalu and Vene (e. g. most importantly, merging two contexts and then adding the third is equivalent to merging the last two and then adding the first; similar rule holds is required for splitting).

EXAMPLE For the indexed partiality comonad, given the liveness coeffect algebra $(\{D, L\}, \sqcap, \sqcup, \sqcap, L)$, the additional lax/colax monoidal operations are:

$$
\begin{array}{lll}
m_{L,L}(x,y) = (x,y) & n_{D,D}\ () = ((),()) & n_{D,L}(x,y) = ((),y) \\
m_{r,s}\ (x,y) = () & n_{L,D}(x,y) = (x,()) & n_{L,L}(x,y) = (x,y)
\end{array}
$$

EXAMPLE Uustalu and Vene model causal dataflow computations using the non-empty list comonad $\mathsf{NEList}\ A = A \times (1 + \mathsf{NEList}\ A)$ [60]. Whilst this comonad implies a trivial indexed comonad, we define an indexed comonad with integer indices for the number of past values demanded of the context.

We define $C^nA = A \times (A \times \ldots \times A)$ where the first A is the current (always available) value, followed by a finite product of n past values. The definition of the operations is a straightforward extension of the work of Uustalu and Vene.

3.3.2 *Categorical Semantics.*

Figure 10 shows the categorical semantics of the coeffect calculus using additional operations π_i for projection of the i^{th} element of a product, usual *curry* and *uncurry* operations, and $\Delta : A \to A \times A$ duplicating a value. While C^r is a family of object mappings, it is promoted to a family of functors with the derived morphism mapping $C^r(f) = (f \circ \varepsilon)^\dagger_{e,r}$.

The semantics of variable access and abstraction are the same as in Uustalu and Vene's semantics, modulo coeffects. Abstraction uses $\mathsf{m}_{r,s}$ to merge the outer context with the argument context for the context of the function body. The indices of e for ε and r, s for $\mathsf{m}_{r,s}$ match the coeffects of the terms. The semantics of application is more complex. It first duplicates the free-variable values inside the context and then splits this context using $\mathsf{n}_{r,s\oplus t}$. The two contexts (with different coeffects) are passed to the two subexpressions, where the argument subexpression, passed a context $(s \oplus t)$, is coextended to produce a context s which is passed into the parameter of the function subexpression (*cf.* given $f : A \to (B \to C)$, $g : A \to B$, then *uncurry* $f \circ (\mathrm{id} \times g) \circ \Delta : A \to C$).

A semantics for sub-coeffecting is omitted, but may be provided by an operation $\iota_{r,s} : C^r A \to C^s A$ natural in A, for all $r, s \in S$ where $s \leqslant r$, which transforms a value $C^r A$ to $C^s A$ by ignoring some of the encoded context.

3.4 SYNTAX-BASED EQUATIONAL THEORY

Operational semantics of every context-dependent language differs as the notion of context is always different. However, for coeffect calculi satisfying certain conditions we can define a universal equational theory. This suggests a pathway to an operational semantics for two out of our three examples (the notion of context for data-flow is more complex).

In a pure λ-calculus, β and η equality for functions (also called *local soundness* and *completeness* respectively [45]) describe how pairs of abstraction and application can be eliminated: $(\lambda x.e_2)e_1 \equiv_\beta e_1[x \leftarrow e_2]$ and $(\lambda x.e\,x) \equiv_\eta e$. The β equality rule, using the usual Barendregt convention of syntactic substitution, implies a *reduction*, giving part of an operational semantics for the calculus.

The call-by-name evaluation strategy modelled by β-reduction is not suitable for impure calculi therefore a restricted β rule, corresponding to call-by-value, is used, i. e. $(\lambda x.e_2)v \equiv e_2[x \leftarrow v]$. Such reduction can be encoded by a *let*-binding term, $\mathbf{let}\ x = e_1\ \mathbf{in}\ e_2$, which corresponds to sequential composition of two computations, where the resulting pure value of e_1 is substituted into e_2 [18, 36].

For an equational theory of coeffects, consider first a notion of *let*-binding equivalent to $(\lambda x.e_2)\ e_1$, which has the following type and coeffect rule:

$$\frac{C^s \Gamma \vdash e_1 : \tau_1 \qquad C^{r_1 \wedge r_2}(\Gamma, x : \tau_1) \vdash e_2 : \tau_2}{C^{r_1 \vee (r_2 \oplus s)}\Gamma \vdash \mathbf{let}\ x = e_1\ \mathbf{in}\ e_2 : \tau_2} \tag{1}$$

For our examples, $\wedge$ is idempotent (i. e., $r \wedge r = r$) implying a simpler rule:

$$\frac{C^s \Gamma \vdash e_1 : \tau_1 \qquad C^{r}(\Gamma, x : \tau_1) \vdash e_2 : \tau_2}{C^{r \vee (r \oplus s)}\Gamma \vdash \mathbf{let}\ x = e_1\ \mathbf{in}\ e_2 : \tau_2} \tag{2}$$

For our examples (but not necessarily *all* coeffect systems), this defines a more "precise" coeffect with respect to $\leqslant$ where $r \vee (r \oplus s) \leqslant r_1 \vee (r_2 \oplus s)$.

This rule removes the non-principality of the first rule (i. e. multiple possible typings). However, using idempotency to split coeffects in abstraction would remove additional flexibility needed by the implicit parameters example.

The coeffect $r \vee (r \oplus s)$ can also be simplified for all our examples, leading to more intuitive rules – for implicit parameters $r \cup (r \cup s) = r \cup s$; for liveness we get that $r \sqcup (r \sqcap s) = r$ and for dataflow we obtain $max(r, r + s) = r + s$.

Our calculus can be extended with *let*-binding and (2). However, we also consider the cases when a syntactic substitution $e_2[x \leftarrow e_1]$ has the coeffects specified by the above rule (2) and prove *subject reduction* theorem for certain coeffect calculi. We consider two common special cases when the coeffect of variables e is the greatest ($\top$) or least ($\bot$) element of the semi-lattice $(S, \vee)$ and derive additional conditions that have to hold about the coeffect algebra:

Lemma 1 (Substitution). *Given* $C^r(\Gamma, x : \tau_2) \vdash e_1 : \tau_1$ *and* $C^s\Gamma \vdash e_2 : \tau_2$ *then* $C^{r \vee (r \oplus s)}\Gamma \vdash e_2[x \leftarrow e_1] : \tau_1$ *if the coeffect algebra satisfies the conditions that* e *is either the greatest or least element of the semi-lattice,* $\oplus = \wedge$*, and* $\oplus$ *distributes over* $\vee$*, i. e.,* $X \oplus (Y \vee Z) = (X \oplus Y) \vee (X \oplus Z)$.

Proof. By induction over $\vdash$, using the laws (§3.2) and additional assumptions. □

Assuming $\rightarrow_\beta$ is the usual call-by-name reduction, the following theorem models the evaluation of coeffect calculi with coeffect algebra that satisfies the above requirements. We do not consider *call-by-value*, because our calculus does not have a notion of *value*, unless explicitly provided by *let*-binding (even a function "value" $\lambda x.e$ may have immediate contextual requirements).

Theorem 1 (Subject reduction). *For a coeffect calculus, satisfying the conditions of Lemma 1, if* $C^r\Gamma \vdash e : \tau$ *and* $e \rightarrow_\beta e'$ *then* $C^r\Gamma \vdash e' : \tau$.

Proof. A direct consequence of Lemma 1. □

The above theorem holds for both the liveness and resources examples, but not for dataflow. In the case of liveness, e is the greatest element ($r \vee e = e$); in the case of resources, e is the *least* element ($r \vee e = r$) and the proof relies on the fact that additional context-requirements can be placed at the context $C^r\Gamma$ (without affecting the type of function when substituted under λ abstraction).

However, the coeffect calculus also captures context-dependence in languages with more complex evaluation strategies than *call-by-name* reduction based on syntactic substitution. In particular, syntactic substitution does not provide a suitable evaluation for dataflow (because a substituted expression needs to capture the context of the original scope).

Nevertheless, the above results show that – unlike effects – context-dependent properties can be integrated with *call-by-name* languages. Our work also provides a model of existing work, namely Haskell implicit parameters [32].

3.5 RELATED AND FURTHER WORK

This paper follows the approaches of effect systems [24, 54, 70] and categorical semantics based on monads and comonads [36, 60]. Syntactically, *coeffects* differ from *effects* in that they model systems where λ-abstraction may split contextual requirements between the declaration-site and call-site.

Our *indexed (monoidal) comonads* (§3.3) fill the gap between (non-indexed) *(monoidal) comonads* of Uustalu and Vene [60] and indexed monads of Atkey [4], Wadler and Thiemann [70]. Interestingly, *indexed* comonads are *more general* than comonads, capturing more notions of context-dependence (§3.1).

COMONADS AND MODAL LOGICS. Bierman and de Paiva [9] model the $\Box$ modality of an intuitionistic S4 modal logic using monoidal comonads, which links our calculus to modal logics. This link can be materialized in two ways.

Pfenning et al. and Nanevski et al. derive term languages using the Curry-Howard correspondence [45, 9, 39], building a *metalanguage* (akin to Moggi's monadic metalanguage [36]) that includes $\Box$ as a type constructor. For example, in [45], the modal type $\Box\tau$ represents closed terms. In contrast, the *semantic* approach uses monads or comonads *only* as a semantics. This has been employed by Uustalu and Vene and (again) Moggi [36, 60]. We follow the semantic approach.

Nanevski et al. extend an S4 term language to a *contextual* modal type theory (CMTT) [39]. The *context* is a set of variables required by a computation, which makes CMTT useful for meta-programming and staged computations. Our contextual types are indexed by a coeffect algebra, which is more general and can capture variable contexts, but also integers, two-point lattices, *etc.*.

The work on CMTT suggests two extensions to coeffects. The first is developing the logical foundations. We briefly considered special cases of our system that permits local soundness in §3.4 and local completeness can be treated similarly. The second problem is developing the coeffects *metalanguage*. The use of coeffect algebras would provide an additional flexibility over CMTT, allowing a wider range of applications.

RELATING EFFECTS AND COEFFECTS. The difference between effects and coeffects is mainly in the (*abs*) rule. While the semantic model (monads vs. comonads) is very different, we can consider extending the two to obtain equivalent syntactic rules. To allow splitting of implicit parameters in lambda abstraction, the reader monad needs an operation that eagerly performs some effects of a function: $(\tau_1 \to M^{r\oplus s}\tau_2) \to M^r(\tau_1 \to M^s\tau_2)$. To obtain a pure lambda abstraction for coeffects, we need to restrict the $m_{r,s}$ operation of indexed comonads, so that the first parameter is annotated with e (meaning no effects): $C^e A \times C^r B \to C^r(A \times B)$.

STRUCTURAL COEFFECTS. To make the liveness analysis practical, we need to associate information with individual variables (rather than the entire context). We can generalize the calculus from this paper by adding a product operation $\times$ to the coeffect algebra. A variable context $x : \tau_1, y : \tau_2, z : \tau_3$ is then annotated with $r \times s \times t$ where each component of the tag corresponds to a single variable. The system then needs to be extended with structural rules such as:

$$(abs)\frac{C^{r\times s}(\Gamma, x:\tau_1) \vdash e : \tau_2}{C^r\Gamma \vdash \lambda x.e : C^s\tau_1 \to \tau_2} \qquad (contr)\frac{C^{r\times s}(x:\tau_1, y:\tau_1) \vdash e : \tau_2}{C^{r \sqcup s}(z:\tau_1) \vdash e[x \leftarrow z][y \leftarrow z] : \tau_2}$$

The context-requirements associated with function are exactly those linked to the specific variable of the lambda abstraction. Rules such as contraction manipulate variables and perform a corresponding operation on the indices.

The structural coeffect system is related to bunched typing [**?**] (but generalizes it by adding indices). We are currently investigating how to use structural coeffects to capture fine-grained context-dependence properties such as secure information flow [63] or, more generally, those captured by dependency core calculus [**?**].

3.6 CONCLUSIONS

We examined three simple calculi with associated static analyses (liveness analysis, implicit parameters, and dataflow analysis). These were unified in the *coeffect calculus*, providing a general coeffect system parameterised by

an algebraic structure describing the propagation of context requirements throughout a program.

We model the semantics of coeffect calculus using *indexed comonad* – a novel structure, which is more powerful than (monoidal) comonads. Indices of the indexed comonad operations manifest the semantic propagation of context such that the propagation of information in the general coeffect type system corresponds exactly to the semantic propagation of context in our categorical model.

We consider the analysis of context to be essential, not least for the examples here but also given increasingly rich and diverse distributed systems.

4 STRUCTURAL COEFFECT LANGUAGE

Introduction

4.1 INTRODUCTION

We already talked about tainting in pathways to coeffects... here is more stuff!

Our second motivating example is the use of *tainting* for the prevention of SQL injection attacks [**?**]. The idea is to (statically) check that SQL commands cannot be directly constructed from, potentially dangerous, inputs provided by the user. Consider the type checking of the following expression in a context containing variables id and msg:

$$\textbf{let}\ \mathsf{name} = \mathsf{query}\ (\texttt{"SELECT Name WHERE Id = "} + \mathsf{id})\ \textbf{in}$$
$$\mathsf{msg} + \mathsf{name}$$

We say that a variable is *tainted* if it may come from untrusted input. In the above example, id must not be tainted. Otherwise, the attacker could specify values such as `"1; DROP TABLE Users"`. The variable msg may or may not be tainted, because it is not used in protected context (i.e. to construct an SQL query). Using the coeffect calculus, security information can be naturally attached to the context. We use tag T for tainted and N for not tainted:

$$C^{\mathsf{T}\times\mathsf{N}}(\mathsf{id} : \mathsf{string}, \mathsf{msg} : \mathsf{string}) \vdash (\ldots) : \mathsf{string}$$

The tags T and N correspond to variables id and msg, respectively. The checking of tainting is a special case of checking of *non-interference* in *secure information flow* [47]. Languages such as FlowCaml [50] can check such properties statically, but it is also possible to embed such checking in a monadic library [46].

Assuming the monadic type $M^s\tau$ represents a value of type τ in a security context s (either T or N):

$$\mathsf{id} : M^{\mathsf{T}}\mathsf{string}, \mathsf{msg} : M^{\mathsf{N}}\mathsf{string} \vdash (\ldots) : M^{\mathsf{T}}\mathsf{string}$$

In this example, the result is tagged with T to denote that it may be tainted. If the result was tagged with N, the first parameter would also have to be N (and we would get fewer information about the function).

The monadic encoding has an unfortunate property from the semantic perspective. The function has monadic structure over the *domain* as well as over the *codomain* and thus it does not match the desirable Kleisli model of expressions $\tau_1 \times \ldots \tau_n \to M\tau$. This makes the it difficult to give standard composable semantics of the library.

In coeffect calculus, expressions are modelled using the coKleisli form $C^{r_1\times\ldots\times r_n}(\tau_1 \times \ldots \tau_n) \to \tau$ with a tags r_n that specify taintedness of inputs. As discussed in detail in Section 4.4.2, this model gives a simple comonadic semantics of language-based security using tainting.

$\boxed{C^r\Gamma \vdash e : \tau}$

$$\frac{}{C^0(v:\tau) \vdash v : \tau} \quad \lambda_{Cs}\text{-Tvar}$$

$$\frac{C^{r\times s}(\Gamma, v:\tau_1) \vdash e : \tau_2 \qquad v \notin \Gamma}{C^r\Gamma \vdash \lambda v.e : C^s\tau_1 \to \tau_2} \quad \lambda_{Cs}\text{-Tfun}$$

$$\frac{C^s\Gamma_1 \vdash e_1 : C^r\tau_1 \to \tau_2 \qquad C^t\Gamma_2 \vdash e_2 : \tau_1}{C^{s\times(r\vee t)}(\Gamma_1,\Gamma_2) \vdash e_1\ e_2 : \tau_2} \quad \lambda_{Cs}\text{-Tapp}$$

$$\frac{C^{r\times s}(\Gamma_1, v:\tau_1) \vdash e_1 : \tau_2 \qquad C^t\Gamma_2 \vdash e_2 : \tau_1}{C^{r\times(s\vee t)}(\Gamma_1,\Gamma_2) \vdash \textbf{let}\ x = e_2\ \textbf{in}\ e_1 : \tau_2} \quad \lambda_{Cs}\text{-Tlet}$$

$$\frac{C^r\Gamma \vdash e : \tau \qquad C^{r'}\Gamma' \Rightarrow_c C^r\Gamma}{C^{r'}\Gamma' \vdash e : \tau} \quad \lambda_{Cs}\text{-Tctx}$$

$\boxed{C^r\Gamma \Rightarrow_c C^r\Gamma}$

$$\frac{C^{r'}\Gamma_1' \Rightarrow_c C^r\Gamma_1}{C^{r'\times s}(\Gamma_1',\Gamma_2) \Rightarrow_c C^{r\times s}(\Gamma_1,\Gamma_2)} \quad \lambda_{Cs}\text{-Tnest}$$

$$C^{r\times s}(\Gamma_1,\Gamma_2) \Rightarrow_c C^{s\times r}(\Gamma_2,\Gamma_1) \quad \lambda_{Cs}\text{-Texch}$$

$$C^{r\times 1}(\Gamma,()) \Rightarrow_c C^r\Gamma \quad \lambda_{Cs}\text{-Tempty}$$

$$C^{r\times 0}(\Gamma, x:\tau_1) \Rightarrow_c C^r\Gamma \quad \lambda_{Cs}\text{-Tweak}$$

$$C^{r\vee s}(x:\tau) \Rightarrow_c C^{r\times s}(x:\tau, x:\tau) \quad \lambda_{Cs}\text{-Tcontr}$$

$$C^{r\times(s\times t)}(\Gamma_1,(\Gamma_2,\Gamma_3)) \Rightarrow_c C^{(r\times s)\times t}((\Gamma_1,\Gamma_2),\Gamma_3) \quad \lambda_{Cs}\text{-Tassoc}$$

$$C^r\Gamma \Rightarrow_c C^s\Gamma \quad (\text{when } s\vee r = s) \quad \lambda_{Cs}\text{-Tsub}$$

Figure 11: Type system for λ_{Cs}

4.2 STRUCTURAL COEFFECT SYSTEM

The *flat coeffect system* presented in the previous sections has a number of uses, but often we need to track context-dependence in a more fine-grained way. To track neededness or security, we need to associate information with individual *variables* of the context.

At the same time, we want to avoid developing multiple variants of coeffect systems – indeed, our motivation is to develop a *single unified mechanism* for tracking context-dependence. In this section, we present a more powerful *structural coeffect calculus* λ_{Cs}, which is a generalization of λ_{Cf}. We show that λ_{Cf} can be obtained as a special case of λ_{Cs}. The structural version of our system is also where our work differs more significantly from well-known effect systems.

4.2.1 *Motivation: Tracking array accesses*

Similarly to the flat version, the *structural coeffect calculus* works with contexts and functions annotated with a coeffectt tags, written $C^r\Gamma$ and $C^r\tau_1 \to \tau_2$, respectively, but we use richer tag structure.

As an example, consider a language that allows us to get a value of a variable (representing some changing data-source) x versions back using the syntax $a_{[x]}$. To track information about individual variables, we use a product-like operation $\times$ on tags to mirrors the product structure of variables. For example:

$$C^{5\times 10}(a : \mathsf{D}_{\mathsf{nat}}, b : \mathsf{D}_{\mathsf{nat}}) \vdash a_{[5]} + b_{[10]} : \mathsf{nat}$$

The coeffect tag 5×10 corresponds to the free-variable context a, b, denoting that we need at most 5 and 10 past values of a and b. If we substitute c for both a and b, we need another operation to combine multiple tags associated with a single variable:

$$C^{5\vee 10}(c : \mathsf{D}_{\mathsf{nat}}) \vdash c_{[5]} + c_{[10]} : \mathsf{nat}$$

In this example, the operation $\vee$ would be the *max* function and so $5 \vee 10 = 10$. Before looking at the formal definition, consider the typing of let bindings:

$$\textbf{let } c = \textbf{if } \mathsf{test}() \textbf{ then } a \textbf{ else } b$$
$$a_{[15]} + c_{[10]}$$

The expression has free variables a and b (we ignore test, which is not a data source). It defines c, which may be assigned either a or b. The variable a may be used directly (second line) or indirectly via c.

The expression assigned to c uses variables a and b, so its typing context is $C^{0\times 0}(a, b)$. The value 0 is the unit of $\vee$ and it denotes empty coeffect. The typing context of the body is $C^{15\times 10}(a, c)$.

To combine the tags, we take the coeffect associated with c and apply it to the tags of the context in which c was defined using the $\vee$ operation. This is then combined with the remaining tags from the body yielding the overall context: $C^{15\times(10\vee(0\times 0))}(a, (a, b))$. Using a simple normalization mechanism (described later), this can be further reduced to $C^{(15\vee 10)\times 10}(a, b)$. This gives us the required information – we need at most $max(15, 10)$ past values of a and at most 10 past values of b.

4.2.2 *Structural coeffect tags*

In the previous section, the $\vee$ operation behaves similarly to the flat $\vee$ operation. However, the type system does not require some of the semilattice properties, because some uses are replaced with the $\times$ operation. We do not require any properties about the $\times$ operation. For example, in the previous example cannot be commutative (since a tag 15×10 has different meaning than 10×15). However, we relate the operations using distributivity laws to allow normalization that was hinted above.

Definition 5. *A* structural coeffect tag structure $(S, \times, \vee, 0, 1)$ *is a tuple where* $(S, \vee)$ *is a lattice-like structure with unit* 0*. The additional structure is formed by*

a binary operation $\times$ *and element* $1 \in S$ *such that for all* $r, s, t \in S$*, the following equalities hold:*

$$r \vee (s \vee t) = (r \vee s) \vee t \qquad \text{(associativity)}$$
$$r \vee s = s \vee r \qquad \text{(commutativity)}$$
$$r \vee 0 = r \qquad \text{(lower bound)}$$
$$r \vee (s \times t) = (r \vee s) \times (r \vee t) \qquad \text{(distributivity)}$$
$$1 \vee r = 1 \qquad \text{(upper bound)}$$

The tag 0 represents that no coeffect is associated with a variable (i.e when a variable is always accessed using standard variable access). The tag 1 is used to annotate empty variable context. For example, the context of an expression $\lambda x.x$ is empty and it needs to carry an annotation. We explain exactly how this works when we introduce the type system. The fact that 1 is the upper bound means that combining it with other coeffect annotations does not affect it and so empty contexts cannot carry any information.

The structure generalizes the *flat coeffect tag structure* introduced in Section **??**, but it additionally requires a special element 1 representing the upper bound. Given a flat coeffect structure, we can construct a structural coeffect structure (but not the other way round). For certain structures, the element 1 may be already present, but in general, it can be added as a new element. This construction will be important in Section **??**, where we show that λ_{Cs} calculus generalizes λ_{Cf}.

Lemma 2. *A flat coeffect tag structure* $(S, \vee, 0)$ *implies a structural coeffect tag structure.*

Proof. Take $1 \notin S$, then $(S \cup \{1\}, \vee, \vee, 0, 1)$ is a structural coeffect tag structure. From the properties of flat coeffect tag structure, we get that the $\vee$ operation is associative, commutative and 0 is the unit with respect to $\vee$.

To prove the distributivity, we need to show $r \vee (s \vee t) = (r \vee s) \vee (r \vee t)$. This easily follows from commutativity, associativity and idempotence of the flat coeffect tag structure. □

4.2.3 *Structural coeffect type system*

The simply typed system for λ_{Cs} uses the same syntax of types as the system for λ_{Cf}. The rules are of a form $C^r \Gamma \vdash e : \tau$ where r is a tag provided by a *structural coeffect tag structure* $(S, \times, \vee, 0)$.

The system differs from λ_{Cf} in a significant aspect. It contains explicit structural rules that manipulate with the context. Such rules allow reordering, duplicating and other manipulations with variable context. Such rules are known from affine or linear type systems where they are removed to obtain more restrictive system. In our system, the rules are present, but they manipulate the variable structure Γ as well as the associated tag structure r.

As in linear and affine systems, the variable context Γ in our system is not a simple set. Instead, we use the following tree-like structure (which is more similar to bunched types than to linear or affine systems):

$$\Gamma ::= () \mid (x : \tau) \mid (\Gamma, \Gamma)$$

The syntax $()$ represents an empty context, so the structure defines a binary trees where leaves are either variables or empty. Contexts such as $C^{1 \times (r \times 1)}((), (x, ()))$ contain unnecessary number of empty contexts $()$. However, we need to construct them temporarily, because certain rules require splitting a context and, by our definition, the context $(x : \tau)$ is not splitable.

The typing rules of the system are shown in Figure 11. Many of the structural rules are expressed in terms of a helper judgement $C^r\Gamma \Rightarrow_c C^r\Gamma$.

STANDARD RULES. Variable access (λ_{Cs} -Tvar) annotates the corresponding variable with an empty coeffect 0. The λ_{Cs} -Tfun rule assumes that the context of the body can be split into the variable of the function and other (potentially empty) context and it attaches the coeffect associated with the function variable to the resulting function type $C^s\tau_1 \to \tau_2$.

The λ_{Cs} -Tapp rule combines coeffects s, t, r associated with the function-returning expression, argument and the function type respectively. The result of evaluating the argument in the context t is passed to the function that requires context r, so the variables used in the context Γ_2 are annotated with the combination of coeffects $r \vee t$. The variable context required to evaluate the function value is independent and so it is annotated just with coeffects s. Finally, the λ_{Cs} -Tlet rule is derived from let binding and application, but we show it separately to aid the understanding.

STRUCTURAL RULES. The remaining rules are not syntax-directed. They are embedded using the λ_{Cs} -Tctx rule and expressed using a helper judgement $C^{r_1}\Gamma_1 \Rightarrow_c C^{r_2}\Gamma_2$ that says that the context on the left-hand side can be transformed to the context on the right-hand side. The transformation can be applied to any part of the context, which is captured using the λ_{Cs} -Tnest rule (it is sufficient to apply the transformation on the left part of the context; the right part can be transformed using λ_{Cs} -Texch).

The λ_{Cs} -Tempty rule allows attaching empty context to any existing context. The rule is needed to type-check lambda abstractions that do not capture any outer variable. The λ_{Cs} -Tweak rule is similar, but it represents *weakening* where an unused variable is added. The associated coeffect tag does not associate context information with the variable. This is needed to type-check lambda abstraction that does not use the argument.

The λ_{Cs} -Tcontr rule is a limited form of contraction. When a variable appears repeatedly, it can be reduced to a single occurrence. The rule is needed to satisfy the side condition of λ_{Cs} -Tfun when the body uses the argument repeatedly. The two associativity rules together with λ_{Cs} -Texch provide ways to rearrange variables. Finally, λ_{Cs} -Tsub represents sub-coeffecting – in λ_{Cs} the rule operates on coeffects of individual variables.

4.2.4 *Properties of reductions*

Similarly to the flat version, the λ_{Cs} calculus is defined abstractly. We cannot define its operational meaning, because that will differ for every concrete application. For example, when tracking array accesses, variables are interpreted as arrays and $a_{[n]}$ denotes access to a specified element.

Just like previously, we can state general properties of the reductions. As the syntax of expressions is the same for λ_{Cs} as for λ_{Cf}, the substitution and reduction $\twoheadrightarrow_\beta$ are also the same and can be found in Figure **??**.

The structural coeffect calculus λ_{Cs} associates information with individual variables. This means that when an expression requires certain context, we know from what scope it comes – the context must be provided by a scope that defines the associated variable, which is either a lambda abstraction or global scope. This distinguishes the structural system from the flat system where context could have been provided by any scope and the lambda rule

$$
\begin{array}{rcl}
C^{1}()[r'|\Gamma'] & = & C^{1}() \\
C^{r}(x:\tau)[r'|\Gamma'] & = & C^{r}(x:\tau) \\
C^{-}(-)[r'|\Gamma'] & = & C^{r'}\Gamma' \\
C^{r_1 \times r_2}(\Gamma_1,\Gamma_2)[r'|\Gamma'] & = & C^{r_1' \times r_2'}(\Gamma_1',\Gamma_2') \\
 & & \text{where } C^{r_i'}\Gamma_i' = C^{r_i}\Gamma_i[r'|\Gamma']
\end{array}
$$

Figure 12: The definition of hole filling operation $\Delta[-]$

allowed arbitrary splitting of context requirements between the two scopes (or declaration and caller site).

INTERNALIZED SUBSTITUTION. Before looking at properties of the evaluation, we consider let binding, which can be viewed as internalized substitution. The typing rule λ_{Cs} -Tlet can be derived from application and abstraction as follows.

Lemma 3 (Definition of let binding). *If* $C^{r}\Gamma \vdash (\lambda x.e_2)\ e_1 : \tau_2$ *then* $C^{r}\Gamma \vdash \textsf{let}\ x = e_1\ \textsf{in}\ e_2 : \tau_2$.

Proof. The premises and conclusions of a typing derivation of $(\lambda x.e_2)\ e_1$ correspond with the typing rule λ_{Cs} -Tlet:

$$
\dfrac{\dfrac{C^{r\times s}(\Gamma_1, v:\tau_1) \vdash e_2 : \tau_2 \qquad v \notin \Gamma_1}{C^{r}\Gamma_1 \vdash \lambda v.e_2 : C^{s}\tau_1 \to \tau_2} \qquad C^{t}\Gamma_2 \vdash e_1 : \tau_1}{C^{r\times(s\vee t)}(\Gamma_1,\Gamma_2) \vdash (\lambda v.e_2)\ e_1 : \tau_2}
$$

□

The term e_2 which is substituted in e_1 is checked in a different variable and coeffect context $C^{t}\Gamma_2$. This is common in sub-structural systems where a variable cannot be freely used repeatedly. The context Γ_2 is used in place of the variable that we are substituting for. The let binding captures substitution for a specific variable (the context is of a form $C^{r\times s}\Gamma, v:\tau$). For a general substitution, we need to define the notion of context with a hole.

SUBSTITUTION AND HOLES. In λ_{Cs}, the structure of the variable context is not a set, but a tree. When substituting for a variable, we need to replace the variable in the context with the context of the substituted expression. In general, this can occur anywhere in the tree. To formulate the statement, we define contexts with holes, written $\Delta[-]$. Note that there is a hole in the free variable context and in a corresponding part of the coeffect tag:

$$
\begin{array}{rcll}
\Delta[-] & ::= & C^{1}() & \\
 & | & C^{r}(x:\tau) & \\
 & | & C^{-}(-) & \\
 & | & C^{r_1\times r_2}(\Gamma_1,\Gamma_2) & (\text{where } C^{r_i}\Gamma_i \in \Delta[-])
\end{array}
$$

Assuming we have a context with hole $C^{r}\Gamma \in \Delta[-]$, the hole filling operation $C^{r}\Gamma[r'|\Gamma']$ fills the hole in the variable context with Γ' and the corresponding coeffect tag hole with r'. The operation is defined in Figure 12. Using contexts with holes, we can now formulate the general substitution lemma for λ_{Cs}.

Lemma 4 (Substitution Lemma). *If* $C^{r}\Gamma[R|v:\tau'] \vdash e : \tau$ *and* $C^{S}\Gamma' \vdash e' : \tau'$ *then* $C^{r}\Gamma[R \vee S|\Gamma'] \vdash e[v \leftarrow e'] : \tau$.

Proof. Proceeds by rule induction over $\vdash$ using the properties of structural coeffect tag structure $(S, \vee, 0, \times, 1)$ (see Appendix **??**). □

Theorem 2 (Subject reduction). *If* $C^r\Gamma \vdash e_1 : \tau$ *and* $e_1 \twoheadrightarrow_\beta e_2$ *then* $C^r\Gamma \vdash e_2 : \tau$.

Proof. Direct consequence of Lemma 4 (see Appendix **??**). □

LOCAL SOUNDNESS AND COMPLETENESS. As with the previous calculus, we want to guarantee that the introduction and elimination rules (λ_{Cs} -Tfun and λ_{Cs} -Tapp) are appropriately strong. This can be done by showing *local soundness* and *local completeness*, which correspond to β-reduction and η-expansion. Former is a special case of subject reduction and the latter is proved by a simple derivation:

Theorem 3 (Local soundness). *If* $C^r\Gamma \vdash (\lambda x.e_2)\ e_1 : \tau$ *then* $C^r\Gamma \vdash e_2[x \leftarrow e_1] : \tau$.

Proof. Special case of subject reduction (Theorem 2). □

Theorem 4 (Local completeness). *If* $C^r\Gamma \vdash f : C^s\tau_1 \to \tau_2$ *then* $C^r\Gamma \vdash \lambda x.fx : C^s\tau_1 \to \tau_2$.

Proof. The property is proved by the following typing derivation:

$$\dfrac{\dfrac{C^r\Gamma \vdash f : C^s\tau_1 \to \tau_2 \qquad C^0(x : \tau_1) \vdash x : \tau_1}{C^{r\times(s\vee 0)}(\Gamma, x : \tau_1) \vdash f\ x : \tau_2}}{C^r\Gamma \vdash \lambda x.fx : C^s\tau_1 \to \tau_2}$$ □

In the last step, we use the *lower bound* property of structural coeffect tag, which guarantees that $s \vee 0 = s$. Recall that in λ_{Cf}, the typing derivation for $\lambda x.fx$ required for local completeness was not the only possible derivation. In the last step, it was possible to split the coeffect tag arbitrarily between the context and the function type.

In the λ_{Cs} calculus, this is not, in general, the case. The $\times$ operator is not required to be associative and to have units and so a unique splitting may exist. For example, if we define $\times$ as the operator of a *free magma*, then it is invertible and for a given t, there are unique r and s such that $t = r \times s$. However, if the $\times$ operation has additional properties, then there may be other possible derivation.

4.3 SEMANTICS OF STRUCTURAL COEFFECTS

The semantics of structural coeffect calculus λ_{Cs} can be defined similarly to the semantics of λ_{Cf}. The most notable difference is that the structure of coeffect tag now mirrors the structure of the variable context. Thus an expression $C^{r\times s}(\Gamma_1, \Gamma_2) \vdash e : \tau$ is modelled as a function $C^{r\times s}(\Gamma_1 \hat{\times} \Gamma_2) \to \tau$.

As discussed in 4.2.3, the variable context Γ in structural coeffect system is not a simple finite product, but instead a binary tree. To model this, we do not use ordinary products in the domain of the semantic function, but instead use a special constructor $\hat{\times}$. This way, we can guarantee that the variable structure corresponds to the tag structure.

$$[\![C^{r_1\times\ldots\times r_n}(x_1:\tau_1\times\ldots\times x_n:\tau_n)\vdash e:\tau]\!] : C^{r_1\times\ldots\times r_n}(\tau_1\times\ldots\times\tau_n)\to\tau$$

$$\begin{aligned}
[\![C^0\Gamma\vdash x_i:\tau_i]\!] &= \epsilon_0\\
[\![C^r\Gamma\vdash \lambda x.e : C^s\tau_1\to\tau_2]\!] &= \Lambda([\![C^{r\times s}(\Gamma,x:\tau_1)\vdash e:\tau_2]\!]\circ \mathsf{m}_{r,s})\\
[\![C^{s\times(r\vee t)}(\Gamma_1,\Gamma_2)\vdash e_1\ e_2:\tau]\!] &= (\lambda(\gamma_1,\gamma_2)\to [\![C^s\Gamma_1\vdash e_1 : C^r\tau_1\to\tau_2]\!]\ \gamma_1\ ([\![C^t\Gamma_2\vdash e_2:\tau_1]\!]^\dagger_{t,r}\ \gamma_2\\
[\![C^{r'}\Gamma'\vdash e:\tau]\!] &= [\![C^r\Gamma\vdash e:\tau]\!]\circ[\![C^{r'}\Gamma'\Rightarrow_c C^r\Gamma]\!]
\end{aligned}$$

$$\begin{aligned}
[\![C^{r'\times s}(\Gamma_1',\Gamma_2)\Rightarrow_c C^{r\times s}(\Gamma_1,\Gamma_2)]\!] &= \mathsf{m}_{r,s}\circ([\![C^{r'}\Gamma_1'\Rightarrow_c C^r\Gamma_1]\!]\times\mathsf{id})\circ \mathsf{n}_{r',s}\\
[\![C^{r\times s}(\Gamma_1,\Gamma_2)\Rightarrow_c C^{s\times r}(\Gamma_2,\Gamma_1)]\!] &= \mathsf{m}_{s,r}\circ\mathsf{swap}\circ\mathsf{n}_{r,s}\\
[\![C^{r\times 1}(\Gamma,())\Rightarrow_c C^r\Gamma]\!] &= \mathsf{fst}\circ\mathsf{n}_{r,1}\\
[\![C^{r\times 0}(\Gamma,x:\tau)\Rightarrow_c C^r\Gamma]\!] &= \mathsf{fst}\circ\mathsf{n}_{r,0}\\
[\![C^{r\vee s}(x:\tau)\Rightarrow_c C^{r\times s}(x:\tau,x:\tau)]\!] &= \mathsf{m}_{r,s}\circ\Delta_{r,s}\\
[\![C^{r\times(s\times t)}(\Gamma_1,(\Gamma_2,\Gamma_3))\Rightarrow_c C^{(r\times s)\times t}((\Gamma_1,\Gamma_2),\Gamma_3)]\!] &= \mathsf{m}_{r\times s,t}\circ(\mathsf{m}_{r,s}\times\mathsf{id})\circ\mathsf{assoc}_1\circ(\mathsf{id}\times\mathsf{n}_{s,t})\circ\mathsf{n}_{r,}\\
[\![C^r\Gamma\Rightarrow_c C^s\Gamma]\!] &= \iota_{r,s}
\end{aligned}$$

Figure 13: Categorical semantics for λ_{Cs}

4.3.1 *Structural tagged comonads*

To model composition of functions, we reuse the definition of *tagged comonads* from Section **??** without any change. This means that composing morphisms $T^r\tau_1\to\tau_2$ with $T^s\tau_2\to\tau_3$ still gives us a morphism $T^{r\vee s}\tau_1\to\tau_3$ and we use the $\vee$ operation to combine the context-requirements.

However, functions that do not exist in context have only a single input variable (with a single corresponding tag). To model complex variable contexts, we need two additional operations that allow manipulation with the variable context. Similarly to the model of λ_{Cf}, we also require operations that model duplication and sub-coeffecting:

Definition 6 (Structural tagged comonad)**.** *Given a structural coeffect tag structure* $(S,\times,\vee,0,1)$ *a* structural tagged comonad *is a tagged comonad over* $(S,\vee,0)$ *comprising of* T^r, ϵ_0 *and* $(-)^\dagger_{r,s}$ *together with a mapping* $-\hat{\times}-$ *from a pair of objects* $\mathrm{obj}(\mathcal{C})\times\mathrm{obj}(\mathcal{C})$ *to an object* $\mathrm{obj}(\mathcal{C})$ *and families of mappings:*

$$\begin{aligned}
\mathsf{m}_{r,s} &: T^rA\times T^sB\to T^{(r\times s)}(A\hat{\times}B)\\
\mathsf{n}_{r,s} &: T^{(r\times s)}(A\hat{\times}B)\to T^rA\times T^sN
\end{aligned}$$

And with a family of mappings $\iota_{r,s} : T^rA\to T^sA$ *for all* $r,s\in S$ *such that* $r\vee s = r$.

The family of mappings $\iota_{r,s}$ is the same as for *flat* coeffects and it can still be used to define a family of mappings that represents *duplicating* of variables while splitting the additional coeffect tags:

$$\begin{aligned}
&\Delta_{r,s} : T^{(r\vee s)}A\to T^rA\times T^sA\\
&\Delta_{r,s}(\gamma) = (\iota_{(r\vee s),r}\ \gamma,\iota_{(r\vee s),s}\ \gamma)
\end{aligned}$$

The type of the $\mathsf{m}_{r,s}$ operation looks similar to the one used for *flat* coeffects, but with two differences. Firstly, it combines tags using $\times$ instead of $\vee$, which corresponds to the fact that the variable context now consists of two parts (a tree node). Secondly, to model the tree node, the resulting context is modelled as $A \hat{\times} B$ (instead of $A \times B$ as previously).

To model structural coeffects, we also need $\mathsf{n}_{r,s}$, which serves as the dual of $\mathsf{m}_{r,s}$. It represents *splitting* of context containing multiple variables. The operation was not needed for λ_{Cf}, because there *splitting* could be defined in terms of *duplication* provided by $\Delta_{r,s}$. For λ_{Cs}, the situation is different. The $\mathsf{n}_{r,s}$ operation takes a context annotated with $r \times s$ that carries $A \hat{\times} B$.

Examples of *structural tagged comonads* are shown in Section 4.4.2. Before looking at them, we finish our discussion of categorical semantics.

CATEGORICAL NOTES. The mapping T^r can be extended to an endofunctor $\hat{T}^r$ in the same way as in Section **??**. However, we still cannot freely manipulate the variables in the context. Given a context modelled as $T^{r \times s}(A \hat{\times} B)$, we can lift a morphism f to $\hat{T}^{r \times s}(f)$, but we cannot manipulate the variables, because $A \hat{\times} B$ is not a product and does not have projections π_i.

This also explains why n cannot be defined in terms of Δ. Even if we could apply $\Delta_{r,s}$ on the input (if the tag $r \times s$ coincided with tag $r \vee s$) we would still not be able to obtain $T^r A$ from $T^r(A \hat{\times} B)$.

This restriction is intentional – at the semantic level, it prevents manipulations with the context that would break the correspondence between tag structure and the product structure.

4.3.2 *Categorical semantics*

The categorical semantics of $\lambda_{\mathsf{Cs}}$is shown in Figure 13. It uses the *structural tagged comonad* structure introduced in the previous section, together with the helper operation $\Delta_{r,s}$ and the following simple helper operations:

$$\begin{aligned} \mathsf{assoc} &= \lambda(\delta_r, (\delta_s, \delta_t)) \to ((\delta_r, \delta_s), \delta_t) \\ \mathsf{swap} &= \lambda(\gamma_1, \gamma_2) \to (\gamma_2, \gamma_1) \\ f \times g &= \lambda(x, y) \to (f\ x, g\ y) \end{aligned}$$

When compared with the semantics of λ_{Cf}(Figure **??**), there is a number of notable differences. Firstly, the rule λ_{Cs} -Svar is now interpreted as ϵ_0 without the need for projection π_i. When accessing a variable, the context contains only the accessed variable. The λ_{Cs} -Sfun rule has the same structure – the only difference is that we use the $\times$ operator for combining context tags instead of $\vee$ (which is a result of the change of type signature in $\mathsf{m}_{r,s}$).

The rule λ_{Cs} -Sapp now uses the operation $\mathsf{n}_{s,(r \vee t)}$ instead of $\Delta_{s,(r \vee t)}$, which means that it splits the context instead of duplicating it. This makes the system more structural – the expressions use disjunctive parts of the context – and also explains why the composed coeffect tag is $s \times (r \vee t)$.

The only rule from λ_{Cf} that was not syntax-directed (λ_{Cf} -Ssub) is now generalized to a number of non-syntax-directed rules λ_{Cs} -SC that perform various manipulations with the context. The semantics of $[\![C^{r_1}\Gamma_1 \Rightarrow_c C^{r_2}\Gamma_2]\!]$ is a function that, when given a context $C^{r_1}\Gamma_1$ produces a new context $C^{r_2}\Gamma_2$. The semantics in λ_{Cs} -Sctx then takes a context, converts it to a new context which is compatible with the original expression e. The context manipulation rules work as follows:

- The λ_{Cs} -SCnest and λ_{Cs} -SCexch rules use $n_{r,s}$ to split the context into a product of contexts, then perform some operation with the contexts – transform one and swap them, respectively. Finally, they re-construct a single context using $m_{r,s}$.
- The λ_{Cs} -SCempty and λ_{Cs} -SCweak rules have the same semantics. They both split the context and discard one part (containing either an unused variable or an empty context).
- If we interpreted λ_{Cs} -SCcontr by applying functor $T^{r \vee s}$ to a function that duplicates a variable, the resulting context would be $C^{r \vee s}(x : \tau, x : \tau)$, which would break the correspondence between coeffect tag and context variable structure. However, that interpretation would be incorrect, because we use $\hat{\times}$ instead of normal product for variable contexts. As a result, the rule has to be interpreted as a composition of $\Delta_{r,s}$ and $m_{r,s}$, which also turns a tag $r \vee s$ into $r \times s$.
- The λ_{Cs} -SCassoc rule is similar to λ_{Cs} -SCexch in the sense that it de-constructs the context, manipulates it (using assoc) and then re-constructs it.
- Finally, the λ_{Cs} -SCsub rule interprets sub-coeffecting on the context associated with a single variable using the primitive natural transformation $\iota_{r,s}$.

ALTERNATIVE: SEPARATE VARIABLES. As an alternative, we could model an expression by attaching the context separately to individual variables. This an expression $C^{r \times s}(\Gamma_1, \Gamma_2) \vdash e : \tau$ would be modelled as $C^r\Gamma_1 \times C^s\Gamma_2 \to \tau$. However, this approach largely complicates the definition of application (where tag of all variables in a context is affected). Moreover, it makes it impossible to express λ_{Cf} in terms of λ_{Cs} as discussed in Section **??**.

ALTERNATIVE: WITHOUT SUB-COEFFECTING. The semantics presented above uses the natural transformation $\iota_{r,s}$, which represents sub-coeffecting, to define the duplication operation $\Delta_{r,s}$. However, structural coeffect calculus λ_{Cs}does not require sub-coeffecting in the same way as flat λ_{Cf}(where it is required for subject reduction).

This means that it is possible to define a variant of the system that does not have the λ_{Cs} -Tsub typing rule. Then the semantics does not need the $\iota_{r,s}$ transformation, but instead, the following natural transformation has to be provided:

$$\Delta_{r,s} : T^{(r \vee s)}A \to T^rA \times T^sA$$

This variant of the system could be used to define a system that ensures that all provided context is used and is not over-approximated. This difference is similar to the difference between affine type systems (where a variable can be used at most once) and linear type systems (where a variable has to be used exactly once).

4.4 EXAMPLES OF STRUCTURAL COEFFECTS

4.4.1 *Example: Neededness analysis*

4.4.2 *Example: Tracking tainting*

4.5 SUMMARY

Oops!

5 COEFFECT META-LANGUAGE

Introduction

5.1 INTRODUCTION

?

5.2 SUMMARY

Oops!

$$(\textit{var})\ \frac{x : \alpha \in \Gamma}{\Gamma \vdash x : \alpha}$$

$$(\textit{app})\ \frac{\Gamma \vdash e_1 : \alpha \to \beta \qquad \Gamma \vdash e_2 : \alpha}{\Gamma \vdash e_1\ e_2 : \beta}$$

$$(\textit{abs})\ \frac{\Gamma, x : \alpha \vdash e : \beta}{\Gamma \vdash \lambda x.e : \alpha \to \beta}$$

$$(\textit{letbox})\ \frac{\Gamma \vdash e_1 : C^{r \oplus s}\,\alpha \qquad \Gamma, x : C^{r}\,\alpha \vdash e_2 : \beta}{\Gamma \vdash \textbf{let box}\ x = e_1\ \textbf{in}\ e_2 : C^{s}\,\beta}$$

$$(\textit{eval})\ \frac{\Gamma \vdash e : C^{e}\alpha}{\Gamma \vdash\, !e : \alpha}$$

$$(\textit{sub})\ \frac{\Gamma \vdash e : C^{s}\alpha}{\Gamma \vdash e : C^{r}\alpha}\ (s \leqslant r)$$

Figure 14: Type system for the coeffect meta-language λ_{cm}

[1] M. Abadi, A. Banerjee, N. Heintze, and J. G. Riecke. A core calculus of dependency. In *Proceedings of POPL*, 1999.

[2] D. Ahman, J. Chapman, and T. Uustalu. When is a container a comonad? In *Proceedings of the 15th international conference on Foundations of Software Science and Computational Structures*, FOSSACS'12, pages 74–88, Berlin, Heidelberg, 2012. Springer-Verlag.

[3] A. W. Appel. *Modern compiler implementation in ML*. Cambridge University Press, 1998.

[4] R. Atkey. Parameterised notions of computation. *J. Funct. Program.*, 19, 2009.

[5] J. E. Bardram. The java context awareness framework (jcaf)–a service infrastructure and programming framework for context-aware applications. In *Pervasive Computing*, pages 98–115. Springer, 2005.

[6] A. Benveniste, P. Caspi, S. A. Edwards, N. Halbwachs, P. Le Guernic, and R. De Simone. The synchronous languages 12 years later. *Proceedings of the IEEE*, 91(1):64–83, 2003.

[7] G. Biegel and V. Cahill. A framework for developing mobile, context-aware applications. In *Pervasive Computing and Communications, 2004. PerCom 2004. Proceedings of the Second IEEE Annual Conference on*, pages 361–365. IEEE, 2004.

[8] G. Bierman, M. Hicks, P. Sewell, G. Stoyle, and K. Wansbrough. Dynamic rebinding for marshalling and update, with destruct-time ? In *Proceedings of the eighth ACM SIGPLAN international conference on Functional programming*, ICFP '03, pages 99–110, New York, NY, USA, 2003. ACM.

[9] G. M. Bierman and V. C. V. de Paiva. On an intuitionistic modal logic. *Studia Logica*, 65:2000, 2001.

[10] S. Brookes and S. Geva. Computational comonads and intensional semantics. Applications of Categories in Computer Science. London Mathematical Society Lecture Note Series, Cambridge University Press, 1992.

[11] J. Cheney, A. Ahmed, and U. A. Acar. Provenance as dependency analysis. In *Proceedings of the 11th international conference on Database programming languages*, DBPL'07, pages 138–152, Berlin, Heidelberg, 2007. Springer-Verlag.

[12] E. Cooper, S. Lindley, P. Wadler, and J. Yallop. Links: Web programming without tiers. FMCO '00, 2006.

[13] P. Costanza and R. Hirschfeld. Language constructs for context-oriented programming: an overview of contextl. In *Proceedings of the 2005 symposium on Dynamic languages*, DLS '05, pages 1–10, New York, NY, USA, 2005. ACM.

[14] K. Crary, D. Walker, and G. Morrisett. Typed memory management in a calculus of capabilities. In *Proceedings of the 26th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 262–275. ACM, 1999.

[15] R. Davies and F. Pfenning. A modal analysis of staged computation. *J. ACM*, 48(3):555–604, May 2001.

[16] Developers (Android). Creating multiple APKs for different API levels. http://developer.android.com/training/multiple-apks/api.html, 2013.

[17] W. Du and L. Wang. Context-aware application programming for mobile devices. In *Proceedings of the 2008 C3S2E conference*, C3S2E '08, pages 215–227, New York, NY, USA, 2008. ACM.

[18] A. Filinski. Monads in action. In *Proceedings of POPL*, 2010.

[19] A. Filinski. Towards a comprehensive theory of monadic effects. In *Proceeding of the 16th ACM SIGPLAN international conference on Functional programming*, ICFP '11, pages 1–1, 2011.

[20] C. Flanagan and M. Abadi. Types for Safe Locking. ESOP '99, 1999.

[21] C. Flanagan and S. Qadeer. A type and effect system for atomicity. In *Proceedings of Conference on Programming Language Design and Implementation*, PLDI '03.

[22] O. Frieder and M. E. Segal. On dynamically updating a computer program: From concept to prototype. *Journal of Systems and Software*, 14(2):111–128, 1991.

[23] M. Gabbay and A. Nanevski. Denotation of syntax and metaprogramming in contextual modal type theory (cmtt). *CoRR*, abs/1202.0904, 2012.

[24] D. K. Gifford and J. M. Lucassen. Integrating functional and imperative programming. In *Proceedings of Conference on LISP and func. prog.*, LFP '86, 1986.

[25] N. Halbwachs, P. Caspi, P. Raymond, and D. Pilaud. The synchronous data flow programming language lustre. *Proceedings of the IEEE*, 79(9):1305–1320, 1991.

[26] W. Halfond, A. Orso, and P. Manolios. Wasp: Protecting web applications using positive tainting and syntax-aware evaluation. *IEEE Trans. Softw. Eng.*, 34(1):65–81, Jan. 2008.

[27] W. G. Halfond, A. Orso, and P. Manolios. Using positive tainting and syntax-aware evaluation to counter sql injection attacks. In *Proceedings of the 14th ACM SIGSOFT international symposium on Foundations of software engineering*, pages 175–185. ACM, 2006.

[28] M. Hicks, J. T. Moore, and S. Nettles. *Dynamic software updating*, volume 36. ACM, 2001.

[29] R. Hirschfeld, P. Costanza, and O. Nierstrasz. Context-oriented programming. *Journal of Object Technology*, 7(3), 2008.

[30] P. Jouvelot and D. K. Gifford. Communication Effects for Message-Based Concurrency. Technical report, Massachusetts Institute of Technology, 1989.

[31] R. B. Kieburtz. Codata and Comonads in Haskell, 1999.

[32] J. R. Lewis, M. B. Shields, E. Meijert, and J. Launchbury. Implicit parameters: dynamic scoping with static types. In *Proceedings of POPL*, POPL '00, 2000.

[33] F. Loitsch and M. Serrano. Hop client-side compilation. *Trends in Functional Programming, TFP*, pages 141–158, 2007.

[34] J. M. Lucassen and D. K. Gifford. Polymorphic effect systems. In *Proceedings of the 15th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, POPL '88, pages 47–57, New York, NY, USA, 1988. ACM.

[35] E. Meijer, B. Beckman, and G. Bierman. Linq: reconciling object, relations and xml in the .net framework. In *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*, SIGMOD '06, pages 706–706, New York, NY, USA, 2006. ACM.

[36] E. Moggi. Notions of computation and monads. *Inf. Comput.*, 93:55–92, July 1991.

[37] T. Murphy, VII., K. Crary, and R. Harper. Type-safe distributed programming with ML5. TGC'07, pages 108–123, 2008.

[38] T. Murphy VII, K. Crary, R. Harper, and F. Pfenning. A symmetric modal lambda calculus for distributed computing. LICS '04, pages 286–295, 2004.

[39] A. Nanevski, F. Pfenning, and B. Pientka. Contextual modal type theory. *ACM Trans. Comput. Logic*, 9(3):23:1–23:49, June 2008.

[40] P. O'Hearn. On bunched typing. *J. Funct. Program.*, 13(4):747–796, July 2003.

[41] P. W. O'Hearn, J. C. Reynolds, and H. Yang. Local reasoning about programs that alter data structures. In *Proceedings of the 15th International Workshop on Computer Science Logic*, CSL '01, pages 1–19, London, UK, UK, 2001. Springer-Verlag.

[42] D. Orchard. Programming contextual computations.

[43] T. Petricek. Client-side scripting using meta-programming.

[44] T. Petricek. Evaluations strategies for monadic computations. In *Proceedings of Mathematically Structured Functional Programming*, MSFP 2012.

[45] F. Pfenning and R. Davies. A judgmental reconstruction of modal logic. *Mathematical. Structures in Comp. Sci.*, 11(4):511–540, Aug. 2001.

[46] A. Russo, K. Claessen, and J. Hughes. A library for light-weight information-flow security in haskell. In *Proceedings of the first ACM SIGPLAN symposium on Haskell*, Haskell '08, pages 13–24, 2008.

[47] A. Sabelfeld and A. C. Myers. Language-based information-flow security. *IEEE J.Sel. A. Commun.*, 21(1):5–19, Sept. 2006.

[48] T. Sans and I. Cervesato. QWeSST for Type-Safe Web Programming. In *Third International Workshop on Logics, Agents, and Mobility*, LAM'10, 2010.

[49] P. Sewell, J. J. Leifer, K. Wansbrough, F. Z. Nardelli, M. Allen-Williams, P. Habouzit, and V. Vafeiadis. Acute: High-level programming language design for distributed computation. *J. Funct. Program.*, 17(4-5):547–612, July 2007.

[50] V. Simonet. Flow caml in a nutshell. In *Proceedings of the first APPSEM-II workshop*, pages 152–165, 2003.

[51] G. Stoyle, M. Hicks, G. Bierman, P. Sewell, and I. Neamtiu. Mutatis mutandis: safe and predictable dynamic software updating. In *ACM SIGPLAN Notices*, volume 40, pages 183–194. ACM, 2005.

[52] N. Swamy, N. Guts, D. Leijen, and M. Hicks. Lightweight monadic programming in ml. In *Proceedings of the 16th ACM SIGPLAN international conference on Functional programming*, ICFP '11, pages 15–27, New York, NY, USA, 2011. ACM.

[53] D. Syme, A. Granicz, and A. Cisternino. Building mobile web applications. In *Expert F# 3.0*, pages 391–426. Springer, 2012.

[54] J. Talpin and P. Jouvelot. The type and effect discipline. In *Logic in Computer Science, 1992. LICS'92.*, pages 162–173, 1994.

[55] R. Tate. The sequential semantics of producer effect systems. In *Proceedings of the 40th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, POPL '13, pages 15–26, New York, NY, USA, 2013. ACM.

[56] P. Thiemann. A unified framework for binding-time analysis. In *TAPSOFT'97: Theory and Practice of Software Development*, pages 742–756. Springer, 1997.

[57] F. Tip. A survey of program slicing techniques. *Journal of programming languages*, 3(3):121–189, 1995.

[58] M. Tofte and J.-P. Talpin. Region-based memory management. *Information and Computation*, 132(2):109–176, 1997.

[59] T. Uustalu and V. Vene. The essence of dataflow programming. In *Proceedings of the Third Asian conference on Programming Languages and Systems*, APLAS'05, pages 2–18, Berlin, Heidelberg, 2005. Springer-Verlag.

[60] T. Uustalu and V. Vene. Comonadic Notions of Computation. *Electron. Notes Theor. Comput. Sci.*, 203:263–284, June 2008.

[61] T. Uustalu and V. Vene. The Essence of Dataflow Programming. *Lecture Notes in Computer Science*, 4164:135–167, Nov 2006.

[62] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna. Cross site scripting prevention with dynamic data tainting and static analysis. In *Proceeding of the Network and Distributed System Security Symposium (NDSS)*, volume 42, 2007.

[63] D. Volpano, C. Irvine, and G. Smith. A sound type system for secure flow analysis. *J. Comput. Secur.*, 4:167–187, January 1996.

[64] J. Vouillon and V. Balat. From bytecode to javassript: the js_of_ocaml compiler. *Software: Practice and Experience*, 2013.

[65] B. Wadge. Monads and intensionality. In *International Symposium on Lucid and Intensional Programming*, volume 95, 1995.

[66] W. W. Wadge and E. A. Ashcroft. *LUCID, the dataflow programming language*. Academic Press Professional, Inc., San Diego, CA, USA, 1985.

[67] P. Wadler. Strictness analysis aids time analysis. In *Proceedings of the 15th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pages 119–132. ACM, 1988.

[68] P. Wadler. Linear types can change the world! In *Programming Concepts and Methods*. North, 1990.

[69] P. Wadler and S. Blott. How to make ad-hoc polymorphism less ad hoc. In *Proceedings of the 16th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, POPL '89, pages 60–76, New York, NY, USA, 1989. ACM.

[70] P. Wadler and P. Thiemann. The marriage of effects and monads. *ACM Trans. Comput. Logic*, 4:1–32, January 2003.

[71] D. Walker. *Substructural Type Systems*, pages 3–43. MIT Press.