Michael Jing Long Lee

WOLFSON COLLEGE

UNIVERSITY OF CAMBRIDGE

Everything in Scope

A Comprehensive Comparison
of Scope Extrusion Checks

Declaration

I, *Michael Jing Long Lee* of *Wolfson College*, being a candidate for the Master of Philosophy in Advanced Computer Science, hereby declare that this report and the work described in it are my own work, unaided except as may be specified below, and that the report does not contain material that has already been used to any substantial extent for a comparable purpose. In preparation of this report, I adhered to the Department of Computer Science and Technology AI Policy. I am content for my report to be made available to the students and staff of the University.

Signed   Michael Jing Long Lee
Date   June 7, 2025

Acknowledgements

I am extremely grateful to:

Abstract

Everything in Scope: A Comprehensive Comparison of Scope Extrusion Checks

Metaprogramming and effect handlers interact in unexpected, and sometimes undesirable, ways. One example is scope extrusion: the generation of ill-scoped code. There are many different ways to solve the problem of scope extrusion, but to my knowledge, until now there has been no way to evaluate them against each other. This dissertation introduces such a mechanism, which I use to evaluate the correctness, expressiveness, and efficiency of existing scope extrusion solutions. Additionally, I introduce a novel solution, a dynamic Best-Effort check, that I show is correct, and occupies a goldilocks zone between expressiveness and efficiency.

Contents

1. Introduction

Many compilers perform a wide range of optimisations. Compiler optimisations empower programmers to focus on writing maintainable code, leaving the compiler to optimise said code.

While compiler optimisation is often all one needs, it is difficult for compiler engineers to ensure, *a priori*, that every user has all the optimisations they require [26, 27]. When users discover that their desired optimisation has not been implemented, what can they do, beyond submitting a pull request, or optimising their code by hand?

Metaprogramming (for example, `C++` templates) [1] allows the user to "teach the compiler a class of [new] tricks" [30], and is therefore one possible solution. Metaprogramming allows programmers to write **maintainable** code which directs the compiler to generate **efficient** code.

For example, assume a `memcpy` function whose performance is heavily system dependent. How would one write a function that picks, depending on the system, the most performant implementation?

One possibility is via a dynamic conditional:

```OCaml
let memcpy source target n = if (architecture == AArch64) then
                                 (* return this program *)
                             else
                                 match vector_extensions with
                                 | None -> (* return this program *)
                                 | Some(AVX512) -> (* return this program *)
                                 | ...
memcpy source target n
```

Since `architecture` and `vector_extensions` are known at compile-time, they may be eliminated by an optimising compiler. If the compiler does not perform this optimisation, programmers might have to duplicate their code, increasing maintenance costs. Alternatively, they may use pre-processing directives, though this may lead to awkward code structures. With metaprogramming, however, they may write:

```MacoCaml
(* macro and $ can be read as annotations which
   indicate that the code should be run at compile-time *)
macro memcpy source target n = if (architecture == AArch64) then
                                  (* generate this program, to be run later *)
                               else
                                  match vector_extensions with
                                  | None -> (* generate this program *)
                                  | Some(AVX512) -> (* generate this program *)
                                  | ...
$(memcpy <<source>> <<target>> <<n>>)
```

Importantly, the `memcpy` macro is executed by the compiler, guaranteeing that the branches

will be eliminated. This process of using metaprogramming to select the most performant `memcpy` on any given system is used in practice, for instance, by the `xine` media player [10].

To support metaprogramming, languages have to provide the ability to build programs *to be run later*. These suspended programs are best thought of as abstract syntax trees. The following code constructs the program $(\lambda x.x)1$.

```ocaml
if (architecture == AArch64) then
  let build_app (f: (int -> int) expr) (v: int expr) = App(f, v) in
  let id_ast: (int -> int) expr = Lam(Var(x), Var(x)) in
  build_app(id_ast, Int(1)) (* int expr *)
else
  (*...*)
```

Metaprogramming is known to interact unexpectedly with effects. This interaction can be extremely desirable, for example, allowing programmers to manually perform loop-invariant code-motion [16] without making major modifications to their existing code [21].

Unfortunately, the interaction can also be undesirable. One problem is *scope extrusion* [16]. Scope extrusion occurs when the programmer accidentally generates code with unbound variables. In the following program, effects and metaprogramming combine to extrude **Var**(x) beyond its scope. The program stores **Var**(x) in a heap cell (l), and subsequently retrieves it outside its scope. The program thus evaluates to **Var**(x), which is unbound.

```ocaml
let l: int expr ref = new(Int(1)) in
let id_ast : (int -> int) expr = Lam(Var(x), l := Var(x); Int(1)) in
!l
```

The aforementioned example illustrated how the state effect could cause scope extrusion. The choice of effect is arbitrary. Scope extrusion could be caused by many other effects, like resumable exceptions.

To parameterise over the specific effect, I turn to effect handlers. Effect handlers, which have recently been added to `OCaml` [31], are a powerful language construct that can simulate many effects (state, I/O, greenthreading) [25]. It is thus strategic, and timely, to study scope extrusion in the context of effect handlers.

The problem of scope extrusion has been widely studied, resulting in multitudinous mechanisms for managing the interaction between metaprogramming and effects. Some solutions adapt the type system (Refined Environment Classifiers [19, 12], Closed Types [5]), others insert dynamic checks into the generated code [16]. However, there are two issues.

First, I am not studying scope extrusion abstractly. The MacoCaml [37] project aims to extend the `OCaml` programming language, which has effect handlers, with compile-time metaprogramming. However, until now, the MacoCaml project has had no clear policy on how metaprogramming and effect handlers should interact. In this setting, the options become more limited. Type-based approaches require unfeasible modification of the `OCaml` type-checker, and tend to limit expressiveness, disallowing a wide range of programs that do not lead to scope extrusion. Dynamic solutions are inefficient, reporting scope extrusion long after the error occurs, or unpredictable, allowing

some programs, but disallowing morally equivalent programs. Further, many of the dynamic solutions have not been proved correct.

Second, and more importantly, I lacked a way to evaluate solutions fairly and holistically. My evaluation criterion is three-pronged: correctness, efficiency, and expressiveness. Each solution is described in its own calculus, which made solutions difficult to compare. It is non-trivial to show that the definitions of scope extrusion in differing calculi agree. Hence, one solution may be correct with respect to its own definition, but wrong with respect to another. Further, expressiveness and efficiency are inherently comparative criteria.

This thesis solves both these problems. In Chapter 3, I design a novel, common language for encoding and evaluating different solutions. In Chapter 4, I use the designed language to formally describe and evaluate various checks. This process led to a novel Best-Effort dynamic check (Section 4.3), which I argue lands in a goldilocks zone, and should be adopted by MacoCaml.

1.1. Contributions

Concretely, the contributions of this work are:

1. A novel two-stage calculus, $\lambda_{\langle\langle op\rangle\rangle}$, that allows for effect handlers at both stages: compile-time and run-time (Chapter 3). $\lambda_{\langle\langle op\rangle\rangle}$ is well-typed, has the expected metatheoretic properties (Section 3.4), and is designed to facilitate comparative evaluation of different scope extrusion checks (Chapter 4).

2. In $\lambda_{\langle\langle op\rangle\rangle}$, a formal description of the MetaOCaml check described by Kiselyov [16] (Section 2.3.1), as well as an evaluation of its correctness (Section 4.2.1), expressiveness (Section 4.2.2), and efficiency (Section 4.2.3).

3. In $\lambda_{\langle\langle op\rangle\rangle}$, a formal description of a novel Dynamic Best-Effort check (Section 4.3), which I prove correct (Section 4.3.1), and argue, by comparison with other checks, lands in a goldilocks zone between expressiveness (Section 4.3.2) and efficiency (Section 4.3.3).

4. An encoding of refined environment classifiers [19] into $\lambda_{\langle\langle op\rangle\rangle}$, with a proof of correctness via logical relation (Section 4.4.1), and an evaluation of its expressiveness compared to other checks (Section 4.4.2).

5. Implementations of the three dynamic checks in MacoCaml.

2. Background

The aim of this dissertation is to evaluate existing, and propose new, policies for mediating the interaction between MacoCaml-style **metaprogramming** and **effect handlers**, by addressing the issue of **scope extrusion**.

This chapter provides technical overviews of each of the key concepts: metaprogramming (Section 2.1), effect handlers (Section 2.2), and scope extrusion (Section 2.3).

2.1. Metaprogramming

What is MacoCaml-style metaprogramming? This section provides an answer in two steps. Section 2.1.1 motivates metaprogramming, by illustrating the challenge of writing code that is both fast and maintainable. Section 2.1.2 considers the design space of metaprogramming, highlighting decisions made by the MacoCaml designers.

2.1.1. Metaprogramming for Fast and Maintainable Code

Metaprogramming helps programmers write fast and maintainable code. How does one write fast and maintainable code? Programmer skill is insufficient, because maintainability and efficiency are in constant tension.

To observe this tension, consider an example from the JAX machine learning library (adapted to OCaml): computing the gradient of a differentiable function as part of backpropagation over a neural network. More precisely, assume a type diff of differentiable functions (for simplicity, comprising only polynomials and composition)

```OCaml
type diff = Poly of int list
          | Compose of diff * diff
```

For example, the following expression represents $2(x^2 + 2x) + 4$.

```OCaml
Compose(Poly([1 ; 2 ; 0]), Poly([2 ; 4]))
```

The app: diff -> int -> int function evaluates elements of type diff.

```OCaml
let rec app (f: diff) (x: int) =
  let rec app_poly (cs: int list) (x : int) (acc: int) = match cs with
    | [] -> acc
    | c::cs -> app_poly cs x (c + (x * acc))
  in match f with
    | Poly(cs)      -> match cs with
                        | [] -> 0
                        | c::cs -> app_poly cs x c
    | Compose(g, h) -> app h (app g x)
```

4

The challenge is to write a function grad: diff -> **int** -> **int** that computes the gradient of its first argument with respect to its second. The grad_main function (Listing 1) is one maintainable way to compute gradients:

```ocaml
let rec grad_main (f: diff) (x: int) =
  let grad_poly (cs: int list) (x: int) =
    let grad_p c (a, b) = (c * b :: a, b + 1)
    let (res, _) = List.fold_right grad_p cs ([], 0) in
    app Poly(remove_last res) x (*remove_last removes the last element of a list*)
  in match f with
    | Poly(cs)      -> grad_poly cs x
    | Compose(g, h) -> grad_main g x * grad_main h (app g x)
```

Listing 1: A maintainable implementation of grad

If the function to be differentiated (f) is known in advance, for example, $f = 2(x^2 + 2x) + 4$, then this approach is inefficient. Instead, grad could be specialised to a more efficient grad_spec function (Listing 2), whose body is simply a hardcoded equation:

```ocaml
let grad_spec x = 4 * x + 4
```

Listing 2: An implementation of grad, specialised to $f = 2(x^2 + 2x) + 4$

What if there were multiple such fs? We could use grad_main to parameterise over the possible fs, relying on one implementation. Abstraction centralises implementations, reducing maintenance costs, but resulting in inefficiency. Alternatively, we could hardcode one variant of grad_spec for each f, creating an army of efficient functions. Specialisation applies known arguments in advance, creating opportunities for optimisation, but at the cost of maintainability.

The tension between maintainability (abstraction) and efficiency (specialisation) has also been observed in other works on metaprogramming, in domains such as regex matching [33], parsing [40], linking [29], statistical modelling [36], and hardware design [34].

A better approach might therefore be to write maintainable code, delegating the responsibility of optimisation to the compiler. While this suffices for many cases, relying solely on compiler optimisation can be insufficient. The compiler may not implement the desired optimisations. While compiler engineers might have an economic incentive to write optimisations for the machine learning community, this may not be true for less lucrative domains [27]. Even in machine learning, many libraries are built on top of existing languages, like Python, which might not perform the desired optimisations. Further, even if the compiler does implement the optimisation, the programmer has little control over the optimisation process: the compiler may not optimise as frequently as desired, or optimise in ways that do not meet all of the programmer's desiderata (for example, by inflating binary sizes). Moreover, the optimisation process may be sensitive to small changes in the source code.

How does one write maintainable and efficient code, **when one is not certain that the compiler will optimise one's code exactly as desired**?

One answer, and the approach taken by JAX [13], is metaprogramming, which gives users the ability to perform code-generation. Programmers may thus take matters into

their own hands: manually generating optimised code when the compiler may not automatically do so for them.

The Mechanics of Metaprogramming

Metaprogramming allows for code that, when executed, generates code. Thus, it can be utilised to write a function, grad_gen, which resembles grad_main (inheriting its maintainability), but that generates a program which resembles grad_spec (inheriting its efficiency).

Listing 3 presents the metaprogrammed grad_gen function. Notice that it is exactly grad_main, but extended with annotations: **macro**, <<->>, and $-. Further, the type of x on line 1 (for example) is now **int** expr, rather than **int**. These changes provide the necessary mechanisms for code generation: on line 20, grad_gen is used to generate (2 + (y*2)) * 2 (notice the resemblance to grad_spec).

```
                                                                          MacoCaml
1   macro rec app_gen (f: diff) (x: int expr) =
2     let rec app_poly_gen (cs: int list) (x : int expr) (acc: int expr) = match cs with
3       | [] -> acc
4       | c::cs -> app_poly_gen cs x <<c + ($x * $acc)>>
5     in match f with
6       | Poly(cs)       -> match cs with
7                           | [] -> <<0>>
8                           | c::cs -> app_poly cs x <<c>>
9       | Compose(g, h) -> app_gen h (app_gen g x)
10
11  macro rec grad_gen (f: diff) (x: int expr) =
12    let grad_poly_gen (cs: int list) (x: int expr) =
13      let grad_p c (a, b) = (c * b :: a, b + 1)
14      let (res, _) = List.fold_right grad_p cs ([], 0) in
15      app_gen Poly(remove_last res) x
16    in match f with
17      | Poly(cs)       -> grad_poly_gen cs x
18      | Compose(g, h) -> << $(grad_main g <<x>>) * $(grad_main h (app_gen g <<x>>)) >>
19
20  let grad_spec y = $(grad_gen Compose(Poly([1 ; 2 ; 0]), Poly([2 ; 4])) <<y>>)
21                    (* generates (2 + (y * 2)) * 2 *)
```

Listing 3: A metaprogrammed grad_gen function, which resembles grad_main but generates a function resembling grad_spec

In MacoCaml, the programmer is able to generate code at compile-time, for use at run-time. I separate this into two language features:

1. A type for code ('a expr), with mechanisms (<<->>, $-) for creating and manipulating values of this type. Expressions that return values of code type serve as code generators.

2. A mechanism for executing expressions *at compile-time*. By using the type-system, MacoCaml ensures only code generators can be executed at compile-time. Thus compile-time evaluation will always produce code values that can be evaluated at run-time (as opposed to **int**s, for example, which cannot).

First, in MacoCaml, code of type `'a` has type `'a expr`. For example, code of type `int` has type `int expr`. In MacoCaml, the `<<->>` ("quote") annotation converts expressions to code values (similar to how `[-]` converts expressions to list values). For example, `<<1>>` has type `int expr`. Under a quotation, the `$-` ("splice") annotation stops this conversion, allowing for evaluation under a quotation. For example,

$$<<\$(\text{print\_int } 1+2; <<1+2>>) + 0 >>$$

prints 3 and evaluates to `<<1+2+0>>`.

While not an accurate description of MacoCaml, it can be useful to think of elements of type `'a expr` as abstract syntax trees (ASTs). In this conceptual model, quotation creates ASTs, by converting a program into its AST representation. For example,

$$<< x + 0 >> \text{ can be thought of as } \textbf{Plus}(\textbf{Var}(x), \textbf{Int}(0))$$

Under a quotation, the `$` annotation stops this conversion, allowing for programs that *manipulate* ASTs.

$$<< \$x + 0 >> \text{ can be thought of as } \textbf{Plus}(x, \textbf{Int}(0))$$

Interleaving quotes and splices executes code to build ASTs

$$<<\$(\text{print\_int } 1+2; <<1+2>>) + 0>>$$
$$\text{can be thought of as}$$
$$\textbf{Plus}(\text{print\_int } 1+2; \textbf{Plus}(\textbf{Int}(1), \textbf{Int}(2)), \textbf{Int}(0))$$

Second, to evaluate expressions at compile-time, MacoCaml offers the top-level splice, a splice (`$`) annotation not surrounded by quotes (`<<>>`). Notice that `$` is overloaded. We must be careful to disambiguate between **top-level splices**, which execute programs at compile-time, and **splices under quotations**, which stop conversion to the code type. In Listing 3, there is only one top-level splice, on line 20: `$(grad_gen ...)`. We may now shift expressions of type `'a expr` under top-level splices, to perform generation at compile time.

Note that to access `grad_gen` at compile-time, we must also move it under the top-level splice, resulting in code duplication:

```
                                                                    MacoCaml
1  let grad_spec y  = $(let grad_gen = ... in
2                      grad_gen Compose(Poly([1 ; 2 ; 0]), Poly([2 ; 4])) <<y>>)
3  let grad_spec' y = $(let grad_gen = ... in
4                      grad_gen Compose(Poly([4; 3 ; 1 ; 7]), Poly([1 ; 8])) <<y>>)
```

To allow compile-time functions, like `grad_gen`, to be re-used across multiple top-level splices, MacoCaml introduces the **macro** keyword, giving us:

```
                                                                    MacoCaml
1  macro grad_gen = ...
2  let grad_spec y  = $(grad_gen Compose(Poly([1 ; 2 ; 0]), Poly([2 ; 4])) <<y>>)
3  let grad_spec' y = $(grad_gen Compose(Poly([4; 3 ; 1 ; 7]), Poly([1 ; 8])) <<y>>)
```

2.1.2. The Design Space of Metalanguages

Different metalanguages provide slightly different variants of metaprogramming to the user. Different variants could interact differently with effect handlers. This thesis focuses on homogenous, compile-time, two-stage metaprogramming:

1. **Homogenous or Heterogenous**
   Do the generated and generating languages agree or differ?

   If the generated and generating languages are the same, this is known as homogenous metaprogramming. Otherwise, it is heterogenous [17].

   The metaprogramming supported by MacoCaml is homogenous, where `OCaml` code generates `OCaml` code. I focus on homogenous metaprogramming.

2. **Run-time or Compile-Time**
   When does the generation take place?

   Code generation could take place at compile-time or at run-time.

   Run-time and compile-time metaprogramming differ non-trivially. For example, with run-time metaprogramming, generated and generating programs may share a heap.

   In MacoCaml, code generation occurs at compile-time, and I pay no further attention to run-time metaprogramming.

3. **Two-stage or Multi-stage**
   How many stages of code generation are allowed?

   When introducing MacoCaml, I illustrated how one uses top-level splices to shift computation from run-time ("level 0") to compile-time ("level -1"). I describe levels formally in Section 3.1.1 (Definition 3.1.1, Page 28). For now, it suffices to think of a level as a phase of evaluation: everything at level -1 must be fully evaluated before anything at level 0 is evaluated. Might it be possible to shift computation from compile-time to a pre-compile-time ("level -2") phase, for example, via a nested splice?

   ```MacoCaml
   1    $($ grad_gen f <<y>> )
   ```

   In a two-stage system, one is restricted to operating between two levels, so this is disallowed. In contrast, in a multi-stage system, one can operate between any number of levels. Multi-stage metaprogramming is thus strictly more general than two-stage metaprogramming.

   Although nested splices are disallowed in MacoCaml, it is a multi-stage system, since entire modules may be imported at a decremented level [38]. However, I focus on two-stage metaprogramming.

The restriction from multi-stage to two-stage metaprogramming was motivated by a cost-benefit analysis:

1. **Cost**: Since in MacoCaml, the module system is the only mechanism for achieving multi-stage programming, investigating multi-stage metaprogramming would require the investigation of module systems, effects, and metaprogramming. The

interaction between module systems and metaprogramming is still an ongoing area of research [7].

2. **Benefit**: In practice, "almost all uses" of multi-stage metaprogramming only use two stages [11]. Further, scope extrusion can be observed, and is often studied, in two-stage systems [12, 19].

2.2. Effect Handlers

What is an effect handler? Section 2.2.1 first motivates effect handlers, as a way to build composable and customisable effects. Section 2.2.2 introduces a calculus for studying the operational behaviour of effect handlers, à la Pretnar [25]. This calculus is useful both for precise description of effect handlers, and as a basis for investigating the interaction between metaprogramming and effect handlers. Finally, since different design decisions for effect handlers could affect the nature of their interaction with metaprogramming, Section 2.2.3 considers the design space of effect handlers.

2.2.1. Composable and Customisable Effects

Effects are a mechanism by which a program interacts with its environment. Examples of effects include state, (resumable) exceptions, non-determinism, and I/O. Different effects are typically defined and understood separately from each other, meaning they are not easily composable. They are also typically implemented by compiler engineers rather than programmers, meaning they are not customisable. In contrast, effect handlers provide a unifying and programmable framework that may be instantiated into different effects, allowing for composable and customisable treatment of effects [15].

Much like how exception handlers allow users to create custom exceptions with custom semantics, effect handlers provide a general framework for creating custom effects with custom semantics. The interaction between effect handlers is described abstractly, parameterising over the exact semantics of the effect. Hence, implementing effects as effect handlers ensures composability by design.

Since effect handlers may be instantiated into a range of different effects, considering the interaction of metaprogramming with effect handlers is an exercise in killing many birds with a single stone. Additionally, effect handlers were recently added to `OCaml` [31], making their interaction with metaprogramming a timely problem.

2.2.2. λ_{op}: A Calculus for Effect Handlers

This section presents a calculus, λ_{op}, for reasoning about the operational behaviour of effect handlers. λ_{op} is broadly similar to the calculus described by Pretnar [25] [1], and will be used in later sections to study the interaction between effect handlers and metaprogramming.

Figure 2.1 collates the base syntax of λ_{op}. In this section, I additionally assume λ_{op} additionally supports a unit value (), pairs with pattern matching, strings with concatenation and Python-style format strings.

For example, treating **do** $x \leftarrow c_1$ **in** c_2 as a let-binding (and ignoring **return**, which is explained shortly), the following code evaluates to "Revolution 9".

---

[1]Differences will be clarified as they arise

Syntax

Values	v	$::=$	$x \mid n \mid \lambda x.c \mid \kappa x.c$
Computations	c	$::=$	$v_1 v_2 \mid$ **return** $v \mid$ **do** $x \leftarrow c_1$ **in** c_2
			$\mid$ **op**$(v) \mid$ **handle** c **with** $\{h\} \mid$ **continue** $v_1 \, v_2$
Handlers	h	$::=$	**return**$(x) \mapsto c \mid h;$ **op**$(x, k) \mapsto c$

Figure 2.1.: The syntax of λ_{op}. Terms are syntactically divided into values v, computations c, and handlers h

```
do (x, y) ← return ("Revolution", f"{9}") in x ˆ y
```

```
return "Revolution 9"
```

Further, I use $c_1; c_2$ as syntactic sugar for **do** $\_ \leftarrow c_1$ **in** c_2. This section explains key language constructs in turn, with reference to a running example: the λ_{op} program in Listing 4.

```
handle
  do x ← print(1); return 1 in do y ← print(2); return 2 in x + y
with
  {return(x) ↦ return (x, "");
   print(x, k) ↦ do (v, s) ← continue k () in return (v, f"{x}; " ˆ s)}
```

```
return (3, "1;2")
```

Listing 4: A λ_{op} program that returns $(3, "1;2")$. It is used as a running example throughout this section.

Sequencing computations: do and return

Effects force us to carefully consider the order of evaluation. For example, consider the following OCaml programs:

```
1  let pure     = (1+0) + (2+0)
2  let effectful = let l = ref 0 in (l := 1; 1) + (l := 2; 2)
```

The result of pure, which has no effects, is independent of the evaluation order. In contrast, the result of effectful *is* dependent on the evaluation order. If terms are evaluated left-to-right, the value of !l is 2, otherwise, it is 1.

In order to be precise about the order of evaluation, λ_{op} follows Pretnar's approach of stratifying terms into distinct syntactic categories, with "inert values" (v) disjoint from "potentially effectful computations" (c). However, while Pretnar treats handlers h as values, in λ_{op}, they are a third syntactic category, disjoint from both values and computations. **return** v lifts values into computations, and is also the result of fully evaluating a computation. **do** $x \leftarrow c_1$ **in** c_2 acts like a let-binding, sequencing computations. This

forces programmers to be explicit the order of evaluation. First, c_1 is fully evaluated to obtain some **return** v. The value v is then bound to x, and finally c_2 is evaluated.

For example, extending λ_{op} with a `plus` function, what is the order of evaluation of `plus` c_1 c_2, where c_1 and c_2 are compuations that evaluate to naturals? Are both arguments evaluated before application, or are evaluation and application interleaved? The syntax forces programmers to choose explicitly. The programmer can either fully evaluate both arguments before applying them in turn,

> **do** $x \leftarrow c_1$ **in** (**do** $y \leftarrow c_2$ **in** (**do** $f \leftarrow$ `plus` x **in** fy)) $\qquad \lambda_{\mathsf{op}}$

or alternatively, c_1, apply it, then evaluate c_2

> **do** $x \leftarrow c_1$ **in** (**do** $f \leftarrow$ `plus` x **in** (**do** $y \leftarrow c_2$ **in** fy)) $\qquad \lambda_{\mathsf{op}}$

Both choices are valid, but the programmer must choose. For clarity, where the order cannot affect the result (for example, $c_1 =$ **return** 1, $c_2 =$ **return** 2), I abuse notation and write $c_1 + c_2$. Similarly, for clarity, I implicitly cast values to computations (writing $1 + 2$ rather than **return** $1 +$ **return** 2).

Performing effects: `op`, `handle`, and `continue`

Recall that effect handlers allow users to register custom effects with custom semantics. λ_{op} assumes that the effects have been registered in advanced, parameterising over them with the placeholder **op**(v). Assume that the user has declared the effect **print** in advance. They may thus write programs which refer to **print**:

> **do** $x \leftarrow$ **print**(1); **return** 1 **in do** $y \leftarrow$ **print**(2); **return** 2 **in** $x + y$ $\qquad \lambda_{\mathsf{op}}$

In the program fragment above, **print** is an effect, but with as-yet-unknown semantics. Effect handlers, which comprise a **return handler** and zero or more **operation handlers**, specify how effects interact with their environment, and thus may be used to give effects meaning. Consider defining an effect handler that accumulates print statements in a string (some "`stdout`"). For example, the aforementioned program should return $(3, "1;~2")$.

First, an effect handler must handle programs that have no calls to **print**. For such a program, the accummulating handler should return both the value and the empty string: $(3, "")$. The return handler is written as follows:

$$\textbf{return}(x) \mapsto c$$

where c is set to **return** $(x, "")$. All effect handlers must specify a return handler. In many cases, the return handler is simply the identity.

Next, an effect handler must handle programs that perform **print** effects, by specifying an operation handler of the form:

$$\textbf{print}(x, k) \mapsto c$$

where c is the user-defined semantics for **print**. Concretely, one instance of c is

$$\textbf{do}~(v, s) \leftarrow \textbf{continue}~k~() ~\textbf{in return}~(v, \texttt{f"}\{x\}\texttt{;"}~\hat{}~s)$$

In the definition of c, the programmer may refer to x, the argument passed to **print**, and k, a delimited continuation from the point the effect was performed to the point it was handled. The delimited continuation can be thought of as a suspended program, awaiting a value from its environment. Effects allow programs to receive data from their environments, as in

$$\boxed{\texttt{handle}} \quad \texttt{get\_int\_from\_user}() + 1 \quad \boxed{\texttt{with } \{\texttt{get\_int\_from\_user}(x, k) \mapsto \ldots\}}$$

The delimited continuation $\kappa y.y + 1$,
captured from the point the effect was
performed to the point it was handled.

where the program that adds one is suspended until the value is received. I write the suspended program as $\kappa y.\ y + 1$, where the variable y indicates the as-yet-unknown value. $\kappa y.\ y + 1$ is the continuation bound to k. The syntax is evocative: continuations can be thought of as being *like* functions $\lambda y.\ y + 1$ (in Pretnar's calculus, functions and continuations share a type). However, for technical reasons relating to scope extrusion (Sections 4.3 and 4.4), in λ_{op}, continuations and functions are disambiguated both syntactically and at the type-level (mirroring the approach by Isoda et al. [12]). The expression

$$\texttt{continue } k\, v$$

is used to resume the suspended program, substiting value v for y. For example,

$$\texttt{handle } 1 + \texttt{get\_int\_from\_user}() \texttt{ with } \{\texttt{get\_int\_from\_user}(x, k) \mapsto \texttt{continue } k\, 2\}$$

steps to $1 + 2$ (and thus evaluates to 3).

In λ_{op}, the continuation to be bound to k is calculated. In contrast, in Pretnar's calculus, it is explicitly written by the programmer, using the syntax

$$\mathbf{op}(v; y.c)$$

where $y.c$ is the continuation to be bound to k. Pretnar acknowledges that the approach adopted by λ_{op} is an equivalent formulation.

The concrete operation handler thus resumes the suspended program, supplying a unit value, since **print** effects do not receive values. Evaluating the (now unsuspended) program eventually returns a value v and some partially accumulated stdout s. The handler then prepends the printed value, x, onto s.

Having defined the semantics for **print**, the user may now interpret the earlier example with their semantics, using the **handle** e **with** $\{h\}$ construct. Doing so results in the program in Listing 4.

Notice that multiple effects may be handled by the same handler, and the same effect might be handled by multiple handlers, potentially with different semantics.

Operational Semantics

The semantics of λ_{op} are made precise via an operational semantics (Figure 2.2). The operational semantics is given on configurations of the form $\langle c; E \rangle$, where c is a term and E is an evaluation context, in the style of Felleisen and Friedman [8]. Evaluation contexts are represented as a stack of evaluation frames F, à la Kiselyov [15]. The two

Operational Semantics λ_{op}

Auxiliary Definitions

$$
\begin{aligned}
\text{Evaluation Frame} \qquad & F \quad ::= \quad \textbf{do } x \leftarrow [-] \textbf{ in } c_2 \mid \textbf{handle } [-] \textbf{ with } \{h\} \\
\text{Evaluation Context} \qquad & E \quad ::= \quad [-] \mid E[F]
\end{aligned}
$$

$$
\begin{aligned}
\text{Domain of Handler} \qquad \text{dom}(h) \quad &\triangleq \quad \text{dom}(\textbf{return}(x) \mapsto c) = \emptyset, \\
& \qquad\; \text{dom}(h; \textbf{op}(x,k) \mapsto c) = \text{dom}(h) \cup \{\textbf{op}\} \\
\text{Handled Effects} \qquad \text{handled}(E) \quad &\triangleq \quad \text{handled}([-]) = \emptyset, \\
& \qquad\; \text{handled}(E[\textbf{do } x \leftarrow [-] \textbf{ in } c_2]) = \text{handled}(E), \\
& \qquad\; \text{handled}(E[\textbf{handle } [-] \textbf{ with } \{h\}]) = \text{handled}(E) \cup \text{dom}(h),
\end{aligned}
$$

Operational Semantics

$$
\begin{aligned}
(\textsc{Red-App}) \qquad & \langle (\lambda x.c)v; E \rangle \quad \rightarrow \quad \langle c[v/x]; E \rangle \\
(\textsc{Red-Seq}) \qquad & \langle \textbf{do } x \leftarrow \textbf{return } v \textbf{ in } c; E \rangle \quad \rightarrow \quad \langle c[v/x]; E \rangle \\
(\textsc{Red-Hdl}) \qquad & \langle \textbf{handle return } v \textbf{ with } \{h\}; E \rangle \quad \rightarrow \quad \langle c[v/x]; E \rangle \quad (\text{where } \textbf{return}(x) \mapsto c \in h)
\end{aligned}
$$

$$
\begin{aligned}
(\textsc{Cng-Psh}) \qquad & \langle F[c]; E \rangle \quad \rightarrow \quad \langle c; E[F] \rangle \\
(\textsc{Cng-Pop}) \qquad & \langle \textbf{return } v; E[F] \rangle \quad \rightarrow \quad \langle F[\textbf{return } v]; E \rangle
\end{aligned}
$$

$$
\begin{aligned}
(\textsc{Eff-Op}) \quad & \langle \textbf{op}(v); E_1[\textbf{handle } E_2 \textbf{ with } \{h\}] \rangle \rightarrow \langle c[v/x, \kappa x.\, \textbf{handle } E_2[\textbf{return } x] \textbf{ with } \{h\}/k]; E_1 \rangle \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{where } \textbf{op} \in \text{dom}(h) \text{ and } \textbf{op} \notin \text{handled}(E_2)) \\
(\textsc{Eff-Cnt}) \quad & \langle \textbf{continue } (\kappa x. E_2[\textbf{return } x])\, v; E_1 \rangle \rightarrow \langle \textbf{return } v; E_1[E_2] \rangle
\end{aligned}
$$

Figure 2.2.: The operational semantics of λ_{op}. The semantics is given on configurations of the form $\langle c; E \rangle$. Rules are divided into three classes: reduction rules $\textsc{Red-}X$, which perform computation, congruence rules $\textsc{Cng-}Y$ which manipulate the evaluation context, and effect rules $\textsc{Eff-}Z$ that are special to λ_{op}.

key rules are $\textsc{Eff-Op}$, the mechanism for giving effects custom semantics, and $\textsc{Eff-Cnt}$, the mechanism for resuming programs.

To illustrate the operation of $\textsc{Eff-Op}$ and $\textsc{Eff-Cnt}$, I consider the evaluation of [Listing 4], beginning with an empty context. Let h be the handler body

$$
\begin{aligned}
&\{\textbf{return}(x) \mapsto \textbf{return } (x, ""); \\
&\; \textbf{print}(x,k) \mapsto \textbf{do } (v,s) \leftarrow \textbf{continue } k\, () \textbf{ in return } (v, \texttt{f"}\{x\}\texttt{;"} \verb|^| s)\}
\end{aligned}
$$

Several applications of $\textsc{Cng-Psh}$ produces the configuration

$$
\begin{aligned}
\langle\, \textbf{print}(1) \; ; \; &\textbf{handle} \\
& \textbf{do } x \leftarrow [-]; \textbf{return } 1 \textbf{ in do } y \leftarrow \textbf{print}(2); \textbf{return } 2 \textbf{ in } x + y \\
& \textbf{with } \{h\} \,\rangle
\end{aligned}
$$

Let $E = \textbf{do } x \leftarrow \textbf{return } u; \textbf{return } 1 \textbf{ in do } y \leftarrow \textbf{print}(2); \textbf{return } 2 \textbf{ in } x + y$. Applying $\textsc{Eff-Op}$ suspends the program, finds the handler h with the user's semantics for **print**, and gives the **print** effect the desired semantics

$$
\langle\, \textbf{do } (v,s) \leftarrow \textbf{continue } (\kappa u.\, \textbf{handle } E \textbf{ with } \{h\})\, () \textbf{ in return } (v, \texttt{f"}\{1\}\texttt{;"} \verb|^| s) \; ; \; [-] \,\rangle
$$

Applying $\textsc{Cng-Psh}$,

$$
\langle\, \textbf{continue } (\kappa u.\, \textbf{handle } E \textbf{ with } \{h\})\, () \; ; \; \textbf{do } (v,s) \leftarrow [-] \textbf{ in return } (v, \texttt{f"}\{1\}\texttt{;"} \verb|^| s) \,\rangle
$$

Applying EFF-CNT resumes the program that was suspended

$$\langle \textbf{return } () \; ; \; \textbf{do}(v, s) \leftarrow$$
$$\textbf{handle}$$
$$\textbf{do } x \leftarrow ([-]; \textbf{return } 1)\textbf{in}$$
$$\textbf{do } y \leftarrow (\textbf{print}(2); \textbf{return } 2)$$
$$\textbf{in } x + y$$
$$\textbf{with } \{h\}$$
$$\textbf{in return } (v, \textbf{f"}\{1\}; \text{"} \hat{} \; s) \rangle$$

The side-condition on EFF-OP is needed because the user may define multiple handlers with different semantics for the same effect. The side-condition resolves any ambiguity by using the *latest* handler. For example, the following program has a **read** effect that is given two definitions: it could read either 1 or 2. The ambiguity is resolved by choosing the latest handler: in this case, the program reads 1.

```
                                                                                    λop
handle
   handle read() with {return(y) ↦ return y; read(x, k) ↦ continue k 1}
with
   {return(y) ↦ return y; read(x, k) ↦ continue k 2}
───────────────────────────────────────────────────────────────────────
return 1
```

To be precise, the domain of a handler h, $\mathrm{dom}(h)$, is the set of operations for which it has handlers. For example, the domain of

$$\{\textbf{return}(x) \mapsto \textbf{return } x; \textbf{read}(\_, k) \mapsto \textbf{continue } k \; 1; \textbf{shirk}(x, k) \mapsto \textbf{shirk}(x)\}$$

is $\{\textbf{read}, \textbf{shirk}\}$ (even though the responsibility for handling the **shirk** effect is shirked). Given an evaluation context, E, the set of effects handled by the context $\mathrm{handled}(E)$, is the union of all of the domains of the handler frames in E. That is,

$$\mathrm{handled}(\textbf{handle } (\textbf{handle } [-] + 1 \textbf{ with } \{h_1\}) \textbf{ with } \{h_2\}) = \mathrm{dom}(h_1) \cup \mathrm{dom}(h_2)$$

The latest handler h for an effect **op** in a context E is found by decomposing E into

$$E_1[\textbf{handle } E_2 \textbf{ with } \{h\}]$$

such that $\textbf{op} \in \mathrm{dom}(h)$ (h handles **op**) and $\textbf{op} \notin \mathrm{handled}(E_2)$ (no handlers for **op** in E_2). If such an h exists, this condition identifies it uniquely.

Type-and-Effect System

Figure 2.3 collates the syntax of λ_{op} types. Types are divided into value types (for example, $\mathbb{N}$), computation types ($\mathbb{N} ! \{\textbf{print}\}$), and handler types ($\mathbb{N} ! \{\textbf{print}\} \Longrightarrow \mathbb{N} ! \emptyset$). Since computations may have effects, computation types track unhandled effects using an effects row (Δ), which in λ_{op} is simply a set. This type-and-effect system allows us to distinguish between values, computations that return values, and computations that return values and additionally have some unhandled side effects.

Term	Type
3	$\mathbb{N}$
$\textbf{do } x \leftarrow \textbf{return } 1 \textbf{ in do } y \leftarrow \textbf{return } 2 \textbf{ in } x + y$	$\mathbb{N} ! \emptyset$
$\textbf{do } x \leftarrow \textbf{print}(1); \textbf{return } 2 \textbf{ in do } y \leftarrow \textbf{return } 2 \textbf{ in } x + y$	$\mathbb{N} ! \{\textbf{print}\}$

Types

Effects row	$\Delta ::= \emptyset \mid \Delta \cup \{\text{op}_i\}$
Value type	$S, T ::= \mathbb{N}$
	$\mid S \xrightarrow{\Delta} T$ functions
	$\mid S \xrightarrow{\Delta} T$ continuations
Computation type	$T ! \Delta$
Handler type	$S ! \Delta_1 \Longrightarrow T ! \Delta_2$

Figure 2.3.: λ_{op} types. Notice that, just as terms are divided into values, computations, and handlers, types are divided into value types (S, T), computation types $(T ! \Delta)$, and handler types $(S ! \Delta_1 \Longrightarrow T ! \Delta_2)$.

Functions are values, and are applied to other values, but produce computations on application. For example, the function

$$\lambda x : \mathbb{N}.\ \textbf{print}(x); \textbf{return}\ x$$

is a value that accepts a value of type $\mathbb{N}$ and returns a computation of type $\mathbb{N} ! \{\textbf{print}\}$. Functions thus have suspended effects, which I write $S \xrightarrow{\Delta} T$. In this case, the function has type $\mathbb{N} \xrightarrow{\{\text{print}\}} \mathbb{N}$. For technical reasons, continuations and functions need to be distinguished, but in most cases they may be treated equivalently.

Handlers transform computations of one type to computations of another type. This happens in two ways: first, by handling effects, and thus removing them from the effects row. Second, by modifying the return type of computations. To reflect both abilities, handlers are given a type of the form $S ! \Delta_1 \Longrightarrow T ! \Delta_2$. For example, a handler of the form

$$\{\textbf{return}(x) \mapsto \textbf{return}\ (x, ""); \\ \textbf{print}(x, k) \mapsto \textbf{do}\ (v, s) \leftarrow \textbf{continue}\ k\ () \ \textbf{in return}\ (v, \text{f"}\{x\}; "\,\hat{}\ s)\}$$

may be given type $\mathbb{N} ! \{\textbf{print}\} \Longrightarrow (\mathbb{N} \times \text{String}) ! \emptyset$, reflecting both the handling of the **print** effect and the transformation of the return type to include the collated print statements.

λ_{op} assumes that the user declares their effects in advance. It additionally assumes that they declare the types of their effects in advance, and that this mapping is stored in Σ. That is,

$$\text{op} : A \rightarrow B \in \Sigma$$

In `OCaml`, this would correspond to writing:

```
1   type _ Effect.t += Op: A -> B
```

λ_{op} does not impose any restrictions on A and B. In particular, they may be recursive, and refer to op. For example:

$$\text{recursive} : 1 \rightarrow (1 \xrightarrow{\{\text{recursive}\}} 1)$$

2. Background

Thus, one may write programs which do not terminate, by "tying the knot", for example

```
handle (λ_.recursive())() with {recursive(_, k) ↦ continue k (λ_.recursive())}
```

$\lambda_{\mathbf{op}}$

Note that for the program to be well-typed, the program fragment $\lambda_-.\mathbf{recursive}()$ must refer to **recursive** in its type: $1 \xrightarrow{\{\text{recursive}\}} 1$. Thus, the declared type of the **recursive** effect must be recursive.

The typing rules for terms are collated in Figure 2.4. Since types are stratified, so are typing judgements:

Value Typing Judgment	$\Gamma \vdash v : T$
Computation Typing Judgment	$\Gamma \vdash c : T\,!\,\Delta$
Handler Typing Judgement	$\Gamma \vdash h : S\,!\,\Delta_1 \Longrightarrow T\,!\,\Delta_2$

The key rules are RETURN, DO, OP, and the handler rules (RET-HANDLER, OP-HANDLER).

The RETURN rule permits **return** v to be typed with any set of effects. For example:

$$\frac{}{\Gamma \vdash \mathbf{return}\ 0 : \mathbb{N}\,!\,\{\mathbf{print}\}}$$

This flexibility is important, because to type **do** $x \leftarrow c_1$ **in** c_2, the Do rule requires c_1 and c_2 to have the same effects. For example, without this flexibility, it would not be possible to complete the following typing derivation:

$$\frac{\vdots}{\Gamma \vdash \mathbf{do}\ x \leftarrow \mathbf{print}(0)\ \mathbf{in}\ \mathbf{return}\ 0 : \mathbb{N}\,!\,\{\mathbf{print}\}}$$

A valid alternative would be to add explicit subtyping. However, such an approach would no longer be syntax directed.

The OP rule forces the performed operation to be tracked by the effects row ($\mathbf{op} \in \Delta$): flexibility allows the type system to over-approximate the effects in a term, but not to underapproximate them.

Following the approach by Biernacki et al. [4], handlers are typed clause-by-clause, using the RET-HANDLER and OP-HANDLER rules. In contrast, Pretnar types a handler with a single rule that checks all clauses at once. Consider typing the handler:

$$\{\mathbf{return}(x) \mapsto \mathbf{return}\ (x, "");$$
$$\mathbf{print}(x, k) \mapsto \mathbf{do}\ (v, s) \leftarrow \mathbf{continue}\ k\ ()\ \mathbf{in}\ \mathbf{return}\ (v, \mathtt{f"}\{x\}; \mathtt{"}\ \hat{}\ s)\}$$

with type $\mathbb{N}\,!\,\{\mathbf{print}\} \Longrightarrow (\mathbb{N} \times \mathsf{String})\,!\,\emptyset$. This involves applying the OP-HANDLER rule, which is transcribed below. Preconditions are numbered for reference.

(OP-HANDLER)
$$(1)\,\mathbf{op} : A \to B \in \Sigma$$
$$(2)\,\Gamma \vdash h : S\,!\,\Delta_1 \Longrightarrow T\,!\,\Delta_2$$
$$\frac{(3)\,\Gamma, x : A, k : B \xrightarrow{\Delta_2} T \vdash c : T\,!\,\Delta_2 \qquad (4)\,\Delta_2 \subseteq \Delta_1 \setminus \{\mathbf{op}\} \qquad (5)\,\mathbf{op}(x', k') \mapsto c' \notin h}{\Gamma \vdash h; \mathbf{op}(x, k) \mapsto c : S\,!\,\Delta_1 \Longrightarrow T\,!\,\Delta_2}$$

It is therefore sufficient to show that:

(1) **print** $: \mathbb{N} \to 1 \in \Sigma$, which is true by assumption

Typing Rules

λ_{op}

$\boxed{\Gamma \vdash v : T}$

(NAT)

$$\overline{\Gamma \vdash n : \mathbb{N}}$$

(VAR)

$$\frac{\Gamma(x) = T}{\Gamma \vdash x : T}$$

(LAMBDA)

$$\frac{\Gamma, x : S \vdash c : T \,!\, \Delta}{\Gamma \vdash \lambda x.c : S \xrightarrow{\Delta} T}$$

(CONTINUATION)

$$\frac{\Gamma, x : S \vdash c : T \,!\, \Delta}{\Gamma \vdash \kappa x.c : S \xrightarrow{\Delta}\!\!\!\twoheadrightarrow T}$$

$\boxed{\Gamma \vdash c : T \,!\, \Delta}$

(APP)

$$\frac{\Gamma \vdash v_1 : S \xrightarrow{\Delta} T \qquad \Gamma \vdash v_2 : S}{\Gamma \vdash v_1\, v_2 : T \,!\, \Delta}$$

(CONTINUE)

$$\frac{\Gamma \vdash v_1 : S \xrightarrow{\Delta}\!\!\!\twoheadrightarrow T \qquad \Gamma \vdash v_2 : S}{\Gamma \vdash \mathbf{continue}\, v_1\, v_2 : T \,!\, \Delta}$$

(RETURN)

$$\frac{\Gamma \vdash v : T}{\Gamma \vdash \mathbf{return}\, v : T \,!\, \Delta}$$

(DO)

$$\frac{\Gamma \vdash c_1 : S \,!\, \Delta_1 \qquad \Gamma, x : S \vdash c_2 : T \,!\, \Delta}{\Gamma \vdash \mathbf{do}\; x \leftarrow c_1 \; \mathbf{in}\; c_2 : T \,!\, \Delta}$$

(OP)

$$\frac{\Gamma \vdash v : S \qquad \mathsf{op} : S \to T \in \Sigma \qquad \mathsf{op} \in \Delta}{\Gamma \vdash \mathbf{op}(v) : T \,!\, \Delta}$$

(HANDLE)

$$\frac{\Gamma \vdash c : S \,!\, \Delta_1 \qquad \Gamma \vdash h : S \,!\, \Delta_1 \Longrightarrow T \,!\, \Delta_2 \qquad \forall \mathsf{op} \in \Delta \setminus \Delta_2.\, \mathsf{op} \in \mathsf{dom}(h)}{\Gamma \vdash \mathbf{handle}\; c \; \mathbf{with}\; \{h\} : T \,!\, \Delta_2}$$

$\boxed{\Gamma \vdash h : S \,!\, \Delta_1 \Longrightarrow T \,!\, \Delta_2}$

(RET-HANDLER)

$$\frac{\Gamma, x : S \vdash c : T \,!\, \Delta_2}{\Gamma \vdash \mathbf{return}(x) \mapsto c : S \,!\, \Delta_1 \Longrightarrow T \,!\, \Delta_2}$$

(OP-HANDLER)

$$\frac{\mathsf{op} : A \to B \in \Sigma \qquad \Gamma \vdash h : S \,!\, \Delta_1 \Longrightarrow T \,!\, \Delta_2 \qquad \Gamma, x : A, k : B \xrightarrow{\Delta_2}\!\!\!\twoheadrightarrow T \vdash c : T \,!\, \Delta_2 \qquad \Delta_2 \subseteq \Delta_1 \setminus \{\mathsf{op}\} \qquad \mathbf{op}(x', k') \mapsto c' \notin h}{\Gamma \vdash h;\mathbf{op}(x, k) \mapsto c : S \,!\, \Delta_1 \Longrightarrow T \,!\, \Delta_2}$$

Figure 2.4.: Typing rules for λ_{op} terms. Typing judgements are stratified into value, computation, and handler judgments.

(2) The rest of the handler $h = \mathtt{return}(x) \mapsto \mathtt{return}\ (x, "")$ has type $\mathbb{N}\,!\,\{\mathtt{print}\} \Longrightarrow$ $(\mathbb{N} \times \mathsf{String})\,!\,\emptyset$. This follows from a trivial application of the RET-HANDLER rule.

(3) The body
$$\mathtt{do}\ (v, s) \leftarrow \mathtt{continue}\ k\ ()\ \mathtt{in\ return}\ (v, \mathtt{f"}\{x\};\texttt{"}\,\hat{}\,s)$$
has type $(\mathbb{N} \times \mathsf{String})\,!\,\emptyset$, assuming x has type $\mathbb{N}$ and k has type $1 \xrightarrow{\ \emptyset\ }\!\!\!\!\twoheadrightarrow (\mathbb{N} \times \mathsf{String})$. This is easy to show.

(4) The handler *only* removes $\mathtt{print}$ from the effects row, and no other effects. This check passes, but would fail if we tried to type the handler with, for example, $\mathbb{N}\,!\,\{\mathtt{print}, \mathtt{get}\} \Longrightarrow (\mathbb{N} \times \mathsf{String})\,!\,\emptyset$

(5) There are no other handlers for $\mathtt{print}$ in h.

Finally, I define a notion of well-typed closed computation. To show that a closed computation is well-typed, it is sufficient to type it with an empty effects row.

> **Definition 2.2.1 (Well-typed closed computation)**
> c *is well-typed if* $\cdot \vdash c : T\,!\,\emptyset$

Metatheory

Discussion around the interaction between effect handlers and metaprogramming will build on some metatheoretic properties of λ_{op}, which are proven by Bauer and Pretnar [2].

> **Theorem 2.2.2 (Progress)**
> *If* $\Gamma \cdot \vdash E[c] : T\,!\,\Delta$ *then either*
>
> 1. *c is of the form* $\mathtt{return}\ v$ *and* $E = [-]$,
>
> 2. *c is of the form* $\mathtt{op}(v)$ *for some* $op \in \Delta$, *and* $op \notin handled(E)$
>
> 3. *$\exists.E', c'$ such that* $\langle c; E \rangle \rightarrow \langle c'; E' \rangle$

> **Theorem 2.2.3 (Preservation)**
> *If* $\Gamma \cdot \vdash E[c] : T\,!\,\Delta$ *and* $\langle c; E \rangle \rightarrow \langle c'; E' \rangle$, *then* $\Gamma \cdot \vdash E'[c'] : T\,!\,\Delta$

> **Corollary 2.2.4 (Type Safety)**
> *If* $\cdot \vdash c : T\,!\,\emptyset$ *then either*
>
> 1. $\langle c; [-] \rangle \rightarrow^{\omega}$ *(non-termination)*
>
> 2. $\langle c; [-] \rangle \rightarrow^{*} \langle \mathtt{return}\ v; [-] \rangle$

2.2.3. The Design Space of Effect Handlers

The design space of effect handlers is large. Different design decisions could impact how effect handlers interact with metaprogramming. This thesis focuses on unnamed and deep effect handlers that permit multi-shot continuations:

1. **Named or Unnamed Handlers**
   Can an effect invoke a specific handler, rather than the latest?

   In λ_{op}, when there are multiple handlers for the same effect, the "latest" handler for that effect is invoked. An alternative approach is **named handlers** [37], where, by associating each handler with a *name*, the programmer can more easily specify which handler should be invoked.

   While named handlers can be more ergonomic, they do not provide greater expressiveness [37]. This thesis only considers unnamed handlers.

2. **Deep, Shallow, or Sheep Handlers**
   Are multiple instances of the same effect handled by the same handler?

   In λ_{op}, continuations reinstate handlers (Eff-Op) and thus multiple instances of the same effect are handled by the same handler. For example, in the following example, the effect **addn** is handled by the same handler, adding one each time. These are known as **deep** handlers.

   ```
   handle                                                    λop
      addn(1) + addn(2)
   with
      {return(x) ↦ return x;
       addn(y, k) ↦ continue k (y + 1)}
   ─────────────────────────────────────────────────────────
   return 5
   ```

   An alternative semantics would *not* to reinstate the handler, in an approach known as **shallow** handlers [9]. The example above would be stuck, since the second **addn** would not be handled.

   Another alternative would be to modify the interface for **continue** such that it accepts a handler

   $$\textbf{continue}\ k\ v\ h$$

   This would allow multiple effects to be handled by different handlers. That is, the programmer could add 1 the first time **addn** is performed, and 2 the second time (the program would return $2 + 4 = 6$). These handlers behave as a hybrid of shallow and deep handlers, and are thus termed **sheep** handlers [23].

   In keeping with most prior work on scope extrusion, this thesis focuses on deep handlers [12].

3. **One-Shot or Multi-Shot Continuations**
   How many times can the same continuation be resumed?

   In λ_{op}, continuations may be resumed multiple times. For example, the programmer can write

```
                                                                        λ_op
handle
  performTwice(1)
with
  {return(x) ↦ return x;
   performTwice(y, k) ↦ (continue k y) + (continue k y)}
──────────────────────────────────────────────────────────
return 2
```

Such an effect system is said to permit **multi-shot continuations**. Multi-shot continuations are useful for simulating certain effects, like non-determinism [23].

In `OCaml`, multi-shot continuations are not allowed: continuations are only allowed to be resumed once. These systems permit only **one-shot continuations**.

Although continuations in `OCaml` are one-shot, this thesis studies effect systems with multi-shot continuations.

2.3. Scope Extrusion

Scope extrusion is an undesirable consequence of unrestricted interaction between effect handlers and metaprogramming. To illustrate scope extrusion, I first extend λ_{op} (Section 2.2.2) with quotes $\langle\langle e \rangle\rangle$ and splices $\$e$.

Scope extrusion is observed when programs are evaluated. To evaluate quotes and splices, I rely on the conceptual model introduced in Section 2.1, where quotes convert terms to ASTs, and splices under quotes suspend this conversion (made precise in Section 3.3). Additionally, in this section, I assume all computation implicitly takes place under a top-level splice. For example, extending λ_{op} with **skip**, the following program:

```
                                                                        λ_op
⟨⟨λx : ℕ. $(skip; ⟨⟨x⟩⟩) + 0⟩⟩
```

is desugared into:

```
                                                                        λ_op
return Lam(skip; Var(x_ℕ), Plus(Var(x_ℕ), Nat(0)))
```

and thus evaluates to:

```
                                                                        λ_op
return Lam(Var(x_ℕ), Plus(Var(x_ℕ), Nat(0)))
```

Listing 5 illustrates the problem of scope extrusion. The program performs an effect, **extrude**, with type $\mathbb{N}\,\mathsf{expr} \to \mathbb{N}\,\mathsf{expr}$. The handler for **extrude** discards the continuation, returning the value it was given: $\mathsf{Var}(x_\mathbb{N})$. The program evaluates to $\mathsf{Var}(x_\mathbb{N})$, and the generated AST is ill-scoped. The result of evaluation demonstrates scope extrusion.

```
                                                                              λop
handle
   ⟨⟨ λx : ℕ. $ (extrude( ⟨⟨x⟩⟩ )) ⟩⟩
with
   {return(u) ↦ return ⟨⟨0⟩⟩;
    extrude(y, k) ↦ return y}
─────────────────────────────────────────────
return Var(x_ℕ)
```

Listing 5: A λ_{op} program that evaluates to $\text{Var}(x_\mathbb{N})$. The AST is ill-scoped, and thus exhibits scope extrusion. It is used as a running example.

```
                                                                              λop
handle
   ⟨⟨ λx : ℕ. $ (extrude( ⟨⟨x⟩⟩ )) ⟩⟩
with
   {return(u) ↦ return u;
    extrude(y, k) ↦ continue k y}
─────────────────────────────────────────────
return Lam(Var(x_ℕ), Var(x_ℕ))
```

Listing 6: A λ_{op} program where the result of the program is well-scoped, but not all intermediate results are well-scoped.

It is difficult to give a precise definition to scope extrusion, because there are multiple competing definitions [16, 19], and many are given informally. For example, is scope extrusion a property of the *result* of evaluation [19], as in Listing 5, or is it a property of *intermediate* configurations [16]? It is possible to build ASTs with extruded variables that are bound at some future point in the execution. The program in Listing 6 produces, during its evaluation, the intermediate AST $\text{Var}(x_\mathbb{N})$, which is not well scoped. However, the result of evaluation, $\text{Lam}(\text{Var}(x_\mathbb{N}), \text{Var}(x_\mathbb{N}))$, is well scoped. Whether Listing 6 exhibits scope extrusion depends on the definition of scope extrusion.

Nevertheless, both definitions agree on the example in Listing 5. Making precise the competing definitions of scope extrusion is a contribution of this dissertation.

2.3.1. Existing Solutions to the Scope Extrusion Problem

There are multiple solutions to the problem of scope extrusion. The solution space can be broadly divided into two types of approaches: static (type-based) and dynamic (checks are inserted into code generators, and errors raised when the code generator is executed). This section surveys two dynamic approaches, which I term the lazy and eager checks, and one static approach, the method of refined environment classifiers [19, 12].

Lazy Dynamic Check

Scope extrusion of the kind in Listing 5 may seem trivial to resolve: evaluate the program to completion, and check that the resulting AST is well-scoped [16]. I term this the **lazy dynamic check**. This approach, while clearly correct and maximally expressive, is not ideal for efficiency and error reporting reasons.

```
                                                                      λ_op
do x ← handle
        ⟨⟨ λx : ℕ. $ (extrude( ⟨⟨x⟩⟩ )) ⟩⟩
      with
        {return(u) ↦ return ⟨⟨0⟩⟩;
         extrude(y, k) ↦ return y}
in some very long program; return x
```
```
return Var(x_ℕ)
```

Listing 7: A λ_{op} program that evaluates to $\text{Var}(x_\mathbb{N})$. Executing the entire program to determine if it exhibits scope extrusion is inefficient.

To illustrate the inefficiency of this approach, consider a slight variation of Listing 5, Listing 7. In Listing 7, in theory, it is possible to report a warning as soon as the effect is handled. Waiting for the result of the program can be much more inefficient.

In terms of error reporting, note that, in waiting for the result of execution, the lazy dynamic check loses information about *which program fragment* was responsible for scope extrusion, reducing the informativeness of reported errors [16].

Eager Dynamic Check

Motivated by the problems with the lazy dynamic check, the **eager dynamic check**, first introduced by Kiselyov [16] and implemented in BER MetaOCaml, adopts a stricter definition of scope extrusion: unbound free variables in intermediate ASTs are defined to be scope extrusion. By this definition, Listing 6 exhibits scope extrusion. To report scope extrusion, checks are inserted at various intermediate points of code generation (in contrast to the lazy dynamic check, where only one check is inserted at the end of code generation). The eager dynamic check offers better efficiency and error reporting guarantees over the lazy dynamic check [16].

However, the eager dynamic check is not without issues. First, even by its own definition, the eager dynamic check does not catch all occurrences of scope extrusion: while the program in Listing 6 is theoretically scope extrusion, scope extrusion is not actually reported by the check.

Second, the check is unpredictable. The problem relates to *when* the checking is performed, which will be made precise in Section 4.2. To illustrate the problem, consider Listing 8, a slight variation of Listing 6 in which the program fragment y in **continue** $k\,y$ is replaced with **continue** $k\,\langle\langle\$y + 0\rangle\rangle$. In contrast to Listing 6, Listing 8 will fail the check: scope extrusion will be reported.

```
                                                                      λ_op
handle
  ⟨⟨ λx : ℕ. $ (extrude( ⟨⟨x⟩⟩ )) ⟩⟩
with
  {return(u) ↦ return u;
   extrude(y, k) ↦ continue k ⟨⟨$y + 0⟩⟩}
```
```
return Lam(Var(x_ℕ), Plus(Var(x_ℕ), Nat(0)))
```

Listing 8: A λ_{op} program that is a slight variation of Listing 6, but that (unlike Listing 6) fails the eager dynamic check.

Without knowledge of the internal operation of the check (Section 4.2), it is difficult to reason about which programs will pass, and which will fail, the eager dynamic check. I conjecture that this behaviour is unintuitive, and exposes too much of the internal operation of the check to the programmer.

Refined Environment Classifiers

Refined environment classifiers are a static check that uses the type system to prevent scope extrusion. Recall that metaprogramming involves the *creation* and *manipulation* of ASTs. Refined environment classifiers prevent scope extrusion by checking that:

1. *Created* ASTs are well-scoped

2. *Manipulating* ASTs preserves well-scopedness

First, ignoring the ability to manipulate ASTs, how do refined environment classifiers ensure *created* ASTs are well-scoped? What does it mean to be well-scoped? Consider Figure 2.5, the AST of the following term:

$$(\lambda f.\lambda x.f x)(\lambda y.y)$$

Informally, a scope represents a set of variables that are permitted to be free. In the example, there are four scopes: one where no variables are free, one where only f is free, one where f and x are free, and one where y is free. An AST is well-scoped *at a scope* if it is well-typed, and where the only free variables are those permitted by the scope.

Refined environment classifiers make this notion precise. Each classifier represents a scope. The AST has four scopes, corresponding to four classifiers:

$\gamma_\perp$ The top-level, where no free variables are permitted

γ_f Only $\mathsf{Var}(f)$ permitted to be free

γ_{fx} Only $\mathsf{Var}(f)$ and $\mathsf{Var}(x)$ permitted to be free

γ_y Only $\mathsf{Var}(y)$ permitted to be free

As every variable binder creates a scope, we may refer to the classifier created by the binder $\mathsf{Lam}(\mathsf{Var}(\alpha), -)$, $\mathsf{classifier}(\mathsf{Lam}(\mathsf{Var}(\alpha), -))$. For example, $\mathsf{classifier}(\mathsf{Lam}(\mathsf{Var}(x), -)) = \gamma_{fx}$.

Classifiers make precise "the variables permitted to be free (within the scope)". As illustrated by the nesting in Figure 2.5, scopes are related to other scopes. For example, since the scope γ_{fx} is created within scope γ_f, any variable tagged with γ_f may be safely used in the scope γ_{fx}. γ_f is compatible with γ_{fx}, written:

$$\gamma_f \sqsubseteq \gamma_{fx}$$

The compatibility relation ($\sqsubseteq$) is a partial order, meaning $\sqsubseteq$ is reflexive, anti-symmetric, and transitive. Further, it identifies a smallest classifier. Reflexivity expresses that $\mathsf{Var}(\alpha)$ may be used within the scope it creates
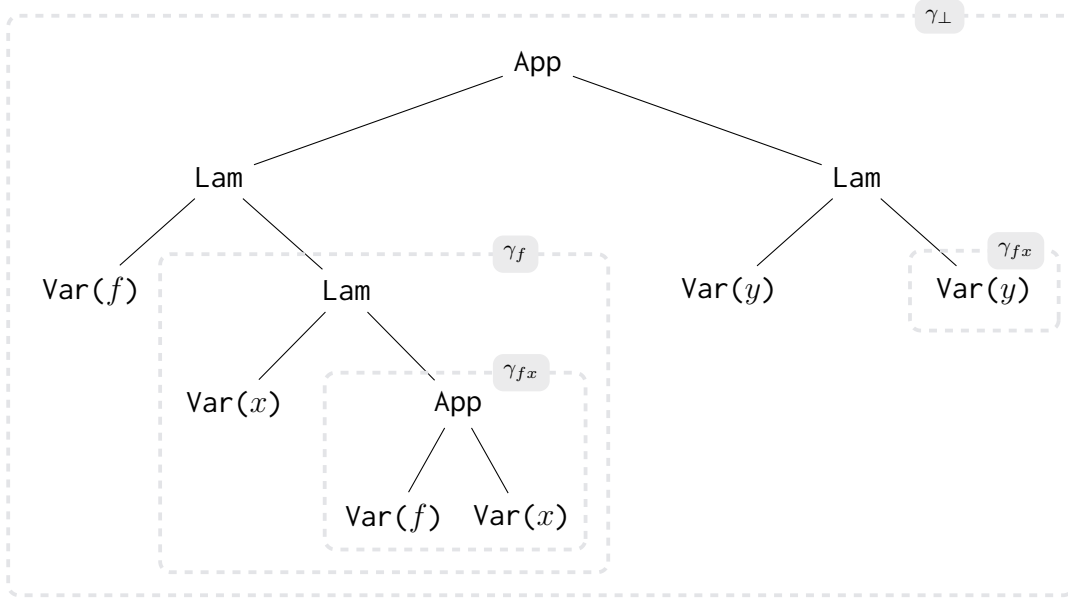
$$\forall \gamma. \gamma \sqsubseteq \gamma$$

Figure 2.5.: The AST of $(\lambda f.\lambda x.fx)(\lambda y.y)$, where each scope is labelled with the corresponding environment classifier.

anti-symmetry captures that nesting only proceeds in one direction

$$\forall \gamma_1, \gamma_2.\ \gamma_1 \sqsubseteq \gamma_2 \land \gamma_2 \sqsubseteq \gamma_1 \implies \gamma_1 = \gamma_2$$

and transitivity accounts for nestings within nestings

$$\forall \gamma_1, \gamma_2, \gamma_3.\ \gamma_1 \sqsubseteq \gamma_2 \land \gamma_2 \sqsubseteq \gamma_3 \implies \gamma_1 \sqsubseteq \gamma_3$$

$\gamma_\bot$ acts as the least element of this partial order, and captures the notion of "top-level"

$$\forall \gamma.\ \gamma_\bot \sqsubseteq \gamma$$

A classifier γ thus defines a set of variables which are permitted to be free, written permitted(γ):

$$\mathsf{permitted}(\gamma) \triangleq \{\mathsf{Var}(\alpha) \mid \mathsf{classifier}(\mathsf{Lam}(\mathsf{Var}(\alpha), -)) \sqsubseteq \gamma\}$$

For example, $\mathsf{permitted}(\gamma_{fx}) = \{\mathsf{Var}(f), \mathsf{Var}(x)\}$

An AST n is well-scoped at type T and scope γ if it is well-typed at T, and all free variables in n are in $\mathsf{permitted}(\gamma)$, written:

$$\Gamma \vdash^\gamma n : T$$

Ensuring that created ASTs are well-scoped is the responsibility of the type system. The key rule is the C-ABS rule, which, **assuming we know that we are creating an AST**, has roughly the following shape[2]:

$$
\text{(C-ABS)}\\
\frac{\gamma \in \Gamma \qquad (2)\,\gamma' \text{ fresh} \qquad (3)\,\Gamma, \gamma', \gamma \sqsubseteq \gamma', (x : T_1)^{\gamma'} \vdash^{\gamma'} c : T_2}{(1)\,\Gamma \vdash^\gamma \lambda x.c : T_1 \longrightarrow T_2}
$$

The premises and conclusions have been numbered for reference, and many technical details have been simplified for clarity. Figure 2.6 visually depicts the typing rule.

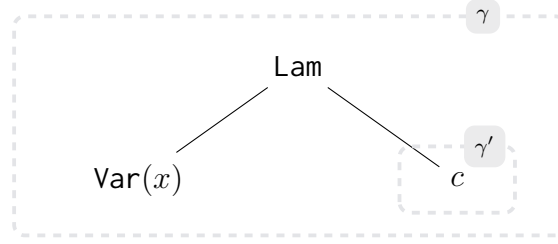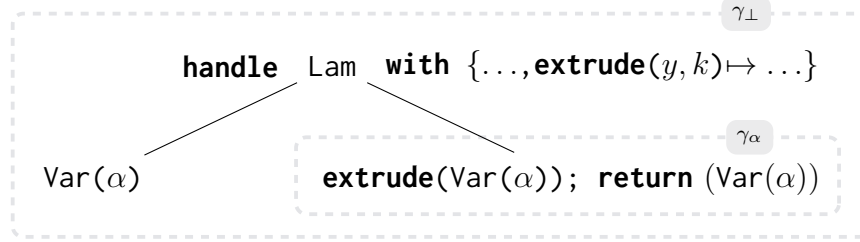[2]I revisit this assumption in Section 3.1.1

Figure 2.6.: Visual depiction of the C-ABS typing rule.

Figure 2.7.: The "AST" of the scope extrusion example, Listing 5. Notice that in place of AST nodes, we may now have compile-time executable programs that *evaluate* to AST nodes.

(1) The goal of the typing rule is to ensure the function is well-scoped at type $T_1 \to T_2$ and scope γ.

(2) Since the function introduces a new variable binder, $\text{Var}(x)$, one has to create a new scope. This is achieved by picking a fresh classifier γ'.

(3) We record the following:

  (a) Since γ' is created within the scope of γ, $\gamma \sqsubseteq \gamma'$.

  (b) $\text{classifier}(\text{Lam}(\text{Var}(x), -)) = \gamma'$ (as a shorthand $(x : T_1)^{\gamma'}$)

  With this added knowledge, we ensure that the function body is well-scoped at type T_2 and γ'.

The above example focused on **creating** ASTs, and had no compile-time executable code. Refined environment classifiers additionally ensure well-scopedness is maintained while **manipulating** ASTs. Consider Figure 2.7, the "AST" of the scope extrusion example in Listing 5. Notice that in place of AST nodes, we may now have compile-time executable programs that *evaluate* to AST nodes. Thus, both programs and AST nodes reside within scopes. We have two classifiers: $\gamma_\perp$ and γ_α, with $\text{classifier}(\text{Var}(\alpha)) = \gamma_\alpha$.

Key to the prevention of scope extrusion is the typing of handlers and operations, like **extrude**, that manipulate ASTs. Since these rules are complex, I describe them informally. The handle expression

$$\textbf{handle } e \textbf{ with } \{h\}$$

is in scope $\gamma_\perp$. Therefore, for each operation handled by h (e.g. **extrude**), the argument to the operation must either not be an AST, or be an AST that is well-scoped at some $\gamma \sqsubseteq \gamma_\perp$. However, $\text{Var}(\alpha)$ is typed at γ_α, and clearly, $\gamma_\alpha \not\sqsubseteq \gamma_\perp$. There is thus no way to type the scope extrusion example in Listing 5.

Note that the analysis was independent of the *body* of the handler. Therefore, the examples in Listings 6 and 8 are *also* not well-typed. Perhaps somewhat surprisingly, so too is Listing 9 (which would pass both the eager and lazy dynamic checks). Refined environment classifiers statically prevent variables ($\text{Var}(\alpha)$) from becoming *available* in program fragments ($\textbf{op}(y, k) \mapsto \ldots$) where, *if misused*, *might* result in scope extrusion. This is, of course, an over-approximation that rejects benign programs such as Listing 9.

```
                                                                        λop
handle
  ⟨⟨ λx : ℕ. $ (extrude( ⟨⟨x⟩⟩ )) ⟩⟩
  {return(u) ↦ return ⟨⟨1⟩⟩;
   extrude(y, k) ↦ return ⟨⟨0⟩⟩}
───────────────────────────────────────────────────────────
return Nat(0)
```

Listing 9: A λ_{op} program that passes the eager and lazy dynamic checks, but is not well-typed under the refined environment classifiers type system.

Listing 9 thus illustrates one of the key drawbacks of refined environment classifiers: the check is too stringent, and restricts expressiveness.
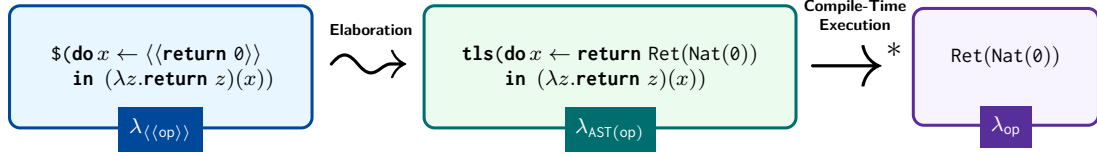
3. Calculus

Figure 3.1.: $\lambda_{\langle\langle op\rangle\rangle}$ is first elaborated into $\lambda_{\mathsf{AST(op)}}$, which is then executed **at compile-time** to obtain the AST of a run-time λ_{op} program.

This thesis considers the interaction between homogenous, compile-time, two-stage **metaprogramming** (Page 4), and deep, unnamed **effect handlers** with multi-shot continuations (Page 9). This chapter describes a calculus, $\lambda_{\langle\langle op\rangle\rangle}$, for studying said interaction. $\lambda_{\langle\langle op\rangle\rangle}$ has both metaprogramming and effect handlers. To the best of my knowledge, this is the first calculus in which one may write effectful compile-time code that generates effectful run-time code (where to be effectful is to have effect handlers). However, $\lambda_{\langle\langle op\rangle\rangle}$ does not mediate the interaction between metaprogramming and effects: scope extrusion prevention is not a language feature. Rather, the aim is to extend $\lambda_{\langle\langle op\rangle\rangle}$ with various scope extrusion checks, and evaluate these checks in a comparative fashion.

Programs written in $\lambda_{\langle\langle op\rangle\rangle}$ cannot be directly executed. Rather, following the style of Xie et al. [38], one must first elaborate (or compile) from $\lambda_{\langle\langle op\rangle\rangle}$ (the "source" language) to $\lambda_{\mathsf{AST(op)}}$ (the "core" language). Programs written in $\lambda_{\mathsf{AST(op)}}$ may then be executed, to obtain the AST of a run-time λ_{op} program. This process, which mirrors the approach by Calcagno et al. [6], is summarised in Figure 3.1. Elaboration is useful, since it simplifies the operational semantics, and is a convenient mechanism for inserting dynamic checks (Chapter 4).

This chapter first introduces $\lambda_{\langle\langle op\rangle\rangle}$ (Section 3.1), then $\lambda_{\mathsf{AST(op)}}$ (Section 3.2). Following this, Section 3.3 describes the elaboration from $\lambda_{\langle\langle op\rangle\rangle}$ to $\lambda_{\mathsf{AST(op)}}$, and Section 3.4 discusses the metatheoretic properties of $\lambda_{\langle\langle op\rangle\rangle}$.

3.1. The Source Language: $\lambda_{\langle\langle \mathbf{op}\rangle\rangle}$

$\lambda_{\langle\langle op\rangle\rangle}$ extends λ_{op} with quotes and splices. Additionally, the continuation term former $\kappa x.e$ is removed, since it cannot be written explicitly in λ_{op} and only occurs during execution, but $\lambda_{\langle\langle op\rangle\rangle}$ has no reduction semantics. Recall that λ_{op} divides terms into three syntactic categories: values (v), computations (c), and handlers (h). $\lambda_{\langle\langle op\rangle\rangle}$ is similar, dividing terms into values (v), expressions (e), and handlers (h) (Figure 3.2).

Notice that values cannot be quoted: only effectful programs may be generated using quotes. For example, $\langle\langle 1\rangle\rangle$ is not valid syntax, instead, one must write $\langle\langle\mathbf{return}\ 1\rangle\rangle$. Similarly, $\langle\langle\mathbf{return}\ 1\rangle\rangle$ is a computation, not a value, so one must write

$$\mathbf{do}\ a \leftarrow \langle\langle\mathbf{return}\ 1\rangle\rangle\ \mathbf{in}\ \mathsf{op}(a)$$

3. Calculus

Syntax

$\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$

Values	v	$::=$	the natural lifting of λ_{op} values, with no term former for continuations
Expressions	e	$::=$	the natural lifting of λ_{op} expressions $\mid \langle\langle e \rangle\rangle \mid \$e$
Handlers	h	$::=$	the natural lifting of λ_{op} handlers

Figure 3.2.: $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ syntax. The syntax is broadly the same as λ_{op}, except with the addition of quotes and splices, and the removal of the continuation term former $\kappa x.e$.

rather than **op**($\langle\langle$**return** $1\rangle\rangle$). However, I will abuse notation and write **op**($\langle\langle 1 \rangle\rangle$) in place of **do** $a \leftarrow \langle\langle$**return** $1\rangle\rangle$ **in op**(a).

3.1.1. Type System

The $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ types are summarised in Figure 3.3. There are three important details: types are stratified into two levels (-1 for compile-time and 0 for run-time), effect rows are similarly stratified, and run-time code is made available at compile-time via a Code type.

First, **types are stratified into two levels,** T^0 **(run-time), and** T^{-1} **(compile-time).**

To motivate this stratification, consider the type of the number 3 in $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$. Perhaps surprisingly, the type of 3 is not $\mathbb{N}$. Since $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ is a two-stage system, it carefully disambiguates between run-time naturals and compile-time naturals, since these are not interchangeable. For example, the following program should **not** be well-typed, since 3 is a compile-time natural, whereas x is a run-time natural:

$$\lambda x : \mathbb{N}. \; \$(3 + x)$$

However, removing the splice makes the program well-typed:

$$\lambda x : \mathbb{N}. \; 3 + x$$

As is conventional for multi-staged languages, $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ introduces integer levels to enforce separation between compile-time and run-time naturals. While the precise notion of level is slightly more involved (Definition 3.1.1), for $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$, it is sufficient to think of level 0 as run-time (so $\mathbb{N}^0$ is a run-time natural), and -1 as compile-time. Naturals can be annotated with levels, hence, the ill-typed example becomes:

$$\lambda x : \mathbb{N}^0. \; \$((3 : \mathbb{N}^{-1}) + (x : \mathbb{N}^0))$$

and the well-typed example becomes (note that, like naturals, the $+$ operator can be annotated with a level):

$$\lambda x : \mathbb{N}^0. \; (3 : \mathbb{N}^0) + (x : \mathbb{N}^0)$$

More precisely, levels are defined as follows:

> **Definition 3.1.1 (Level)**
> *The level of an expression e is calculated by subtracting the number of surrounding splices from the number of surrounding quotations.*

Effects Row

Run-Time	$\xi ::= \emptyset \mid \xi \cup \{\mathsf{op}_i^0\}$
Compile-Time	$\Delta ::= \emptyset \mid \Delta \cup \{\mathsf{op}_i^{-1}\}$

Types

Level 0	Values	$S^0, T^0 ::= \mathbb{N}^0$	naturals
		$\mid (S^0 \xrightarrow{\xi} T^0)^0$	functions
		$\mid (S^0 \xrightarrow{\xi} T^0)^0$	continuations
	Computations	$T^0 \,!\, \xi$	
		$\mid T^0 \,!\, \Delta$	
		$\mid T^0 \,!\, \Delta; \xi$	
	Handlers	$(S^0 \,!\, \xi_1 \Longrightarrow T^0 \,!\, \xi_2)^0 \,!\, \Delta$	
Level -1	Values	$S^{-1}, T^{-1} ::= \mathbb{N}^{-1}$	naturals
		$\mid (S \xrightarrow{\Delta} T)^{-1}$	functions
		$\mid (S \xrightarrow{\Delta} T)^{-1}$	continuations
		$\mid \mathsf{Code}(T^0 \,!\, \xi)^{-1}$	run-time code
	Computations	$T^{-1} \,!\, \Delta$	
	Handlers	$(S^{-1} \,!\, \Delta_1 \Longrightarrow T^{-1} \,!\, \Delta_2)^{-1}$	

Figure 3.3.: $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ types. Types are stratified into two levels, 0 and -1. Similarly, effects are stratified into two levels, ξ (for run-time effects) and Δ (for compile-time effects). The Code type allows compile-time programs to manipulate ASTs of run-time code.

The definition of level generalises to multi-stage languages, where negative levels $(-1, -2, \ldots)$ represent compile-time and non-negative levels $(0, 1, \ldots)$ represent runtime [1]. In a multi-stage language, separation is even more granular: for example, level 1 and level 0 run-time naturals are distinguished. However, since $\lambda_{\langle\langle op \rangle\rangle}$ is a two-stage language, it is sufficient to consider only levels 0 and -1. Definition 3.1.1, and the examples above, further imply that the "default" level, in the absence of quotes and splices, is level 0. Intuitively, in the absence of quotes and splices, the programmer is ignoring metaprogramming facilities, and writing a run-time program.

It is impossible, without further information, to assign a type to *program fragments*, like 3. Without knowledge of the wider context, it is impossible to know which level the program fragment is at: in the ill-typed example, 3 occurs under a splice, but no quotes, so it occurs at level -1 and has type $\mathbb{N}^{-1}$. In contrast, in the well-typed example, 3 occurs at level 0 and has type $\mathbb{N}^0$. Unless otherwise stated, I always assume program fragments occur at level 0.

Second, **effect rows are stratified into ξ (run-time) and Δ (compile-time)**. The following example prints 1 at compile-time, and 2 at run-time. Further, it reads an integer at run-time.

$$\$(\mathbf{print}(1); \langle\langle \mathbf{print}(2); \mathbf{readInt}() \rangle\rangle)$$

Hence, $\Delta = \{\mathbf{print}\}$ and $\xi = \{\mathbf{print}, \mathbf{readInt}\}$. Disambiguating run-time and compile-time effects stratifies types. Unlike in λ_{op}, where a term is either of value or computation type, in $\lambda_{\langle\langle op \rangle\rangle}$, the stratification of types is thus more granular:

T^0	Compile-time value, run-time value (value types)
	Example: The type of x in $\lambda x.\mathbf{return}\ x$
$T^0\,!\,\xi$	Compile-time value, run-time computation
	Example: The type of x in $\$(\mathbf{do}\ x \leftarrow \langle\langle \mathbf{return}\ 1 \rangle\rangle\ \mathbf{in\ return}\ x)$
$T^0\,!\,\Delta$	Compile-time computation, run-time value
	Example: $\lambda x.\mathbf{return}\ x$
$T^0\,!\,\Delta;\xi$	Compile and run-time computation
	Example: $\$(\mathbf{do}\ x \leftarrow \langle\langle \mathbf{return}\ 1 \rangle\rangle\ \mathbf{in\ return}\ x)$

Further, the relationship between syntax and types is more complicated than in λ_{op}. For example, level 0 $\lambda_{\langle\langle op \rangle\rangle}$ values (v) do not have value type (T^0). Rather, since level 0 values are elaborated into compile-time computations that produce ASTs of run-time values, they have computation type $T^0\,!\,\Delta$ (Table 3.1). As the stratification is subtle, it is best revisited after covering the typing rules (Section 3.1.1), core language (Section 3.2), and elaboration (Section 3.3).

Third, **there is a level -1 Code type, representing run-time ASTs**. Stratifying types ensures that run-time (resp. compile-time) terms only interact with run-time (compile-time) terms. However, to enable meta-programming, run-time terms should be available at compile-time as ASTs. This is exactly the role of the Code type, thus allowing level -1 programs to manipulate ASTs of level 0 terms.

Putting it all together, we can now interpret complex $\lambda_{\langle\langle op \rangle\rangle}$ types, like the following:

---

[1] Many existing languages only consider compile-time **or** run-time metaprogramming, not both, and will thus have either non-positive or non-negative levels.

$$(\text{Code}(\mathbb{N}^0!\{\text{print}\}))^{-1} \xrightarrow{\{\text{get}\}} \text{Code}(\mathbb{N}^0!\{\text{print}, \text{readInt}\})^{-1})^{-1}$$

Compile-time ② effects

Compile-time ① function

③ Input: AST of a run-time computation of type $\mathbb{N}!\{\text{print}\}$

④ Output: AST of a run-time computation of type $\mathbb{N}!\{\text{print}, \text{readInt}\}$
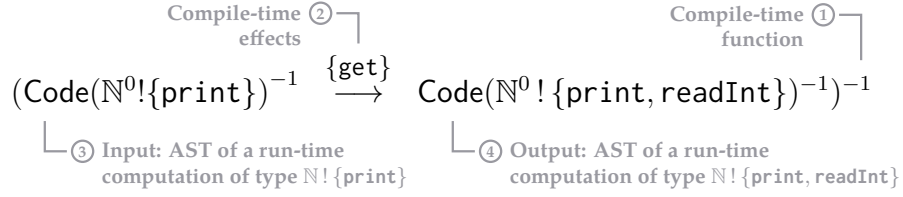
Typing Judgements

	Value (v)	**Expression** (e)	**Handler** (h)
Compile (c)	$\Gamma \vdash_{\mathsf{c}}^{0} v : T^0 ! \Delta$	$\Gamma \vdash_{\mathsf{c}}^{0} e : T^0 ! \Delta; \xi$	$\Gamma \vdash_{\mathsf{c}}^{0} h : (S^0 ! \xi_1 \Longrightarrow T^0 ! \xi_2)^0 ! \Delta$
Quote (q)	$\Gamma \vdash_{\mathsf{q}}^{0} v : T^0 ! \Delta$	$\Gamma \vdash_{\mathsf{q}}^{0} e : T^0 ! \Delta; \xi$	$\Gamma \vdash_{\mathsf{q}}^{0} h : (S^0 ! \xi_1 \Longrightarrow T^0 ! \xi_2)^0 ! \Delta$
Splice (s)	$\Gamma \vdash_{\mathsf{s}}^{-1} v : T^{-1}$	$\Gamma \vdash_{\mathsf{s}}^{-1} e : T^{-1} ! \Delta$	$\Gamma \vdash_{\mathsf{s}}^{-1} h : (S^{-1} ! \Delta_1 \Longrightarrow T^{-1} ! \Delta_2)^{-1}$

Table 3.1.: The nine $\lambda_{\langle\langle op \rangle\rangle}$ typing judgements

The $\lambda_{\langle\langle op \rangle\rangle}$ typing rules are collated in Figures 3.5 and 3.6. As in Xie et al. [38], typing judgements are indexed by a level and a compiler mode:

$$\Gamma \vdash_{\textbf{Mode}}^{\textbf{Level}} - : =$$

For each (level, mode) pair, similarly to λ_{op}, there are three typing judgements: one for values (v), expressions (e), and handlers (h). This section shows that each compiler mode uniquely determines a level (once shown, I drop the level from the typing judgement). As there are three compiler modes – **Compile** (c), **Quote** (q), and **Splice** (s) – there are nine typing judgements in total, three for each mode (Table 3.1).

Level. Recall that, when describing the λ_{op} types, it was not possible to type a program fragment, like 3, directly. One must also know the *level* (0 or -1), which is attached to the typing judgement.

Modes. For the purposes of elaboration, it is useful to classify code into three categories:

c Code that is **ambient** and **inert**.
No surrounding quotes or splices

s Code that **manipulates ASTs** at compile-time.
Last surrounding annotation is a splice

q Code that **builds ASTs** to be manipulated at compile time.
Last surrounding annotation is a quote

The need for modes arises from the following meta-program, which evaluates to the AST of $\lambda x.1 + 2 + 3$:

$$\lambda x. \$(\textbf{do } f \leftarrow (\lambda y.\langle\langle \$(y) + 2 \rangle\rangle) \textbf{ in do } a \leftarrow \langle\langle 1 \rangle\rangle \textbf{ in } fa) + 3$$

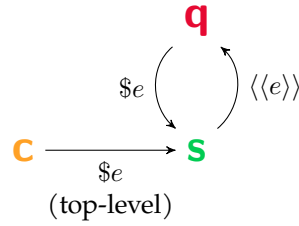c   s   s   q   s   q   s   c

Figure 3.4.: Transitions between modes **c**, **s**, and **q**. Top-level splices transition from **c** to **s**, quotes transition from **s** to **q**, and splices (under quotes) transition from **q** to **s**.

c Identifies AST nodes that are **ambient** (within which computation may take place) and **inert** (cannot themselves be manipulated at compile-time).

$$\lambda x.\, \$(\textbf{do}\ f \leftarrow (\lambda y.\langle\langle \$(y) + 2\rangle\rangle)\ \textbf{in do}\ a \leftarrow \langle\langle 1 \rangle\rangle\ \textbf{in}\ fa) + 3$$

s Identifies code that can be executed at compile-time to **manipulate ASTs**. Will be fully reduced at compile-time, and will not appear at run-time.

$$\lambda x.\, \$(\textbf{do}\ f \leftarrow (\lambda y.\langle\langle \$(y) + 2\rangle\rangle)\ \textbf{in do}\ a \leftarrow \langle\langle 1 \rangle\rangle\ \textbf{in}\ fa) + 3$$

q Identifies code that **builds ASTs** (like **c**-mode) that can be manipulated at compile-time (unlike **c**-mode), to create run-time programs.

$$\lambda x.\, \$(\textbf{do}\ f \leftarrow (\lambda y.\langle\langle \$(y) + 2\rangle\rangle)\ \textbf{in do}\ a \leftarrow \langle\langle 1 \rangle\rangle\ \textbf{in}\ fa) + 3$$

It is possible to transition between modes (Figure 3.4):

1. Top-level splices ($\$e$) transition from **c** (outside the splice) to **s** (within).

2. Quotes ($\langle\langle e\rangle\rangle$) transition from **s** (outside the quote) to **q** (within).

3. Splices ($\$e$) transition from **q** (outside the splice) to **s** (within).

Since $\lambda_{\langle\langle \text{op}\rangle\rangle}$ has only two levels, and the type system bans nested splices and quotations ($\$\$e$ and $\langle\langle\langle\langle e\rangle\rangle\rangle\rangle$ are not valid program fragments), the compiler mode uniquely identifies the level (**c** and **q** imply level 0, and **s** level -1). As shorthand, I thus drop the level from the typing judgement, leaving it implicit.

Further, the typing judgements for **c** and **q** are identical in almost all cases. To avoid repetition, I introduce the following notation:

$$\Gamma \vdash_{\textbf{c}|\textbf{q}} e : T$$

Where, for example, the typing rule

$$\frac{\Gamma_1 \vdash_{\textbf{c}|\textbf{q}} e_1 : T_1 \qquad \cdots \qquad \Gamma_n \vdash_{\textbf{c}|\textbf{q}} e_n : T_n}{\Gamma \vdash_{\textbf{c}|\textbf{q}} e : T}$$

stands for two typing rules, one in **c**-mode and one in **q**-mode.

$$\frac{\begin{array}{c} \Gamma_1 \vdash_{\mathbf{c}} e_1 : T_1 \\ \cdots \\ \Gamma_n \vdash_{\mathbf{c}} e_n : T_n \end{array}}{\Gamma \vdash_{\mathbf{c}} e : T} \qquad \frac{\begin{array}{c} \Gamma_1 \vdash_{\mathbf{q}} e_1 : T_1 \\ \cdots \\ \Gamma_n \vdash_{\mathbf{q}} e_n : T_n \end{array}}{\Gamma \vdash_{\mathbf{q}} e : T}$$

Figure 3.5 summarises the **c** and **q**-mode typing rules. Figure 3.6 summarises the **s**-mode typing rules. In all modes, rules are extremely similar to the λ_{op} typing rules (Figure 2.4, Page 17). Further, the levels of types can, in most cases, be inferred: for readability, they are mostly omitted. The three key rules are **s**-QUOTE, **q**-SPLICE, and **c**-SPLICE.

Recall that the Code type makes level 0 programs available at compile-time, as ASTs. Recall further that $\langle\langle e \rangle\rangle$ is the mechanism for *creating* ASTs (elements of type Code) from run-time programs. This intuition is captured by the **s**-QUOTE rule, where, to verify that, at compile-time, $\langle\langle e \rangle\rangle$ is a valid AST of type Code, it is sufficient to verify that at run-time, e is a program of the corresponding type.

$$\text{(s-QUOTE)}$$
$$\frac{\Gamma \vdash_{\mathbf{q}} e : T^0 \,!\, \Delta; \xi}{\Gamma \vdash_{\mathbf{s}} \langle\langle e \rangle\rangle : \mathsf{Code}(T^0 \,!\, \xi)^{-1} \,!\, \Delta}$$

The dual to $\langle\langle e \rangle\rangle$ is $\$e$, which *eliminates* compile-time ASTs by transforming them (back) into run-time code. This intuition is captured by the **c**-SPLICE (top-level splice) and **q**-SPLICE rules, where, to verify that $\$e$ is a valid run-time program, it is sufficient to verify that e is a valid compile-time AST of the corresponding type.

$$\text{(c-SPLICE)} \qquad\qquad\qquad \text{(q-SPLICE)}$$
$$\frac{\Gamma \vdash_{\mathbf{s}} e : \mathsf{Code}(T^0 \,!\, \xi)^{-1} \,!\, \Delta}{\Gamma \vdash_{\mathbf{c}} \$e : T^0 \,!\, \Delta; \xi} \qquad\qquad \frac{\Gamma \vdash_{\mathbf{s}} e : \mathsf{Code}(T^0 \,!\, \xi)^{-1} \,!\, \Delta}{\Gamma \vdash_{\mathbf{q}} \$e : T^0 \,!\, \Delta; \xi}$$

Note that since there are no **q**-QUOTE or **s**-SPLICE rules, the type system bans nested splices and quotations, and thus we can focus purely on levels 0 and -1.

A closed $\lambda_{\langle\langle \mathsf{op} \rangle\rangle}$ expression is well-typed if, in **c**-mode, it can be typed with empty compile-time and run-time effects rows.

> **Definition 3.1.2 (Well-typed closed expression)**
> *A closed expression e is well-typed if $\cdot \vdash_{\mathbf{c}} e : T^0 \,!\, \emptyset; \emptyset$*

3.2. The Core Language: $\lambda_{\mathsf{AST(op)}}$

The core language, $\lambda_{\mathsf{AST(op)}}$, is a simple extension of λ_{op}. $\lambda_{\mathsf{AST(op)}}$ normal forms (n), terms (t), and handlers (h) are extended versions of λ_{op} values (v), computations (c), and handlers (h) respectively (Figure 3.7).

$\lambda_{\mathsf{AST(op)}}$ extends λ_{op} in two ways. First, it adds machinery for metaprogramming:

1. **AST** nodes (like Nat and Var) and *type-annotated* **formal parameters** (α_R, where R is some run-time value pre-type[2], henceforth simply "type").

---

[2]see Figure 3.9

c and **q**-mode Typing Rules
Level annotations on types mostly omitted

$\lambda_{\langle\langle \mathsf{op}\rangle\rangle}$

$$\boxed{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} v : T^0 \,!\, \Delta}$$

(NAT)

$$\overline{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} m : \mathbb{N} \,!\, \Delta}$$

(VAR)

$$\frac{\Gamma(x) = T^0}{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} x : T^0 \,!\, \Delta}$$

(LAMBDA)

$$\frac{\Gamma, x : S \vdash_{\mathsf{c}|\mathsf{q}} e : T \,!\, \Delta; \xi}{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} \lambda x.e : (S \xrightarrow{\xi} T) \,!\, \Delta}$$

$$\boxed{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} e : T^0 \,!\, \Delta; \xi}$$

(APP)

$$\frac{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} v_1 : (S \xrightarrow{\xi} T) \,!\, \Delta \quad \Gamma \vdash_{\mathsf{c}|\mathsf{q}} v_2 : S \,!\, \Delta}{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} v_1 v_2 : T \,!\, \Delta; \xi}$$

(CONTINUE)

$$\frac{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} v_1 : (S \xrightarrow{\xi} T) \,!\, \Delta \quad \Gamma \vdash_{\mathsf{c}|\mathsf{q}} v_2 : S \,!\, \Delta}{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} \mathbf{continue}\ v_1\ v_2 : T \,!\, \Delta; \xi}$$

(RETURN)

$$\frac{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} v : T \,!\, \Delta}{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} \mathbf{return}\ v : T \,!\, \Delta; \xi}$$

(DO)

$$\frac{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} e_1 : S \,!\, \Delta; \xi \quad \Gamma, x : S \vdash_{\mathsf{c}|\mathsf{q}} e_2 : T \,!\, \Delta; \xi}{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} \mathbf{do}\ x \leftarrow e_1\ \mathbf{in}\ e_2 : T \,!\, \Delta; \xi}$$

(OP)

$$\frac{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} v : S \,!\, \Delta \quad \mathsf{op} : S \to T \in \Sigma \quad \mathsf{op} \in \xi}{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} \mathbf{op}(v) : T \,!\, \Delta; \xi}$$

(HANDLE)

$$\frac{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} e : S \,!\, \Delta; \xi_1 \quad \Gamma \vdash_{\mathsf{c}|\mathsf{q}} h : S \,!\, \xi_1 \Longrightarrow T \,!\, \xi_2 \,!\, \Delta \quad \forall \mathsf{op} \in \xi_1 \setminus \xi_2 . \mathsf{op} \in \mathsf{dom}(h)}{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} \mathbf{handle}\ e\ \mathtt{with}\ \{h\} : T \,!\, \Delta; \xi_2}$$

(**c**-SPLICE)

$$\frac{\Gamma \vdash_{\mathsf{s}} e : \mathsf{Code}(T^0 \,!\, \xi)^{-1} \,!\, \Delta}{\Gamma \vdash_{\mathsf{c}} \$e : T^0 \,!\, \Delta; \xi}$$

(**q**-SPLICE)

$$\frac{\Gamma \vdash_{\mathsf{s}} e : \mathsf{Code}(T^0 \,!\, \xi)^{-1} \,!\, \Delta}{\Gamma \vdash_{\mathsf{q}} \$e : T^0 \,!\, \Delta; \xi}$$

$$\boxed{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} h : (S^0 \,!\, \xi_1 \Longrightarrow T^0 \,!\, \xi_2)^0 \,!\, \Delta}$$

(RET-HANDLER)

$$\frac{\Gamma, x : S \vdash_{\mathsf{c}|\mathsf{q}} e : T \,!\, \Delta; \xi_2}{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} \mathbf{return}(x) \mapsto e : S \,!\, \xi_1 \Longrightarrow T \,!\, \xi_2 \,!\, \Delta}$$

(OP-HANDLER)

$$\frac{\mathsf{op} : A \to B \in \Sigma \quad \Gamma \vdash_{\mathsf{c}|\mathsf{q}} h : S \,!\, \xi \Longrightarrow T \,!\, \xi_2 \,!\, \Delta \quad \Gamma, x : A, k : B \xrightarrow{\xi_2} T \vdash_{\mathsf{c}|\mathsf{q}} e : T \,!\, \Delta; \xi_2 \quad \xi_2 \subseteq \xi_1 \setminus \{\mathsf{op}\} \quad \mathbf{op}(x', k') \mapsto e' \notin h}{\Gamma \vdash_{\mathsf{c}|\mathsf{q}} h; \mathbf{op}(x, k) \mapsto e : S \,!\, \xi_1 \Longrightarrow T \,!\, \xi_2 \,!\, \Delta}$$

Figure 3.5.: The **c**-mode and **q**-mode typing rules for $\lambda_{\langle\langle \mathsf{op}\rangle\rangle}$. The rules are nearly identical to the λ_{op} typing rules. Two additional rules, (**c**-SPLICE) (top-level splice) and (**q**-SPLICE) formalise the transition to **s**-mode.

s-mode Typing Rules

$\lambda_{\langle\langle \text{op} \rangle\rangle}$

Level annotations on types mostly omitted

$$\boxed{\Gamma \vdash_{\mathsf{s}} v : T^{-1}}$$

(**s**-NAT)

$$\frac{}{\Gamma \vdash_{\mathsf{s}} m : \mathbb{N}}$$

(**s**-VAR)

$$\frac{\Gamma(x) = T^{-1}}{\Gamma \vdash_{\mathsf{s}} x : T^{-1}}$$

(**s**-LAMBDA)

$$\frac{\Gamma, x : S \vdash_{\mathsf{s}} e : T \,!\, \Delta}{\Gamma \vdash_{\mathsf{s}} \lambda x.e : (S \xrightarrow{\Delta} T)}$$

(**s**-CONTINUATION)

$$\frac{\Gamma, x : S \vdash_{\mathsf{s}} e : T \,!\, \Delta}{\Gamma \vdash_{\mathsf{s}} \kappa x.e : (S \xRightarrow{\Delta} T)}$$

$$\boxed{\Gamma \vdash_{\mathsf{s}} e : T^{-1} \,!\, \Delta}$$

(**s**-APP)

$$\frac{\Gamma \vdash_{\mathsf{s}} v_1 : (S \xrightarrow{\Delta} T) \qquad \Gamma \vdash_{\mathsf{s}} v_2 : S}{\Gamma \vdash_{\mathsf{s}} v_1 \, v_2 : T \,!\, \Delta}$$

(**s**-CONTINUE)

$$\frac{\Gamma \vdash_{\mathsf{s}} v_1 : (S \xRightarrow{\Delta} T) \qquad \Gamma \vdash_{\mathsf{s}} v_2 : S}{\Gamma \vdash_{\mathsf{s}} \mathtt{continue}\, v_1 \, v_2 : T \,!\, \Delta}$$

(**s**-RETURN)

$$\frac{\Gamma \vdash_{\mathsf{s}} v : T}{\Gamma \vdash_{\mathsf{s}} \mathtt{return}\, v : T \,!\, \Delta}$$

(**s**-DO)

$$\frac{\Gamma \vdash_{\mathsf{s}} e_1 : S \,!\, \Delta \qquad \Gamma, x : S \vdash_{\mathsf{s}} e_2 : T \,!\, \Delta}{\Gamma \vdash_{\mathsf{s}} \mathtt{do}\, x \leftarrow e_1 \;\mathtt{in}\; e_2 : T \,!\, \Delta}$$

(**s**-OP)

$$\frac{\Gamma \vdash_{\mathsf{s}} v : S \qquad \mathsf{op} : S \to T \in \Sigma \qquad \mathsf{op} \in \Delta}{\Gamma \vdash_{\mathsf{s}} \mathbf{op}(v) : T \,!\, \Delta}$$

(**s**-HANDLE)

$$\frac{\begin{array}{c} \Gamma \vdash_{\mathsf{s}} e : S \,!\, \Delta_1 \\ \Gamma \vdash_{\mathsf{s}} h : (S \,!\, \Delta_1 \Longrightarrow T \,!\, \Delta_2) \\ \forall \mathsf{op} \in \Delta_1 \setminus \Delta_2.\, \mathsf{op} \in \mathsf{dom}(h) \end{array}}{\Gamma \vdash_{\mathsf{s}} \mathtt{handle}\, e \;\mathtt{with}\; \{h\} : T \,!\, \Delta_2}$$

(**s**-QUOTE)

$$\frac{\Gamma \vdash_{\mathsf{q}} e : T^0 \,!\, \Delta; \xi}{\Gamma \vdash_{\mathsf{s}} \langle\langle e \rangle\rangle : \mathsf{Code}(T^0 \,!\, \xi)^{-1} \,!\, \Delta}$$

$$\boxed{\Gamma \vdash_{\mathsf{s}} h : (S^{-1} \,!\, \Delta_1 \Longrightarrow T^{-1} \,!\, \Delta_2)^{-1}}$$

(**s**-RET-HANDLER)

$$\frac{\Gamma, x : S \vdash_{\mathsf{s}} e : T \,!\, \Delta_2}{\Gamma \vdash_{\mathsf{s}} \mathtt{return}(x) \mapsto e : (S \,!\, \Delta_1 \Longrightarrow T \,!\, \Delta_2)}$$

(**s**-OP-HANDLER)

$$\frac{\begin{array}{c} \mathsf{op} : A \to B \in \Sigma \\ \Gamma \vdash_{\mathsf{s}} h : (S \,!\, \Delta_1 \Longrightarrow T \,!\, \Delta_2) \\ \Gamma, x : A, k : (B \xRightarrow{\Delta_2} T) \vdash_{\mathsf{s}} e : T \,!\, \Delta_2 \qquad \Delta_2 \subseteq \Delta_1 \setminus \{\mathsf{op}\} \qquad \mathbf{op}(x', k') \mapsto e' \notin h \end{array}}{\Gamma \vdash_{\mathsf{s}} h; \mathbf{op}(x, k) \mapsto e : (S \,!\, \Delta_1 \Longrightarrow T \,!\, \Delta_2)}$$

Figure 3.6.: The **s**-mode typing rules for $\lambda_{\langle\langle \text{op} \rangle\rangle}$. The rules (sans levels) are identical to the λ_{op} typing rules. The additional **s**-QUOTE rule makes level 0 code available at compile-time.

Similarly to Calcagno et al. [6], the syntax explicitly disambiguates between formal parameters (α_R) and AST nodes. The only difference is that Calcagno et al. use untyped formal parameters (α). For example, consider the AST of $\lambda\alpha{:}\mathbb{N}.\,\alpha$, where the formal parameter (left subtree) is contrasted with its usage (right subtree):

$$
\begin{array}{c}
\text{Lam} \\
\swarrow \quad \searrow \\
\alpha_\mathbb{N} \quad \text{Var}(\alpha_\mathbb{N})
\end{array}
$$
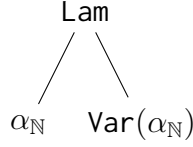
This syntactic distinction is important because it keeps the typing rules syntax directed, and FParams and ASTs need to have different types. If the type system did not distinguish FParams and ASTs, the following malformed AST would be well-typed:

$$
\begin{array}{c}
\text{Lam} \\
\swarrow \quad \searrow \\
\text{Nat(0)} \quad \text{Nat(0)}
\end{array}
$$
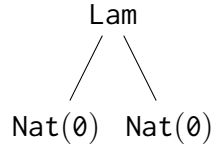
2. **mkvar** R, a primitive for generating fresh formal parameters of type R, α_R, where two different calls to **mkvar** should return two different formal parameters.

   The need for **mkvar** arises from treating $\lambda_{\text{AST(op)}}$ as an elaboration target for $\lambda_{\langle\langle\text{op}\rangle\rangle}$. Consider Listing 10, which should generate the AST of $\lambda\alpha.\lambda\beta.\,\textbf{return }(\alpha,\beta)$.

   ```
   $(do mkfun ← λk.⟨⟨ λx : ℕ⁰. $(k ⟨⟨x⟩⟩) ⟩⟩ in
       mkfun ( λa. mkfun (λb. return (a, b))) )                          λ⟨⟨op⟩⟩

   return Lam(αℕ, Lam(βℕ, Ret(Pair(Var(αℕ), Var(βℕ)))))
   ```

   Listing 10: An example $\lambda_{\langle\langle\text{op}\rangle\rangle}$ program which illustrates the need for **mkvar**

   The compile-time function `mkfun` (Walid's [35] back) is a higher-order function that accepts some compile-time function k. `mkfun` creates a binder ($\lambda x.\_$) and passes the formal parameter x to k. k uses x to construct the body of a function $\lambda x.\text{body}$. For example, `mkfun` $(\lambda y.\langle\langle\$(y)+1\rangle\rangle)$ generates the body $x+1$.

   In Listing 10, k calls `mkfun`. This constructs a *nested* function, whose formal parameters are bound to a and b respectively. If x was not renamed, and simply elaborated into $x_\mathbb{N}$, both a and b would be bound to $x_\mathbb{N}$, generating the following (incorrect) AST:

   $$\textbf{return } \text{Lam}(x_\mathbb{N}, \text{Lam}(x_\mathbb{N}, \text{Ret}(\text{Pair}(\text{Var}(x_\mathbb{N}), \text{Var}(x_\mathbb{N})))))$$

   Thus, `mkfun` should be elaborated into a function that generates *fresh* names for x each time it is called. This is the purpose of **mkvar**.

Second, $\lambda_{\text{AST(op)}}$ extends λ_{op} with machinery for scope extrusion checking. This machinery comprises:

Syntax

$\lambda_{\mathsf{AST(op)}}$

Formal Parameters	α_R		
Normal Forms	n	::=	the natural lifting of λ_{op} values
			$\mid \mathsf{Nat}(m) \mid \alpha_R \mid \mathsf{Var}(\alpha_R) \mid \mathsf{Lam}(n_1, n_2)$
			$\mid \mathsf{App}(n_1, n_2) \mid \mathsf{Continue}(n_1, n_2) \mid \mathsf{Ret}(n)$
			$\mid \mathsf{Do}(n_1, n_2, n_3) \mid \mathsf{Op}(n) \mid \mathsf{Hwith}(n_1, n_2)$
			$\mid \mathsf{Hret}(n_1, n_2)(n_1, n_2) \mid \mathsf{Hop}(n_1, n_2, n_3, n_4)$
Terms	t	:=	the natural lifting of λ_{op} computations
			$\mid \mathbf{check}\, n \mid \mathbf{check}_M\, n \mid \mathbf{dlet}(n, t) \mid \mathbf{tls}(t) \mid \mathbf{err}$
Handlers	h	:=	the natural lifting of λ_{op} handlers

Figure 3.7.: $\lambda_{\mathsf{AST(op)}}$ syntax. The syntax extends λ_{op} with a (countably finite) class of (type-annotated) formal parameters, AST constructors and scope extrusion checking machinery.

1. **err**, an error state for indicating the presence of scope extrusion,

2. **check**, a guarded **return** that either detects scope extrusion, and transitions to **err**, or does not detect scope extrusion, and transitions to **return**,

3. **check**$_M$, which behaves similarly to **check**, but (as Section 4.3 explains) allows a set of *muted* variables M to *temporarily* extrude their scope,

4. **dlet**, a primitive for tracking which variables are well-scoped and which have extruded their scope,

5. **tls**, a marker representing an occurrence of a top-level splice in the source program.

Notice that, while the calculus provides the *machinery* for scope extrusion checking, it does not demand that one *use* it, or use it *properly*. Scope extrusion checking is not a language feature, but an algorithm one builds on top of the calculus.

3.2.1. Operational Semantics

The semantics of $\lambda_{\mathsf{AST(op)}}$ are made precise via an operational semantics. Many rules are identical to those of λ_{op} (Figure 2.2): interesting rules are collated in Figure 3.8. Rules are divided into those related to AST construction (Ast-Rule), and those related to **s**cope **e**xtrusion **c**hecking (Sec-Rule).

Configurations

Like λ_{op}, the operational semantics is defined over *configurations*. In $\lambda_{\mathsf{AST(op)}}$, configurations have the form:

$$\langle t; E; U; M; I \rangle$$

At a high level, t and E are terms and evaluation contexts respectively. U acts as a source of freshness for name generation. M is a set of muted variables, i.e. those that do not trigger a scope extrusion error, even if they have extruded their scope. I indicates the point at which variables in M should be *unmuted*, by setting M to $\emptyset$.

Operational Semantics
Selected Rules

$\lambda_{\mathsf{AST(op)}}$

Evaluation Contexts

$$F ::= \dots \mid \mathbf{dlet}(\alpha_R, [-]) \mid \mathbf{tls}([-])$$

Operational Semantics

(Ast-Sym)	$\langle \mathbf{mkvar}\ R; E; U; M; I \rangle$	$\rightarrow$	$\langle \mathbf{return}\ \alpha_R; E; U \cup \{\alpha\}; M; I \rangle$ (where $\alpha = \mathsf{next}(U),\ \mathsf{next}(U) \notin U,\ \mathsf{next}$ deterministic)
(Sec-Chs)	$\langle \mathbf{check}\ n; E; U; M; I \rangle$	$\rightarrow$	$\langle \mathbf{return}\ n; E; U; M; I \rangle$ (if $\mathsf{FV}^0(n) \subseteq \pi_{\mathsf{Var}}(E)$)
(Sec-Chf)	$\langle \mathbf{check}\ n; E; U; M; I \rangle$	$\rightarrow$	$\langle \mathbf{err}; E; U; M; I \rangle$ (if $\mathsf{FV}^0(n) \not\subseteq \pi_{\mathsf{Var}}(E)$)
(Sec-Cms)	$\langle \mathbf{check}_M\ n; E; U; M; I \rangle$	$\rightarrow$	$\langle \mathbf{return}\ n; E; U; M; I \rangle$ (if $\mathsf{FV}^0(n) \setminus M \subseteq \pi_{\mathsf{Var}}(E)$)
(Sec-Cmf)	$\langle \mathbf{check}_M\ n; E; U; M; I \rangle$	$\rightarrow$	$\langle \mathbf{err}; E; U; M; I \rangle$ (if $\mathsf{FV}^0(n) \setminus M \not\subseteq \pi_{\mathsf{Var}}(E)$)
(Sec-Tls)	$\langle \mathbf{tls}(\mathbf{return}\ n); E; U; M; I \rangle$	$\rightarrow$	$\langle \mathbf{return}\ n; E; U; \emptyset; \top \rangle$
(Sec-Dlt)	$\langle \mathbf{dlet}(\alpha_R, \mathbf{return}\ n); E; U; M; I \rangle$	$\rightarrow$	$\langle \mathbf{return}\ n; E; U; M'; I' \rangle$ (if $\mathsf{len}(E) > I$ then $M' = M, I' = I$ else $M' = \emptyset, I' = \top$)
(Eff-Op)	$\langle \mathbf{op}(v); E_1[\mathbf{handle}\ E_2\ \mathbf{with}\ \{h\}]; U; M; I \rangle$	$\rightarrow$	$\langle c[v/x, \mathsf{cont}/k]; E_1; U; M \cup \pi_{\mathsf{Var}}(E_2); I' \rangle$ (where $\mathsf{cont} = \kappa x.\ \mathbf{handle}\ E_2[\mathbf{return}\ x]\ \mathbf{with}\ \{h\}$ and $\mathbf{op}(x, k) \mapsto c \in h$ and $\mathbf{op} \notin \mathsf{handled}(E_2)$ and $I' = \mathsf{min}(\mathsf{len}(E_1), I)$)

Figure 3.8.: Selected rules of the $\lambda_{\mathsf{AST(op)}}$ operational semantics. Many of the rules can be trivially adapted from the λ_{op} semantics (Figure 2.2). The muting and unmuting of variables is complex, and explained in Section 4.3. For now, these mechanisms are **highlighted**.

AST Rule

The Ast-Gen rule describes the behaviour of **mkvar**: **mkvar** R produces a formal parameter of type R and some name α. Recall that names should be **fresh**: that is, multiple calls to **mkvar** should always return variables with different names. This involves remembering names that have been previously generated, which are collected in U. To ensure determinacy of the semantics, names are chosen *deterministically*.

Scope Extrusion Checking Rules

The **check** primitive acts like a guarded **return**, which can catch occurrences of scope extrusion. For some arbitrary normal form n of AST type, either:

1. All the free variables of n are properly scoped, so **check** n reduces to **return** n (Sec-Chs)

2. Some free variables of n are not properly scoped, so **check** n reduces to **err** (Sec-Chf)

What does it mean to be "properly scoped" (the side condition on SEC-CHS)? The answer is slightly subtle. Consider the following program

$$\textbf{do}\ \text{body} \leftarrow \textbf{check}\ n\ \textbf{in check}\ \mathsf{Lam}(\alpha_\mathbb{N}, \text{body})$$

Should $\mathsf{Var}(\alpha_\mathbb{N})$ occur in n, it should be "properly scoped": it should not cause a transition to **err**. However, it is hard to deduce this from the *static* structure of the program. Instead, one has to reason about the *dynamic* execution of the program. Rather than calculating what is properly scoped as a *language feature*, $\lambda_{\text{AST(op)}}$ defers it to the programmer. Following Kiselyov [17], the programmer must *declare* that a variable is properly scoped through use of the **dlet** keyword.

$$\textbf{dlet}(\alpha_\mathbb{N}, \textbf{do}\ \text{body} \leftarrow \textbf{check}\ n\ \textbf{in check}\ \mathsf{Lam}(\alpha_\mathbb{N}, \text{body}))$$

More precisely, **dlet** places a frame of the form $\textbf{dlet}(\alpha_R, [-])$ on the evaluation context E. The notation $\pi_{\mathsf{Var}}(E)$ filters out the variables declared in this manner from E. For example,

$$\pi_{\mathsf{Var}}(\textbf{dlet}(\alpha_R, \textbf{do}\ x \leftarrow [-]\ \textbf{in}\ t)) = \{\mathsf{Var}(\alpha_R)\}$$

Given a term $E[t]$, I say variable $\mathsf{Var}(\alpha_R)$ in t is "declared safe" if $\mathsf{Var}(\alpha_R) \in \pi_{\mathsf{Var}}(E)$ (Definition 3.2.1):

> **Definition 3.2.1 (Declared Safe)**
> *Given a term $E[t]$, $\mathsf{Var}(\alpha_R)$ in t is declared safe if $\mathsf{Var}(\alpha_R) \in \pi_{\mathsf{Var}}(E)$*

Given a term of the form **check** n in some evaluation context E, where n is an AST, **check** thus succeeds if and only if the free Vars of n, written $\mathsf{FV}^0(n)$, have all been declared safe, $\mathsf{FV}^0(n) \subseteq \pi_{\mathsf{Var}}(E)$.

It may seem lazy to define the semantics of **check** in such a way that places the burden onto the user. Recall, however, that $\lambda_{\text{AST(op)}}$ is *not* meant to be programmed in directly. Rather, it acts as an elaboration target for $\lambda_{\langle\langle\text{op}\rangle\rangle}$. Therefore, the onus is on the person defining the elaboration to justify that **dlet** and **check** are used appropriately.

$\textbf{check}_M$ is a variant of **check**. As Section 4.3 explains, to design an optimal scope extrusion check, it is helpful to *mute* some variables, pretending that they are properly scoped. $\textbf{check}_M$ behaves exactly like **check**, except that it pretends that the muted variables M are properly scoped ($\textbf{check}_M\ n$ succeeds if $\mathsf{FV}^0(n) \setminus M \subseteq \pi_{\mathsf{Var}}(E)$).

Similarly, when justifying the correctness of scope extrusion checks, it is useful to remember the position of top-level splices in the $\lambda_{\langle\langle\text{op}\rangle\rangle}$ source program. The **tls** marker is used to indicate the occurrence of a top-level splice in the source program. Beyond unmuting variables (Section 4.3), **tls** has no operational behaviour (SEC-TLS).

The final two rules, SEC-DLT and EFF-OP, mute or unmute Vars. Muting and unmuting are explained in Section 4.3. For now, the components of transitions corresponding to muting and unmuting are **highlighted**, and can be ignored.

Ignoring muting and unmuting, SEC-DLT silently removes a $\textbf{dlet}(\alpha_R, [-])$ frame

$$\langle \textbf{dlet}(\alpha_R, \textbf{return}\ n); E; U; M; I \rangle \rightarrow \langle \textbf{return}\ n; E; U; M'; I' \rangle$$

and EFF-OP behaves as it does in λ_{op} (Figure 2.2):

$$\langle \textbf{op}(v); E_1[\textbf{handle}\ E_2\ \textbf{with}\ \{h\}]; U; M; I \rangle \ \rightarrow\ \langle c[v/x, \text{cont}/k]; E_1; U; M \cup \pi_{\mathsf{Var}}(E_2); I' \rangle$$
$$(\text{cont} = \kappa x.\ \textbf{handle}\ E_2[\textbf{return}\ x]\ \textbf{with}\ \{h\},$$
$$\textbf{op}(x, k) \mapsto c \in h\ \text{and}\ \textbf{op} \notin \text{handled}(E_2))$$

Types
$\lambda_{\text{AST(op)}}$

Computation and Handler Types omitted

Run-time Pre-types

Effects Row $\quad\quad\quad \xi ::= \emptyset \mid \xi \cup \{\text{op}_i\}$

Value type $\quad\quad\quad Q, R ::= \mathbb{N}$
$\quad\quad\quad\quad\quad\quad\quad\quad\mid Q \xrightarrow{\xi} R \quad$ functions
$\quad\quad\quad\quad\quad\quad\quad\quad\mid Q \twoheadrightarrow^{\xi} R \quad$ continuations

Computation type $\quad R\,!\,\xi$
Handler type $\quad\quad\quad Q\,!\,\xi_1 \Longrightarrow R\,!\,\xi_2$

Types

Value type $\quad S, T ::= \ldots$
$\quad\quad\quad\quad\quad\quad\mid \mathsf{FParam}(R) \quad\quad\quad\quad$ formal parameter
$\quad\quad\quad\quad\quad\quad\mid \mathsf{AST}(R) \quad\quad\quad\quad\quad\;$ AST (value)
$\quad\quad\quad\quad\quad\quad\mid \mathsf{AST}(R\,!\,\xi) \quad\quad\quad\quad$ AST (computation)
$\quad\quad\quad\quad\quad\quad\mid \mathsf{AST}(Q\,!\,\xi_1 \Longrightarrow R\,!\,\xi_2) \quad$ AST (handler)

Figure 3.9.: The types of $\lambda_{\text{AST(op)}}$. $\lambda_{\text{AST(op)}}$ types extend λ_{op} types with an AST type (for ASTs), and an FParam type

3.2.2. Type System

$\lambda_{\text{AST(op)}}$ extends λ_{op} types with an FParam type and an AST type (Figure 3.9).

Typing Rules

The $\lambda_{\langle\langle\text{op}\rangle\rangle}$ typing rules are extremely straightforward: for example, α_R is an FParam of type R, and $\mathsf{Var}(\alpha_R)$ is an AST of type R. **mkvar** R is a computation that produces FParams of type R, and $\mathsf{Lam}(n_1, n_2)$ is well-typed if n_1 is an FParam and n_2 an AST.

Notice that this type system does not guarantee that the resulting AST is *well-scoped*, for example, the following is well-typed:

$$\cdot \vdash \mathsf{Var}(\alpha_R) : \mathsf{AST}(R)$$

The typing rules for scope extrusion checks are even more straightforward: they are effectively invisible to the type system. The only complex case is **err**, which can be assigned any type in any context. **err** thus behaves similarly to **absurd** in `Haskell`, or in the λ-calculus extended with the empty type [28].

A closed $\lambda_{\text{AST(op)}}$ term is well-typed if it can be typed with an empty effects row.

> **Definition 3.2.2 (Well-typed closed term)**
> *A closed term t is well-typed if $\cdot \vdash t : T\,!\,\emptyset$*

$\lambda_{\mathsf{AST(op)}}$

Typing Rules
Selected Rules

(BINDER)

$$\overline{\Gamma \vdash \alpha_R : \mathsf{FParam}(R)}$$

(VARIABLE)

$$\frac{\Gamma \vdash n : \mathsf{FParam}(R)}{\Gamma \vdash \mathsf{Var}(n) : \mathsf{AST}(R)}$$

(MKVAR)

$$\overline{\Gamma \vdash \mathbf{mkvar}\, R : \mathsf{FParam}(R)\,!\,\Delta}$$

(LAMBDA-AST)

$$\frac{\Gamma \vdash n_1 : \mathsf{FParam}(Q) \qquad \Gamma \vdash n_2 : \mathsf{AST}(R\,!\,\xi)}{\Gamma \vdash \mathsf{Lam}(n_1, n_2) : \mathsf{AST}(Q \xrightarrow{\xi} R)}$$

(ERR)

$$\overline{\Gamma \vdash \mathbf{err} : T\,!\,\Delta}$$

(TLS)

$$\frac{\Gamma \vdash t : T\,!\,\Delta}{\Gamma \vdash \mathbf{tls}(t) : T\,!\,\Delta}$$

(DLET)

$$\frac{\Gamma \vdash n : \mathsf{FParam}(R) \qquad \Gamma \vdash t : T\,!\,\Delta}{\Gamma \vdash \mathbf{dlet}(n, t) : T\,!\,\Delta}$$

(CHECK)

$$\frac{\Gamma \vdash n : T \qquad T = \mathsf{AST}(R) \vee \mathsf{AST}(R\,!\,\xi) \vee \mathsf{AST}(Q\,!\,\xi_1 \implies R\,!\,\xi_2)}{\Gamma \vdash \mathbf{check}\, n : T\,!\,\Delta}$$

Figure 3.10.: Selected $\lambda_{\mathsf{AST(op)}}$ typing rules

3.2.3. Implementation

The core calculus $\lambda_{\mathsf{AST(op)}}$ corresponds to a concrete `OCaml` implementation. In the concrete `OCaml` implementation, **check**, **dlet**, and **err** are not primitives. Rather, they are encoded as a *mode of use* of effects and handlers.

1. **check** n is implemented by performing a `FreeVar` effect, that are passed the free variables of n

   check$_M$ n is similar, except there are also `Mute` and `Unmute` effects

2. **dlet**(α_R, t) is implemented as a *handler* of the `FreeVar` effect, which subtracts $\mathsf{Var}(\alpha_R)$ from the set of free variables, and either:

   a) Resumes the continuation, if the set of free variables is now empty (all free variables declared safe)

   b) Performs another `FreeVar` effect, to check that the remaining free variables are declared safe. Following a successful such check, the continuation may be resumed.

3. **err** is an unhandled `FreeVar` effect

3.3. Elaboration from $\lambda_{\langle\langle op \rangle\rangle}$ to $\lambda_{\mathsf{AST(op)}}$

This section describes an elaboration from $\lambda_{\langle\langle op \rangle\rangle}$ to $\lambda_{\mathsf{AST(op)}}$. This elaboration is simple: it does not insert any dynamic scope extrusion checks (other elaborations in Chapter 4, that do insert checks, are built by extending this elaboration).

The elaboration is defined on typing judgements: $\lambda_{\langle\langle op \rangle\rangle}$ judgements elaborate to $\lambda_{\mathsf{AST}(op)}$ judgements. This decomposes into four elaborations: on effect rows, types, contexts, and terms. As the specific elaboration is clear from the context, I write $[\![-]\!]$ for all four.

3.3.1. Elaborating Effect Rows

Elaborating effect rows is just the identity, that is

$$\begin{aligned} [\![\Delta]\!] &= \Delta \\ [\![\xi]\!] &= \xi \end{aligned}$$

3.3.2. Elaborating Types

To define the elaboration of types, it is convenient to refer to a helper function, erase (Appendix A.1), that, given a level 0 type, *erases* all of the level annotations (and elaborates effect rows). For example:

$$\mathsf{erase}((S^0 \xrightarrow{\xi} T^0)^0) = S \xrightarrow{[\![\xi]\!]} T$$

In a nutshell, level 0 types elaborate into AST types, and level -1 types elaborate into themselves (sans level annotations), except for Code types, which elaborate into AST types ($[\![\mathsf{Code}(T^0\,!\,\Delta)^{-1}]\!] = [\![T^0\,!\,\Delta]\!]$).

$$\begin{aligned} [\![T^0]\!] &= \mathsf{AST}(\mathsf{erase}(T^0)) \\ [\![T^0\,!\,\xi]\!] &= \mathsf{AST}(\mathsf{erase}(T^0\,!\,\xi)) \\ [\![T^0\,!\,\Delta]\!] &= \mathsf{AST}(\mathsf{erase}(T^0))\,!\,[\![\Delta]\!] \\ [\![T^0\,!\,\Delta;\xi]\!] &= \mathsf{AST}(\mathsf{erase}(T^0\,!\,\xi))\,!\,[\![\Delta]\!] \\ [\![(S^0\,!\,\xi_1 \Longrightarrow T^0\,!\,\xi_2)^0]\!] &= \mathsf{AST}(\mathsf{erase}((S^0\,!\,\xi_1 \Longrightarrow T^0\,!\,\xi_2)^0)) \end{aligned}$$

$$\begin{aligned} [\![\mathbb{N}^{-1}]\!] &= \mathbb{N} \\ [\![(S^{-1} \xrightarrow{\Delta} T^{-1})^{-1}]\!] &= [\![S^{-1}]\!] \xrightarrow{[\![\Delta]\!]} [\![T^{-1}]\!] \\ [\![(S^{-1} \xrightarrow{\Delta} T^{-1})^{-1}]\!] &= [\![S^{-1}]\!] \xrightarrow{[\![\Delta]\!]} [\![T^{-1}]\!] \\ [\![\mathsf{Code}(T^0\,!\,\xi)^{-1}]\!] &= \mathsf{AST}(\mathsf{erase}(T^0\,!\,\xi)) \end{aligned}$$

$$[\![T^{-1}\,!\,\Delta]\!] = [\![T^{-1}]\!]\,!\,[\![\Delta]\!]$$

$$[\![(S^{-1}\,!\,\Delta_1 \Longrightarrow T^{-1}\,!\,\Delta_2)^{-1}]\!] = [\![S^{-1}]\!]\,!\,[\![\Delta_1]\!] \Longrightarrow [\![T^{-1}]\!]\,!\,[\![\Delta_2]\!]$$

3.3.3. Elaborating Contexts

Elaboration of contexts is subtle. Level 0 types in the context are elaborated into FParam, rather than AST types. Elaboration of contexts thus requires a separate elaboration for context entries, and cannot rely naïvely on the elaboration on types.

$$\begin{aligned} [\![\cdot]\!] &= \cdot \\ [\![\Gamma, x : T^0]\!] &= [\![\Gamma]\!], x : \mathsf{FParam}(\mathsf{erase}(T^0)) \\ [\![\Gamma, x : T^{-1}]\!] &= [\![\Gamma]\!], x : [\![T^{-1}]\!] \end{aligned}$$

To see why level 0 types are elaborated into FParam types, notice that the only cases where the context Γ is extended with a level 0 variable occur in **c** or **q**. These modes build ASTs, and thus x must be an FParam.

Term Elaboration

Selected Rules

$$
\begin{aligned}
[\![x]\!]_{\mathbf{c|q}} &= \mathsf{Var}(x) \\
[\![\lambda x : T^0.\, e]\!]_{\mathbf{c|q}} &= \mathbf{do}\ x \leftarrow \mathbf{mkvar}\ \mathsf{erase}(T^0)\ \mathbf{in}\ \mathbf{do}\ \mathrm{body} \leftarrow [\![e]\!]_{\mathbf{c|q}}\ \mathbf{in}\ \mathbf{return}\ \mathsf{Lam}(x, \mathrm{body}) \\[4pt]
[\![\$e]\!]_{\mathbf{c}} &= \mathbf{tls}([\![e]\!]_{\mathbf{s}}) \\
[\![\$e]\!]_{\mathbf{q}} &= [\![e]\!]_{\mathbf{s}} \\[4pt]
[\![x]\!]_{\mathbf{s}} &= x \\
[\![\lambda x : T^0.\, e]\!]_{\mathbf{s}} &= \lambda x.[\![e]\!]_{\mathbf{s}} \\
[\![\langle\langle e\rangle\rangle]\!]_{\mathbf{s}} &= [\![e]\!]_{\mathbf{q}}
\end{aligned}
$$

Figure 3.11.: Selected term elaboration rules from $\lambda_{\langle\langle op\rangle\rangle}$ to $\lambda_{\text{AST(op)}}$. Term elaboration is very similar to Calcagno et al. [6], adapted for compile-time generation with top-level splices, and modes rather than levels. Elaboration is moderated by the compiler mode. In **c** and **q**, elaboration builds ASTs. In **s**-mode, elaboration is effectively the identity.

3.3.4. Elaborating Terms

Elaboration of terms assumes that all formal parameters have been annotated with their types, for example:

$$\lambda x : \mathbb{N}^0.\, e$$

The elaboration for terms is moderated by the **mode**: **c**, **q**, or **s**. Selected rules are collated in Figure 3.11.

At a high level, in **c** and **q**-mode, one builds ASTs. To ensure formal parameters are appropriately renamed, the elaboration must use **mkvar**.

Take, for example, the elaboration of $\lambda x : \mathbb{N}^0.\ \mathbf{return}\ x$ in **c** or **q**, where $\mathsf{erase}(\mathbb{N}^0) = \mathbb{N}$:
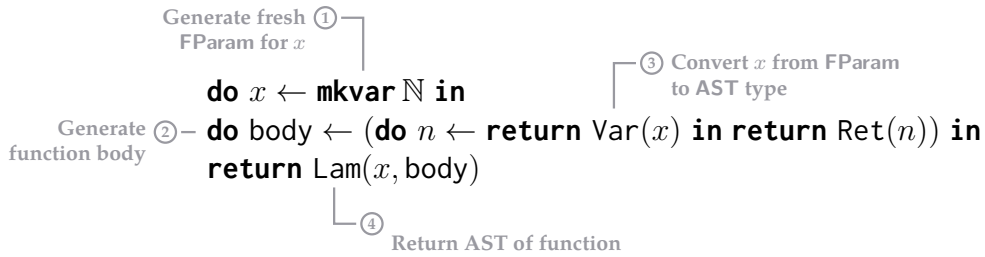
Elaboration in **c** and **q**-modes do not differ significantly, with the exception of the rule for splice, where in **c**-mode, **tls** is inserted, and in **q**-mode, it is not. The **c** and **q**-modes become important when building scope extrusion checks. Elaboration in **s**-mode is effectively the identity.

3.3.5. Elaborating Typing Judgements

Elaboration of typing judgements can now be defined compositionally. For example, take the typing judgement for lambdas in **c**-mode:

$$\frac{\Gamma, x : S \vdash_{\mathbf{c}} e : T \,!\, \Delta; \xi}{\Gamma \vdash_{\mathbf{c}} \lambda x.e : (S \xrightarrow{\xi} T) \,!\, \Delta}$$

which is elaborated by applying the elaboration component-wise:

$$\frac{[\![\Gamma, x : S]\!] \vdash [\![e]\!]_{\mathbf{c}} : [\![T \,!\, \Delta; \xi]\!]}{[\![\Gamma]\!] \vdash [\![\lambda x.e]\!]_{\mathbf{c}} : [\![(S \xrightarrow{\xi} T) \,!\, \Delta]\!]}$$

Letting $R = \mathsf{erase}(S)$, $Q = \mathsf{erase}(T)$, and $[\![e]\!]_{\mathbf{c}} = t$, and applying the elaboration functions defined above, we obtain Typing Derivation 3.1, which, assuming that the premise is valid typing derivation, corresponds to a valid $\lambda_{\mathsf{AST(op)}}$ typing derivation.

$$\frac{[\![\Gamma]\!], x : \mathsf{FParam}(Q) \vdash t : \mathsf{AST}(R \,!\, \xi) \,!\, \Delta}{[\![\Gamma]\!] \vdash \mathbf{do}\ x \leftarrow \mathbf{mkvar}\,\mathsf{erase}(T^0)\ \mathbf{in}\ \mathbf{do}\ \mathsf{body} \leftarrow t\ \mathbf{in}\ \mathbf{return}\ \mathsf{Lam}(x, \mathsf{body}) : \mathsf{AST}(Q \xrightarrow{\xi} R) \,!\, \Delta}$$

Typing Derivation 3.1.: The elaborated derivation of $\Gamma \vdash_{\mathbf{c}} \lambda x.e : S \xrightarrow{\xi} T$

Do $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ typing derivations always elaborate into $\lambda_{\mathsf{AST(op)}}$ typing derivations? Yes, but the question begets a larger point: what properties can be claimed about the calculus as defined? What metatheoretic results may be established?

3.4. Metatheory

This section states and proves several metatheoretic results about $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ and $\lambda_{\mathsf{AST(op)}}$.

First, well-typed $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ programs elaborate into well-typed $\lambda_{\mathsf{AST(op)}}$ programs:

> **Theorem 3.4.1 (Elaboration Preservation)**
> *If $\Gamma \vdash_\star e : \tau$ then $[\![\Gamma]\!] \vdash [\![e]\!]_\star : [\![\tau]\!]$, where $\star = \mathbf{\textcolor{teal}{c}} \mid \mathbf{\textcolor{magenta}{q}} \mid \mathbf{\textcolor{teal}{s}}$ and τ is a level 0 or level -1 value, computation, or handler type.*

The proof is by induction on the typing rules, e.g. Typing Derivation 3.1 in Section 3.3.5.

Additionally, the core language $\lambda_{\mathsf{AST(op)}}$ satisfies appropriate progress and preservation properties.

> **Theorem 3.4.2 (Progress)**
> *If $\cdot \vdash E[t] : T \,!\, \Delta$ then for all U, M, I either*
>
>   *1. t is of the form $\mathbf{return}\ n$ and $E = [-]$,*
>
>   *2. t is of the form $\mathbf{op}(v)$ for some $\mathsf{op} \in \Delta$, and $\mathsf{op} \notin \mathit{handled}(E)$*
>
>   *3. t is of the form $\mathbf{err}$*
>
>   *4. $\exists t', E', U', M', I'$ such that $\langle t; E; U; M; I \rangle \rightarrow \langle t'; E'; U'; M'; I' \rangle$*

Note the third clause, which may be used by the calculus to report scope extrusion.

The proof of progress by induction over the typing derivation. Since $\lambda_{\mathsf{AST(op)}}$ is built by extending λ_{op}, the proof need only consider the augmented typing rules, all of which are straightforward.

> **Theorem 3.4.3 (Reduction Preservation)**
> *If $\cdot \vdash E[t] : T \,!\, \Delta$ and $\langle t; E; U; M; I \rangle \to \langle t'; E'; U'; M'; I' \rangle$ then $\cdot \vdash E'[t'] : T \,!\, \Delta$*

The proof of reduction preservation proceeds by induction over the operational semantics. Once again, one need only consider the augmented rules, which are simple.

As a corollary, we obtain a notion of type safety.

> **Corollary 3.4.4 (Type Safety)**
> *If $\cdot \vdash_{\boldsymbol{c}} e : T^0 \,!\, \emptyset; \emptyset$ then either*
>
> *1. $\langle [\![e]\!]_{\boldsymbol{c}}; [-]; \emptyset; \emptyset; \top \rangle \to^{\omega}$,*
>
> *2. $\langle [\![e]\!]_{\boldsymbol{c}}; [-]; \emptyset; \emptyset; \top \rangle \to^{*} \langle \mathbf{err}; E; U; M; I \rangle$ for some E, U, M, I, or*
>
> *3. $\langle [\![e]\!]_{\boldsymbol{c}}; [-]; \emptyset; \emptyset; \top \rangle \to^{*} \langle \mathbf{return}\ n; [-]; U; M; I \rangle$ for some U, M, I*
>
> *where the initial configuration comprises an elaborated term, the empty evaluation context, an empty set indicating that no variables have been previously generated, another empty set indicating no variables have been muted, and $\top$, indicating that there is (currently) no plan to unmute variables.*

Importantly, this notion of type safety is weak. A semantics which always reports a scope extrusion error ($\mathbf{err}$) would be type safe under this definition. Further, a semantics which never reports scope extrusion would be type safe as well. Due to the potential presence of scope extrusion, the third case of Corollary 3.4.4 cannot additionally claim that the normal form n represents a well-typed λ_{op} program.

Finally, underneath a top-level splice, quotation and splice are duals (Theorem 3.4.5)

> **Theorem 3.4.5 (Quote-Splice Duality)**
> *Under a top-level splice, quotation and splice are duals*
>
> $$\begin{aligned} \$\langle\langle e \rangle\rangle &=_{\boldsymbol{q}} & e \\ \langle\langle \$e \rangle\rangle &=_{\boldsymbol{s}} & e \end{aligned}$$

Where $=_{\star}$ means "elaborates to contextually equivalent $\lambda_{\mathsf{AST(op)}}$ programs in $\star$ mode". Parameterising by the mode is necessary, since the mode affects the result of elaboration. It is possible to prove something stronger: they elaborate to the same $\lambda_{\mathsf{AST(op)}}$ program (contextual equivalence follows from reflexivity). The proof of quote-splice duality is by inspection of the definition of elaboration, where:

$$\begin{aligned} [\![\$\langle\langle e \rangle\rangle]\!]_{\boldsymbol{q}} = t &\iff [\![e]\!]_{\boldsymbol{q}} = t \\ [\![\langle\langle \$e \rangle\rangle]\!]_{\boldsymbol{s}} = t &\iff [\![e]\!]_{\boldsymbol{s}} = t \end{aligned}$$

4. Scope Extrusion

This chapter uses $\lambda_{\langle\langle op \rangle\rangle}$ to formulate precise definitions of scope extrusion, and additionally evaluates four scope extrusion checks:

1. The lazy dynamic check, first described by Kiselyov [16] (Section 4.1).

2. The eager dynamic check, which to the best of my knowledge is a faithful description of the current MetaOCaml check (Section 4.2).

3. A novel best-effort dynamic check, which I argue occupies a goldilocks zone between expressiveness and efficiency (Section 4.3).

4. Refined environment classifiers, a static approach first described by Kiselyov et al. [19] (Section 4.4).

The three dynamic checks have been implemented in MacoCaml. The implementations closely mirror the descriptions in this chapter, and were useful for building an understanding of the correctness and expressiveness of the various checks.

Section 4.5 evaluates $\lambda_{\langle\langle op \rangle\rangle}$'s ability to facilitate comparative evaluation of different scope extrusion checks.

4.1. Lazy Dynamic Check

Recall that one definition of scope extrusion relates to the *result* of compile-time execution (Section 2.3.1, Page 21) [16].

I call this lazy scope extrusion, and define it as a property on $\lambda_{\mathsf{AST}(op)}$ configurations as follows:

> **Definition 4.1.1 (Lazy Scope Extrusion)**
> *A $\lambda_{\mathsf{AST}(op)}$ configuration of the form*
>
> $$\langle t; E; U; M; I \rangle$$
>
> *exhibits lazy scope extrusion if all of the following hold:*
>
> *1. $t = \textbf{return }n$ for some n of AST type*
>
> *2. $E = E'[\textbf{tls}([-])]$ for some E'*
>
> *3. $FV^0(n) \not\subseteq \pi_{\mathsf{Var}}(E)$*

The second condition implies that n is spliced into a larger, ambient and inert, program.

The lazy dynamic check is defined as a modified term elaboration $\llbracket - \rrbracket^{\textbf{Lazy}}$. Two modifications are made to the term elaboration described in Section 3.3. First, **check**s are performed after top-level splices:

$$\llbracket \$e \rrbracket_{\textbf{c}}^{\textbf{Lazy}} \triangleq \textbf{check}\,(\textbf{tls}(\llbracket e \rrbracket_{\textbf{s}}^{\textbf{Lazy}}))$$

Second, **dlet**s are inserted to ensure variables bound outside top-level splices are declared safe (Definition 3.2.1), and thus do not cause the **check** to fail. For example, in $\lambda x : \mathbb{N}. \$\langle\langle \lambda y : \mathbb{N}. \ x + y \rangle\rangle$, x is a binder in **c**-mode while y is a binder in **q**-mode. x should be declared safe (a free x should not cause the **check** to transition to **err**), but y should not. Thus, elaboration of binders in **c**-mode (but not **q**-mode) should insert **dlet**s:

$$\llbracket \lambda x : T^0. e \rrbracket_{\textbf{c}}^{\textbf{Lazy}} = \textbf{do}\ x \leftarrow \texttt{mkvar}\,\mathrm{erase}(T^0)\ \textbf{in}\ \textbf{dlet}(x, \textbf{do}\ \mathrm{body} \leftarrow \llbracket e \rrbracket_{\textbf{c}}^{\textbf{Lazy}}\ \textbf{in}\ \textbf{return}\ \mathsf{Lam}(x, \mathrm{body}))$$

For example, $\lambda x : \mathbb{N}. \$\langle\langle \lambda y : \mathbb{N}. \ x + y \rangle\rangle$ elaborates into (changes from the elaboration in Section 3.3 highlighted in **blue**):

$$
\begin{aligned}
&\textbf{do}\ x \leftarrow \texttt{mkvar}\,\mathbb{N}\ \textbf{in}\\
&\textbf{dlet}(x, \textbf{do}\ \mathrm{body}_1 \leftarrow \textbf{check}(\textbf{tls}(\textbf{do}\ y \leftarrow \texttt{mkvar}\,\mathbb{N}\ \textbf{in}\\
&\qquad\qquad\qquad\qquad\qquad\qquad\quad \textbf{do}\ \mathrm{body}_2 \leftarrow (\textbf{do}\ a \leftarrow \mathsf{Var}(x)\ \textbf{in}\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \textbf{do}\ b \leftarrow \mathsf{Var}(y)\ \textbf{in}\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \textbf{return}\ \mathsf{Plus}(a, b))\\
&\qquad\qquad\qquad\qquad\qquad\qquad\quad \textbf{return}\ \mathsf{Lam}(y, \mathrm{body}_2)))\\
&\textbf{return}\ \mathsf{Lam}(x, \mathrm{body}_1))
\end{aligned}
$$

Due to the simplicity of the algorithm, verifying the correctness and expressiveness of the check is trivial: the check reports scope extrusion if, and only if, the program exhibits lazy scope extrusion.

> **Theorem 4.1.2 (Correctness and Expressiveness of the Lazy Dynamic Check)**
> *Assuming* $\cdot \vdash_{\textbf{c}} e : T^0 \,!\, \emptyset; \emptyset$, *and* $\llbracket e \rrbracket_{\textbf{c}}^{\textit{Lazy}} = t$,
>
> $$\langle t; [-]; \emptyset; \emptyset; \top \rangle \rightarrow^* \langle \textbf{err}; E; U; M; I \rangle$$
> $$\Longleftrightarrow$$
> *For some* E', $\langle t; [-]; \emptyset; \emptyset; \top \rangle \rightarrow^* \langle \textbf{return}\ n; E'; U; M; I \rangle$, *and*
> $\langle \textbf{return}\ n; E'; U; M; I \rangle$ *exhibits lazy scope extrusion*

However, due again to its simplicity, the lazy dynamic check is inefficient and uninformative, and therefore not suitable for practical use [16] (Section 2.3.1, Page 21).

4.2. Eager Dynamic Check

Another definition of scope extrusion relates to *intermediate results* during compile-time execution (Section 2.3.1, Page 22). For example, Kiselyov [16] defines scope extrusion as (emphasis mine):

> *At **any point during the evaluation**, an occurrence of an open-code value with a free variable whose name is not dynamically bound.*

I call this eager scope extrusion, and define it as a property on $\lambda_{\textsf{AST(op)}}$ configurations as follows:

> **Definition 4.2.1 (Eager Scope Extrusion)**
> *A* $\lambda_{\mathsf{AST(op)}}$ *configuration of the form*
>
> $$\langle t; E; U; M; I \rangle$$
>
> *exhibits eager scope extrusion if all of the following hold:*
>
> 1. $t = \textbf{return}\ n$ *for some* n *of AST type*
>
> 2. $FV^0(n) \not\subseteq \pi_{\mathsf{Var}}(E)$

Notice that lazy scope extrusion is a special case of eager scope extrusion, where $E = E'[\textbf{tls}([-])]$.

It is possible to define an eager dynamic check by extending the lazy dynamic check. In addition to the top-level splice check, and the **c**-mode **dlet**s, the eager dynamic check adds **check**s for ASTs constructed in **q**-mode, for example

$$[\![v_1 v_2]\!]^{\textbf{Eager}}_{\textbf{q}} = \textbf{do}\ f \leftarrow [\![v_1]\!]^{\textbf{Eager}}_{\textbf{q}}\ \textbf{in do}\ a \leftarrow [\![v_2]\!]^{\textbf{Eager}}_{\textbf{q}}\ \textbf{in check}\ \mathsf{App}(f, a)$$

notice how **return** $\mathsf{App}(f, a)$ is replaced by **check** $\mathsf{App}(f, a)$.

Consequently, to prevent false positives, variables bound in **q**-mode must also be declared safe via **dlet**:

$$[\![\lambda x : T^0.\ e]\!]^{\textbf{Eager}}_{\textbf{q}} = \textbf{do}\ x \leftarrow \textbf{mkvar}\ \mathsf{erase}(T^0)\ \textbf{in check}\ (\textbf{dlet}(x, \textbf{do}\ \mathsf{body} \leftarrow [\![e]\!]^{\textbf{Eager}}_{\textbf{q}}\ \textbf{in return}\ \mathsf{Lam}(x, \mathsf{body})))$$

The elaboration of $\lambda x : \mathbb{N}.\ \$\langle\langle \lambda y : \mathbb{N}.\ x + y\rangle\rangle$ thus changes to (changes from the lazy dynamic check highlighted in **blue**):

$$
\begin{aligned}
&\textbf{do}\ x \leftarrow \textbf{mkvar}\ \mathbb{N}\ \textbf{in} \\
&\textbf{dlet}(x, \textbf{do}\ \mathsf{body}_1 \leftarrow \textbf{check}(\textbf{tls}(\textbf{do}\ y \leftarrow \textbf{mkvar}\ \mathbb{N}\ \textbf{in check}(\textbf{dlet}(y, \\
&\qquad\qquad\qquad\qquad\qquad\qquad \textbf{do}\ \mathsf{body}_2 \leftarrow (\textbf{do}\ a \leftarrow \mathsf{Var}(x)\ \textbf{in} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \textbf{do}\ b \leftarrow \mathsf{Var}(y)\ \textbf{in} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \textbf{check}\ \mathsf{Plus}(a, b)) \\
&\qquad\qquad\qquad\qquad\qquad\qquad \textbf{return}\ \mathsf{Lam}(y, \mathsf{body}_2))))) \\
&\textbf{return}\ \mathsf{Lam}(x, \mathsf{body}_1))
\end{aligned}
$$

If **dlet**s were not inserted for binders in **q**-mode (e.g. y), then **check** $\mathsf{Plus}(a, b)$ would fail, as y would not be declared safe.

Intuitively, the eager dynamic check performs a check whenever an AST is built. Hence, assume that evaluation reduces to a configuration that exhibits eager scope extrusion. Let the offending AST be n. The error will be detected and reported the next time n is used to build a bigger AST n' in an unsafe way (not all free variables in n' are declared safe).

$$
\begin{aligned}
&\$(\textbf{do}\ z \leftarrow (\textbf{handle}\ \langle\langle\ \lambda x.\ \$(\ \textbf{extrude}(\langle\langle x\rangle\rangle)\ )\ \rangle\rangle \\
&\qquad\qquad \textbf{with}\ \{\textbf{return}(u) \mapsto \langle\langle 0\rangle\rangle; \textbf{extrude}(y, k) \mapsto \textbf{return}\ y\}) \\
&\quad \textbf{in}\ \langle\langle \$z + 1\rangle\rangle)
\end{aligned}
$$

$\lambda_{\langle\langle\textbf{op}\rangle\rangle}$

Listing 11: Illustrating the eager dynamic check: eager scope extrusion is caused by the **return** y expression. Scope extrusion is not immediately detected. Rather, y is bound to z. Scope extrusion is reported when z is used to build a larger AST $\langle\langle \$z + 1\rangle\rangle$, where y is not declared safe

As an example, consider Listing 11. Eager scope extrusion is caused by the **return** y program fragment, where y refers to the unbound variable $\mathsf{Var}(x_\mathbb{N})$[1]. Eager scope extrusion is not caught immediately. Rather, y is bound to z, and scope extrusion is caught when z is used to build a larger AST, $\langle\langle \$z + 1 \rangle\rangle$, where y is not declared safe.

The eager dynamic check also checks at top-level splices, like the lazy dynamic check. Conceptually, a top-level splice builds a larger, ambient and inert, AST (Listing 12):

```
do z ← $(handle ⟨⟨ λx. $( extrude(⟨⟨⟨x⟩⟩⟩) )⟩⟩
        with {return(u) ↦ ⟨⟨0⟩⟩; extrude(y, k) ↦ return y})
in z + 1
```
$\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$

Listing 12: The eager dynamic check additionally checks at top-level splices.

To the best of my knowledge, the eager dynamic check is a faithful model of the MetaOCaml check, as described by Kiselyov [18]. The description was verified by executing translations of Listings 11, 12, 14 and 15 in BER MetaOCaml N153 (Appendix B.1).

4.2.1. Correctness of the Eager Dynamic Check

The eager dynamic check is incorrect: not every case of eager scope extrusion is reported (by transitioning to **err**). Evaluation may result in eager scope extrusion, but the offending AST n may never be used in an unsafe way. Thus, the eager dynamic check will not report that scope extrusion occurred.

For example, recall that $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ permits non-terminating programs. Consider the $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ program in Listing 13, where Ω is some non-terminating program that never refers to z. After translation, the program will reduce to a configuration that exhibits eager scope extrusion (**return** y). However, the program will immediately enter into a non-terminating loop, and scope extrusion will never be reported.

```
$(do z ← (handle ⟨⟨ λx. $( extrude(⟨⟨⟨x⟩⟩⟩) )⟩⟩
         with {return(u) ↦ ⟨⟨0⟩⟩; extrude(y, k) ↦ return y})
  in Ω)
```
$\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$

Listing 13: The eager dynamic check does not report all occurrences of eager scope extrusion. The program causes eager scope extrusion (**return** y), and then enters into a non-terminating loop which never refers to z.

Non-termination is not the only source of this behaviour. For example, the offending AST could be discarded (Listing 14), and therefore, never trigger the check.

```
$(handle ⟨⟨ λx. $( extrude(⟨⟨⟨x⟩⟩⟩) )⟩⟩
  with {return(u) ↦ ⟨⟨0⟩⟩; extrude(y, k) ↦ do w ← return y in ⟨⟨0⟩⟩})
```
$\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$

Listing 14: The eager dynamic check additionally will not report eager scope extrusion in the case where the offending AST is discarded.

---

[1]Technically, the variable should be renamed. For clarity, I do not rename the variables in this example

Finally, in the most interesting example, the program may recover from scope extrusion by *resuming* a continuation. As shown in Listing 15, by resuming the continuation, the program only uses the AST $\mathsf{Var}(x_\mathbb{N})$ in an *safe* way. By resuming the continuation, the program restores the captured evaluation context, thus declaring $\mathsf{Var}(x_\mathbb{N})$ safe. Only then is $\mathsf{Var}(x_\mathbb{N})$ used to build an AST, so the checks will pass.

```
$(handle ⟨⟨ λx. return $( extrude(⟨⟨x⟩⟩) ) ⟩⟩
  with {return(u) ↦ return u; extrude(y, k) ↦ continue k y})
```
$\lambda_{\langle\langle op\rangle\rangle}$

Listing 15: The eager dynamic check will additionally not report cases where the offending AST is used, but only in safe ways. In this case, the continuation restores the context that permits $\mathsf{Var}(x_\mathbb{N})$ to be used.

Kiselyov [16] acknowledges the incorrectness of the eager dynamic check, but argues that it makes the check more permissive. Permissiveness increases expressiveness, and is therefore desirable: a *feature*, not a *bug*.

4.2.2. Expressiveness of the Eager Dynamic Check

The expressiveness of the eager dynamic check, however, is not without issues. First, the eager dynamic check reports false positives (Listing 16), and is thus less expressive than the lazy dynamic check.

```
$(handle ⟨⟨ λx. $( extrude(⟨⟨x⟩⟩) ) ⟩⟩
  with {return(u) ↦ return u; extrude(y, k) ↦ continue k ⟨⟨$y + 0⟩⟩})
```
$\lambda_{\langle\langle op\rangle\rangle}$

Listing 16: A program which will fail the eager dynamic check. The offending AST ($\mathsf{Var}(x_\mathbb{N})$) is used to construct a larger AST in a way that appears to be unsafe $\langle\langle \$y + 0\rangle\rangle$, but is actually not, since the unsafe AST is then only used in a safe way.

In Listing 16, the offending AST ($\mathsf{Var}(x_\mathbb{N})$, bound to y) is used in a context where $\mathsf{Var}(x_\mathbb{N})$ is not declared safe ($\langle\langle \$y + 0\rangle\rangle$), and thus the eager dynamic check will report an error. However, if evaluation had been allowed to proceed, the evaluation context binding $\mathsf{Var}(x_\mathbb{N})$ (and additionally declaring it safe) would have been restored (**continue** $k\,w$), and all variables would have been properly scoped. The program *recovers* from a state of eager scope extrusion, and will not exhibit lazy scope extrusion. The eager dynamic check is thus not as expressive as the lazy dynamic check.

More concerningly, the eager dynamic check is unpredictable: it is difficult to explain, without appealing to the operational semantics, why the check disallows some programs, but allows others. Compare the program in Listing 15, which passes the check, and Listing 16, which *fails* the check. It is clear that the following inequation holds:

$$\langle\langle \$e\rangle\rangle \neq_\mathsf{s} \langle\langle \$e + 0\rangle\rangle$$

More generally, for program fragments P and P':

$$P[e] =_\mathsf{s} P'[e] \;\not\Longrightarrow\; \langle\langle P[\$\langle\langle e\rangle\rangle]\rangle\rangle =_\mathsf{s} \langle\langle P'[\$\langle\langle e\rangle\rangle]\rangle\rangle$$

One has to appeal to the operational behaviour of the eager dynamic check to explain why these equations do not hold. In my opinion, this exposes too much of the internal operation of the check to the user.

One possible attempt to make the eager dynamic check more predictable is to change the **s**-mode elaboration of **return**, such that each **return** elaborates into a **check**:

$$\llbracket \textbf{return } v \rrbracket_\textbf{s} = \textbf{check } \llbracket v \rrbracket_\textbf{s}$$

While this restores certain equations (for example, Listing 14 will now report a scope extrusion error), it will break others. For example, the following equation no longer holds:

$$\textbf{do }\_ \leftarrow \textbf{return } v \textbf{ in } e =_\textbf{s} e$$

since the **return** is elaborated into a **check**, which v may fail.

4.2.3. Efficiency of the Eager Dynamic Check

Additionally, the eager dynamic check is not, in the worst case, more efficient than the lazy dynamic check, since there exist pathological examples (Listing 12). Further, the overhead of the checks cannot be bound: multi-shot continuations may be replayed an unbounded number of times. Multi-shot continuations may capture checks. Thus, the overhead of checking is unbounded. However, I conjecture that in the *common case*, the eager dynamic check detects scope extrusion sufficiently early as to outweigh the checking overhead. This argument is an empirical one, and would require further research, outside the scope of the dissertation, to support.

4.3. Best-Effort Dynamic Check

The lazy dynamic check is too inefficient, and the eager dynamic check too unpredictable. Might it be possible to find a "goldilocks" solution? Such a check should allow the program in Listing 16, and be permissive in a predictable way. For example, a check that eagerly detects programs that *must* cause lazy scope extrusion. I call this best-effort scope extrusion.

> **Definition 4.3.1 (Best-Effort Scope Extrusion)**
> *A* $\lambda_{\mathsf{AST(op)}}$ *configuration of the form*
>
> $$\langle t; E; U; M; I \rangle$$
>
> *exhibits best-effort scope extrusion if there exists some* $i \in \mathbb{N}$ *such that*
>
> $$\langle t; E; U; M; I \rangle \rightarrow^i \langle t'; E'; U'; M'; I' \rangle$$
>
> *and* $\langle t'; E'; U'; M'; I' \rangle$ *exhibits lazy scope extrusion.*

This section describes a best-effort dynamic check that approximates best-effort scope extrusion, with occasional false positives.

The best-effort dynamic check is simple: change all **check**s to **check**$_M$s. For example,

$$\llbracket \lambda x : T^0. e \rrbracket_\textbf{q}^{\textbf{BE}} = \textbf{do } x \leftarrow \mathsf{mkvar}\, \mathsf{erase}(T^0) \textbf{ in check}_M\, (\textbf{dlet}(x, \textbf{do } \mathsf{body} \leftarrow \llbracket e \rrbracket_\textbf{q}^{\textbf{BE}} \textbf{ in return } \mathsf{Lam}(x, \mathsf{body})))$$

4. Scope Extrusion

The $\lambda x : \mathbb{N}.\ \$\langle\langle \lambda y : \mathbb{N}.\ x + y \rangle\rangle$ program elaborates into (changes from the eager dynamic check highlighted in **blue**):

> **do** $x \leftarrow$ **mkvar** $\mathbb{N}$ **in**
> **dlet**$(x, $**do** $\text{body}_1 \leftarrow$ **check**$_M($**tls**$($**do** $y \leftarrow$ **mkvar** $\mathbb{N}$ **in check**$_M($**dlet**$(y,$
> **do** $\text{body}_2 \leftarrow ($**do** $a \leftarrow$ Var(x) **in**
> **do** $b \leftarrow$ Var(y) **in**
> **check**$_M$ Plus$(a, b))$
> **return** Lam$(y, \text{body}_2)))))$
> **return** Lam$(x, \text{body}_1))$

To understand the best-effort dynamic check, consider the program in Listing 16, which is elaborated into $\lambda_{\mathsf{AST(op)}}$[2]. The failing check is underlined.

> ```
> handle
>    do x ← mkvar ℕ in
>    check(dlet(x, do body ← (do a ← Var(x) in extrude(a)) in
>                 return Lam(x, body))
> with
>    {return(u) ↦ return u;
>     extrude(y, k) ↦ do w ← check Plus(y, Nat(0)) in continue k w}
> ```

However, w is only used in a context where Var$(x_\mathbb{N})$ is declared safe

check fails, transitioning to **err**, since y is bound to Var$(x_\mathbb{N})$, which is not declared via **dlet**

The check fails because when an effect is performed, the variable Var$(x_\mathbb{N})$ is no longer declared safe. Since y is bound to Var$(x_\mathbb{N})$, checking the AST Plus$(y, \text{Nat}(0))$ reports an error. The problem is that the continuation k can be used to bind Var$(x_\mathbb{N})$. It is not clear, when the Plus AST is constructed and checked, that eager scope extrusion *must* lead to lazy scope extrusion.

To make the check more expressive, therefore, it may be useful to temporarily allow Var$(x_\mathbb{N})$ to extrude its scope, delaying error reporting until one knows for certain that one must have lazy scope extrusion.

The **check**$_M$ primitive allows Var$(x_\mathbb{N})$ to temporarily extrude its scope. **check**$_M$ checks for scope extrusion, but turns a blind eye to some set of muted variables M. It thus suffices to mute Var$(x_\mathbb{N})$, adding to M. The $\lambda_{\mathsf{AST(op)}}$ operational semantics mutes and unmutes variables, like Var$(x_\mathbb{N})$, at key points.

When effects are performed, the variables which are no longer declared safe (like Var$(x_\mathbb{N})$) are added to the set of muted variables (EFF-OP, Figure 3.8, Page 38):

$$\langle \mathbf{op}(v); E_1[\mathbf{handle}\ E_2\ \mathbf{with}\ \{h\}]; U; M; I \rangle \rightarrow \langle c[v/x, \text{cont}/k]; E_1; U; M \cup \pi_{\mathsf{Var}}(E_2); I' \rangle$$

As an example, consider the reduction of:

> ```
> handle
>    dlet(x_ℕ, do body ← extrude(Var(x_ℕ)) in Lam(x_ℕ, body))
> with
>    {return(u) ↦ return u;
>     extrude(y, k) ↦ do w ← check_M Plus(y, Nat(0)) in continue k w}
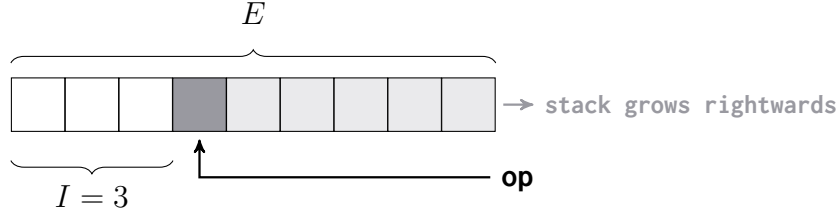> ```

---

[2]The program has been somewhat simplified

Figure 4.1.: An illustration of when variables are unmuted. The stack, E, grows rightwards. Effects are caught by handlers (**dark grey**). This captures a portion of the stack (light grey). We track the length of the stack, in **white**, that are never captured by an operation in this fashion. Frames in **white** will never be able to resume a continuation.

which is a simplified version of Listing 16 (elaborated into $\lambda_{\text{AST(op)}}$). Note additionally that the **check** has been replaced with a **check**$_M$. The first reduction step performs the operation, and the configuration steps to

$$\textbf{do } w \leftarrow \textbf{check}_M \, \text{Plus}(\text{Var}(x_\mathbb{N}), \text{Nat}(\textrm{0})) \textbf{ in continue } k \, w$$

Since the **dlet**$(x_\mathbb{N}, [-])$ frame is no longer on the stack, **check** $\text{Plus}(\text{Var}(x_\mathbb{N}), \text{Nat}(\textrm{0}))$ would throw an error. However, performing the **extrude** operation additionally *mutes* $\text{Var}(x_\mathbb{N})$, and hence **check**$_M$ $\text{Plus}(\text{Var}(x_\mathbb{N}), \text{Nat}(\textrm{0}))$ would not throw an error.

When should a variable like $\text{Var}(x_\mathbb{N})$ be *unmuted*? When there **cannot be** any way to resume a continuation k that could bind $\text{Var}(x_\mathbb{N})$. A safe approximation is the point where there cannot be *any* bound continuations k. This point is identified by tracking the maximal length I of the stack E that was never captured by the handling of an effect (Figure 4.1).

As an example, consider the following program, which builds the AST of the constant 1 function, $\lambda z. \, (\lambda x. \, x + \textrm{0})(\textrm{1})$:

$$\textbf{check}_M(\textbf{dlet}(z_\mathbb{N}, \textbf{do } b \leftarrow$$
$$(\textbf{do } f \leftarrow \textbf{handle}$$
$$\textbf{dlet}(x_\mathbb{N}, \textbf{do } \text{body} \leftarrow \textbf{extrude}(\text{Var}(x_\mathbb{N})) \textbf{ in } \text{Lam}(x_\mathbb{N}, \text{body}))$$
$$\textbf{with}$$
$$\{\textbf{return}(u) \mapsto \textbf{return } u;$$
$$\textbf{extrude}(y, k) \mapsto \textbf{do } w \leftarrow \textbf{check}_M \, \text{Plus}(y, \text{Nat}(\textrm{0})) \textbf{ in continue } k \, w\}$$
$$\textbf{in do } a \leftarrow \textbf{return } \text{Nat}(\textrm{1})$$
$$\textbf{in check}_M \, \text{App}(f, a))$$
$$\textbf{in return } \text{Lam}(\text{Var}(z_\mathbb{N}), b)))$$

Note that the body of f, coloured in grey, is the simplified version of Listing 16. The **extrude** operation is caught by the handler (also in grey), and the surrounding context (in **black**) is never captured by the handling of any effect. This surrounding context, which must have no references to the captured continuation k, is identified by I.

If the stack was never captured by the handling of an effect (for example, no operations were performed), then I is set to $\top$, $\forall n \in \mathbb{N}, \top \geq n$. Performing an effect can thus *decrease* I, but never increase it. This is the side condition on EFF-OP.

$$\langle \textbf{op}(v); E_1[\textbf{handle } E_2 \textbf{ with } \{h\}]; U; M; I \rangle \rightarrow \quad \langle c[v/x, \text{cont}/k]; E_1; U; M \cup \pi_{\text{Var}}(E_2); I' \rangle$$
$$(I' = \text{min}(\text{len}(E_1), I))$$

4. Scope Extrusion

During reduction, when the length of the stack is less than, or equals to, I, there must not be any remaining references to any continuations k, and thus I may be reset to $\top$, and all muted variables may be unmuted. In the previous example, the program eventually reduces to

$$
\begin{aligned}
&\mathbf{check}_M(\mathbf{dlet}(z_{\mathbb{N}}, \mathbf{do}\ b \leftarrow \\
&\quad (\mathbf{do}\ f \leftarrow \boxed{[}\ \mathbf{return}\ \mathtt{Lam}(x_{\mathbb{N}}, \mathtt{Plus}(\mathtt{Var}(x_{\mathbb{N}}), \mathtt{Nat}(0)))\ \boxed{]} \\
&\quad \mathbf{in}\ \mathbf{do}\ a \leftarrow \mathbf{return}\ \mathtt{Nat}(1) \\
&\quad \mathbf{in}\ \mathbf{check}_M\ \mathtt{App}(f, a)) \\
&\quad \mathbf{in}\ \mathbf{return}\ \mathtt{Lam}(\mathtt{Var}(z_{\mathbb{N}}), b)))
\end{aligned}
$$

Where $\boxed{[} - \boxed{]}$ separates the evaluation context (outside) and the term (inside). At this point, since the length of the stack is less than or equals to I, it is safe to unmute all muted variables. When there are no muted variables, $\mathbf{check}_M$ and $\mathbf{check}$ have the same behaviour.

However, altering the semantics in such a manner means that any transition could potentially have a side effect: unmuting variables. To keep the semantics standard, and to more closely model the implementation of the check, I associate the act of unmuting with $\mathbf{dlet}$ and $\mathbf{tls}$. A transition from $\mathbf{dlet}$ conditionally unmutes variables:

$$
\begin{aligned}
\langle \mathbf{dlet}(\alpha_R, \mathbf{return}\ n); E; U; M; I \rangle &\to \langle \mathbf{return}\ n; E; U; \emptyset; \top \rangle \quad \text{if } \mathrm{len}(E) \leq I \\
\langle \mathbf{dlet}(\alpha_R, \mathbf{return}\ n); E; U; M; I \rangle &\to \langle \mathbf{return}\ n; E; U; M; I \rangle \quad \text{if } \mathrm{len}(E) > I
\end{aligned}
$$

In the previous example, the transition from $\mathbf{dlet}(z_{\mathbb{N}}, \mathbf{return}\ n)$ unmutes variables. Therefore, $\mathtt{Var}(x_{\mathbb{N}})$ is still muted when the App constructor is checked, but unmuted when we check the constructor of the outer lambda. This is the side-effect/side-condition in the Sec-Dlt rule (Figure 3.8).

Additionally, transitions from $\mathbf{tls}$ *unconditionally* unmute variables, since the evaluation context beyond $\mathbf{tls}$ must be inert, and thus can never be captured by a handler

$$
\langle \mathbf{tls}(\mathbf{return}\ n); E; U; M; I \rangle \to \langle \mathbf{tls}(\mathbf{return}\ n); E; U; \emptyset; \top \rangle
$$

Since $\mathbf{check}_M$s are at least as permissive as $\mathbf{check}$s, the best-effort dynamic check is at least as expressive as the eager dynamic check. The implementation of the best-effort scope extrusion check allows the program in Listing 16.

4.3.1. Correctness of the Best-Effort Dynamic Check

Correctness of the best-effort dynamic check is easy to show: if there is best-effort scope extrusion, then either one of the the $\mathbf{check}_M$s reports an error, or none do. The latter case degenerates to the lazy dynamic check, where the top-level splice $\mathbf{check}$ must report an error.

> **Theorem 4.3.2 (Correctness of the Best-Effort Check)**
> *If*
>
> 1. $\cdot \vdash_c e : T^0\ !\ \emptyset; \emptyset$,
>
> 2. $[\![e]\!]_c^{BE} = t$
>
> 3. $\langle \textit{erase-checks}(t); [-]; \emptyset; \emptyset; \top \rangle$ *exhibits best-effort scope extrusion*

then there exists E, U, M, I such that

$$\langle t; [-]; \emptyset; \emptyset; \top \rangle \to^* \langle \mathbf{err}; E; U; M; I \rangle$$

Note that in the third condition we have to erase the checks in t, since adding a check can transform a program that will eventually exhibit lazy scope extrusion to one that will not (instead terminating early with an error).

4.3.2. Expressiveness of the Best-Effort Dynamic Check

The best-effort dynamic check occasionally misfires, reporting false positives. It is thus less expressive than the lazy dynamic check. In particular, it does not allow the program in Listing 17. The program in Listing 17 attempts to build the (unsafe) AST $\lambda x.\mathbf{return}\ y$, where y has extruded its scope, but then throws it away, returning instead the AST of 1. Critically, the constructor of the outer lambda, $\lambda x.[-]$, is never captured by any effect. Hence, the program will eventually reduce to a configuration

$$\langle \mathbf{dlet}(x_{\mathbb{N}}, \mathbf{return}\ \mathsf{Lam}(x_{\mathbb{N}}, \mathsf{Var}(y_{\mathbb{N}}))); E[\mathbf{check}[-]]; U; \{\mathsf{Var}(y_{\mathbb{N}})\}; I \rangle$$

where $\mathsf{len}(E[\mathbf{check}\,[-]]) < I$. The transition from this configuration will thus unmute $\mathsf{Var}(y_{\mathbb{N}})$, and the surrounding **check** will fail, as $\mathsf{Var}(y_{\mathbb{N}})$ is free, unmuted, and not declared safe.

```
$(⟨⟨λx.$(handle ⟨⟨λy.$(op(y); return y)⟩⟩            λ⟨⟨op⟩⟩
        with {return(u) ↦ return ⟨⟨0⟩⟩; op(z, k) ↦ return z})⟩⟩);
  ⟨⟨1⟩⟩))
```

Listing 17: The best-effort scope extrusion check reports false positives. This program attempts to build the (unsafe) AST $\lambda x.\mathbf{return}\ y$, where y has extruded its scope, but then throws it away, returning instead the AST of 1. Critically, the program will eventually unmute $\mathsf{Var}(y_{\mathbb{N}})$, and the surrounding **check** will fail, as $\mathsf{Var}(y_{\mathbb{N}})$ is free, unmuted, and not declared safe.

Rather than expressiveness, the best-effort dynamic check exhibits a "Cause for Concern" property. Effectively, if the best-effort check reports an error, **and the offending AST n appears in the final result of compile-time computation**, then there must be lazy scope extrusion. Consequently, in cases like Listing 17, the only way to safely use $\lambda x.\mathbf{return}\ y$ is to throw it away.

> **Theorem 4.3.3 (Cause for Concern Property)**
> *If*
>
> 1. *$\cdot \vdash_{\mathbf{c}} e : T^0 \,!\, \emptyset; \emptyset$,*
>
> 2. *$[\![e]\!]_{\mathbf{c}}^{BE} = t$*
>
> 3. *There exists E, U, M, I such that $\langle t; [-]; \emptyset; \emptyset; \top \rangle \to^* \langle \mathbf{check}_M\, n; E; U; M; I \rangle$ and $\langle \mathbf{check}_M\, n; E; U; M; I \rangle \to \langle \mathbf{err}; E; U; M; I \rangle$*

> *Then for all $i \in \mathbb{N}$, if*
>
>   4. $\langle \textbf{return } n; \textit{erase-checks}(E); U; M; I \rangle \rightarrow^i \langle \textbf{return } m; E'; U'; M'; I' \rangle$
>
>   5. *and n a subtree of m,*
>
> *then $\textsf{FV}^0(m) \nsubseteq \pi_{\textsf{Var}}(E')$*

The proof of Theorem 4.3.3 is by contradiction. By assumption (3) there must be at least one variable, call it $\textsf{Var}(x_T)$, that is free in n and not declared safe in E. Assume for the sake of contradiction that $\textsf{FV}^0(m) \subseteq \pi_{\textsf{Var}}(E')$. Then, by assumption (5), the frame $\textbf{dlet}(x_T, [-])$ must be in E'. By assumptions (1) and (2), we only have to consider terms that are the target of elaboration. By definition of elaboration, the only way to push the frame $\textbf{dlet}(x_T, [-])$ on E' is by resuming a continuation containing $\textbf{dlet}(x_T, [-])$. But then we must have had access to the resumed continuation in E. In turn, this implies $I < \textsf{len}(E)$, and thus $\textsf{Var}(x_T)$ would not have been unmuted. Consequently, $\textbf{check}_M\, n$ would not have failed because of $\textsf{Var}(x_T)$. This contradicts assumption (3).

Note that the eager dynamic check does not have the Cause for Concern property, with Listing 16 being a counter-example. Hence, the best-effort dynamic check is **more** expressive, and more **predictably** expressive, than the eager dynamic check.

4.3.3. Efficiency of the Best-Effort Dynamic Check

The best-effort dynamic check is certainly less efficient than the eager dynamic check. Like the eager dynamic check, I conjecture that the best-effort check is more efficient in the common case than the lazy check, but I leave substantiating the argument to further research.

4.4. Refined Environment Classifiers

The method of refined environment classifiers (Section 2.3.1, Page 23) presents a static approach to preventing scope extrusion. Isoda et al. [12] introduce a calculus with algebraic effects and code combinators (rather than quotes and splices), whose interaction is moderated via refined environment classifiers. This section demonstrates that refined environment classifiers may be encoded, and therefore evaluated, in $\lambda_{\langle\langle \textsf{op} \rangle\rangle}$.

The $\lambda_{\langle\langle \textsf{op} \rangle\rangle}$ type system is augmented with a **simplified** version of Isoda et al.'s type system:

1. $\lambda_{\langle\langle \textsf{op} \rangle\rangle}$ types are straightforwardly extended, by annotating all level -1 Code types with a classifier (Figure 4.2).

2. Similarly, level 0 types are associated with a classifier. However, following Isoda et al. [12], this association is indirect: for level 0 types, classifiers are associated with the judgement rather than annotated onto the type (Figure 4.3).

3. Correspondingly, $\lambda_{\textsf{AST}(\textsf{op})}$ types are extended, with all AST types annotated with a classifier.

For ease of reasoning, it is helpful to define the notion of an **extended** source type.

Types (Refined Environment Classifiers)

Level -1   Values $T^{-1} ::= \ldots \mid (\text{Code}(T^0 \, ! \, \xi)^{\boxed{\gamma}})^{-1}$

Figure 4.2.: Extending $\lambda_{\langle\langle \text{op} \rangle\rangle}$ with refined environment classifiers. The only change is that Code types are now annotated with an environment classifier γ, **highlighted** .

Definition 4.4.1 (Extended source type)
*An **extended** source type is either:*

1. *A level -1 type, for example, $(\text{Code}(\mathbb{N}^0)^\gamma)^{-1}$ or*

2. *A level 0 type annotated with a classifier, for example, $\mathbb{N}^0(\gamma)$.*

3. *A level 0 binder type, which is a level 0 value type (like $\mathbb{N}^0(\gamma)$) annotated with an <u>underline</u> to indicate that it will be elaborated into a binder type, $(\underline{\mathbb{N}^0(\gamma)})$*

Contexts Γ must contain the least classifier $\gamma_\perp$ (so the empty context is no longer permitted), and the definition of closed well-typed expression is adapted to reflect this

---

Definition 4.4.2 (Well-typed closed Expression, Refined Environment Classifiers)
e is a well-typed expression if $\gamma_\perp \vdash_{\boldsymbol{c}}^{\gamma_\perp} e : T^0 \, ! \, \emptyset; \emptyset$

Most typing rules are straightforwardly adapted, with key rules listed in Figure 4.3.

$\$(\textbf{handle do } x \leftarrow \textbf{genlet}(\langle\langle e \rangle\rangle) \textbf{ in } \langle\langle x + x \rangle\rangle$
$\quad \textbf{with } \{\textbf{return}(u) \mapsto u; \textbf{genlet}(y, k) \mapsto \langle\langle \, (\lambda z. \$(\textbf{continue } k \, \langle\langle z \rangle\rangle)) \, y \, \rangle\rangle\})$

Listing 18: An example of let-insertion. For the program to be well-typed, the continuation k should be polymorphic over classifiers. To prove that continuations are always polymorphic in this manner, the type system demands that handlers are polymorphic over classifiers as well.

The **c**|**q**-Lambda rule corresponds to C-Abs in the refined environment classifier literature. Following Isoda et al., handlers and continuations are restricted to Code types; However, types and typing rules are further simplified by eliminating polymorphism. To allow for let-insertion [39], as in Listing 18, Isoda et al.'s typing rules for handlers and continuations are polymorphic over the classifier. In Listing 18, the **genlet** effect is used to generate more efficient code: $(\lambda z.z + z)e$, where e is only evaluated once, rather than $e+e$. The continuation k is resumed under a binder (which introduces a classifier). Thus, for the program to be well-typed, the continuation k should be polymorphic over classifiers. Similarly, the type system demands that handlers are polymorphic over classifiers as well. For example, a more faithful transcription of their handler type would

have the form:

$$\forall \gamma.((\mathsf{Code}(S\,!\,\xi_1)^\gamma)\,!\,\Delta_1 \implies (\mathsf{Code}(T\,!\,\xi_2)^\gamma)\,!\,\Delta_2)$$

The polymorphism ($\forall \gamma$) is useful when proving that programs like the one in Listing 18 will produce well-scoped ASTs.

Reasoning about the correctness of polymorphic typing rules, however, is complex. It is even more complex in $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$. Recall that $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ does not have an operational semantics, but rather must first be elaborated into $\lambda_{\mathsf{AST(op)}}$ terms. Thus, it is difficult to reason directly about the $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$ type system via progress and preservation. One has to appeal to alternative techniques, like Tait-style logical relations [32], increasing the complexity of reasoning.

Given that the focus of this evaluation is on $\lambda_{\langle\langle\mathsf{op}\rangle\rangle}$, rather than refined environment classifiers, I choose to simplify the type system, and minimise the complexity of reasoning.

It is unclear whether Isoda et al.'s system allows for non-termination. Once again, to simplify reasoning, I force effect signatures to be well-founded and, in particular, not recursive. As proven by Kammar et al. [14], all well-typed programs must thus terminate.

Proof of correctness will rely on a weakening lemma. As types are stratified into two levels, and into value, computation, and handler types, there are 6 sub-lemmas. One is listed as an example.

Lemma 4.4.3 (Weakening for Level 0 Values)
If $\Gamma \vdash^\gamma_{c|q} e : T^0$ then

1. $\Gamma, (x : S^0)^{\gamma'} \vdash^\gamma_{c|q} e : T^0$ *for arbitrary $\gamma' \in \Gamma$*

2. $\Gamma, (x : S^{-1}) \vdash^\gamma_{c|q} e : T^0$

3. $\Gamma, \gamma' \vdash^\gamma_{c|q} e : T^0$, *for arbitrary $\gamma' \notin \Gamma$*

4. $\Gamma, \gamma' \sqsubseteq \gamma'' \vdash^\gamma_{c|q} e : T^0$, *for arbitrary $\gamma', \gamma'' \in \Gamma$*

Proof of the weakening lemma is by induction on the typing derivation.

Refined environment classifiers additionally require modification of the elaboration, and the reduction of $\lambda_{\mathsf{AST(op)}}$ terms:

1. Elaboration of types is defined on **extended** source types (Definition 4.4.1). This allows elaboration to carry classifiers. For example, rather than elaborationg $\mathbb{N}^0$, $\mathbb{N}^0(\gamma)$ is elaborated into $\mathsf{AST}(\mathbb{N})^\gamma$.

2. Elaboration of contexts is extended to carry proof-theoretic terms e.g. γ and $\gamma \sqsubseteq \gamma'$.

3. Elaboration of top-level splice $[\![\$e]\!]_c$ is adapted to not insert `tls`.

4. For simplicity, since refined environment classifiers do not require any of the machinery for dynamic scope extrusion checks, I consider the subset of $\lambda_{\mathsf{AST(op)}}$ without **check** (and **check**$_M$), **dlet**, **tls**, and **err**. $\lambda_{\mathsf{AST(op)}}$ configurations can thus be shortened to $\langle t; E; U \rangle$.

To the best of my knowledge, this is the first explicit presentation of refined environment classifiers in a calculus with quotation and splices rather than code combinators.

4.4.1. Correctness of Refined Environment Classifiers

The correctness of refined environment classifiers was previously informally justified in Section 2.3.1 (Page 23). This section shows that $\lambda_{\langle\langle op \rangle\rangle}$ can be used to formally reason about correctness, by proving that every well-typed $\lambda_{\langle\langle op \rangle\rangle}$ term returns a well-scoped AST on termination (Theorem 4.4.4).

> **Theorem 4.4.4 (Correctness of Refined Environment Classifiers)**
> *If $\gamma_\perp \vdash_{\boldsymbol{c}}^{\gamma_\perp} e : T^0 ! \emptyset; \emptyset$, and $[\![e]\!]_{\boldsymbol{c}} = t$,*
> *then for some U, $\langle t; [-]; \emptyset \rangle \rightarrow^* \langle \textbf{return}\ n; [-]; U \rangle$, and $FV^0(n) = \emptyset$*

The proof of Theorem 4.4.4 is via a Tait-style logical relation. A logical relation is useful to show that typing guarantees are maintained by elaboration [3].

The definition of the logical relation, Scoped, is presented in Figure 4.4. Scoped is defined on core language ($\lambda_{\text{AST(op)}}$) terms, and is indexed by:

1. A context of proof-theoretic terms Θ. Given a context of proof theoretic terms and variables Γ, one can project out only the proof theoretic terms $\pi_\gamma(\Gamma)$. For example, given

$$\Gamma = \gamma_\perp, \gamma_1, \gamma_\perp \sqsubseteq \gamma_1, (x : \mathbb{N}^0)^{\gamma_1}, \gamma_2, \gamma_1 \sqsubseteq \gamma_2, y : (\text{Code}(\mathbb{N}^0 ! \emptyset)^{\gamma_2})^{-1}$$

the proof theoretic part of the context is

$$\pi_\gamma(\Gamma) = \gamma_\perp, \gamma_1, \gamma_\perp \sqsubseteq \gamma_1, \gamma_2, \gamma_1 \sqsubseteq \gamma_2$$

which serves as our Θ.

2. An **extended** *source*-level type (Definition 4.4.1).

The two important definitions are the logical relation on the $T^0(\gamma)$ value type, and the logical relation on terms.

For a normal form n to be in the relation of the $T^0(\gamma)$ type, n must be an AST of the right type **and** the free variables of n need to be permitted by γ (permissibility was previously defined in Section 2.3.1, Page 23). Recall that the definition of permissibility assumes some known partial order on classifiers, e.g. $\gamma' \sqsubseteq \gamma$. The partial order is carried by the index Θ.

The logical relation on terms is defined as a least fixed point, following the definitions by Plotkin and Xie [24] and Kuchta [20], where the well-foundedness of the definition is additionally justified. Defining the logical relation as a fixed point gives rise to the principle of Scoped-Induction:

> **Definition 4.4.5 (Scoped-Induction)**
> *For some property Φ on closed terms of type $[\![\tau ! \Delta]\!]$, if*
>
> 1. *$\langle t; [-]; U \rangle \rightarrow^* \langle \textbf{return}\ n; [-]; U' \rangle$ implies $\Phi(t)$*
>
> 2. *$\langle t; [-]; U \rangle \rightarrow^* \langle \textbf{op}(n); E; U' \rangle \nrightarrow$, with op : $A^{-1} \to B^{-1}$, $n \in \textit{Scoped}_{\Theta, A^{-1}}$, and for*

Refined Environment Classifiers Typing Rules
$\lambda_{\langle\langle \mathbf{op} \rangle\rangle}$

Selected Rules

(**c**|**q**-VAR)
$$\frac{(x : T^0)^\gamma \in \Gamma}{\Gamma \vdash^\gamma_{\mathbf{c}|\mathbf{q}} x : T^0 \,!\, \Delta}$$

(**c**|**q**-LAMBDA)
$$\frac{\Gamma, \gamma', \gamma \sqsubseteq \gamma', (x : S)^{\gamma'} \vdash^{\gamma'}_{\mathbf{c}|\mathbf{q}} e : T \,!\, \Delta ; \xi \qquad \gamma \in \Gamma \qquad \gamma' \notin \Gamma}{\Gamma \vdash^\gamma_{\mathbf{c}|\mathbf{q}} \lambda x.e : (S \xrightarrow{\xi} T) \,!\, \Delta}$$

(**s**-OP)
$$\frac{\Gamma \vdash_{\mathbf{s}} v : S \qquad \mathsf{op} : S \to \mathsf{Code}(T \,!\, \xi)^\gamma \in \Sigma \qquad \mathsf{op} \in \Delta}{\Gamma \vdash_{\mathbf{s}} \mathbf{op}(v) : \mathsf{Code}(T \,!\, \xi)^\gamma \,!\, \Delta}$$

(**s**-CONTINUE)
$$\frac{\Gamma \vdash_{\mathbf{s}} v_1 : \mathsf{Code}(S \,!\, \xi_1)^\gamma \xrightarrow{\Delta} \mathsf{Code}(T \,!\, \xi_2)^{\gamma'} \qquad \Gamma \vdash_{\mathbf{s}} v_2 : \mathsf{Code}(S \,!\, \xi_1)^\gamma}{\Gamma \vdash_{\mathbf{s}} \mathbf{continue}\, v_1\, v_2 : \mathsf{Code}(T \,!\, \xi_2)^{\gamma'} \,!\, \Delta}$$

(**s**-HANDLE)
$$\frac{\Gamma \vdash_{\mathbf{s}} e : \mathsf{Code}(S \,!\, \xi)^\gamma \,!\, \Delta \qquad \qquad \qquad \qquad}{\Gamma \vdash_{\mathbf{s}} h : (\mathsf{Code}(S \,!\, \xi_1)^\gamma) \,!\, \Delta_1 \Longrightarrow (\mathsf{Code}(T \,!\, \xi_2)^\gamma) \,!\, \Delta_2 \qquad \forall \mathsf{op} \in \Delta_1 \setminus \Delta_2.\, \mathsf{op} \in \mathsf{dom}(h)}{\Gamma \vdash_{\mathbf{s}} \mathbf{handle}\, e\, \mathbf{with}\, \{h\} : \mathsf{Code}(T \,!\, \xi_2)^\gamma \,!\, \Delta_2}$$

(**c**|**q**-SPLICE)
$$\frac{\Gamma \vdash_{\mathbf{s}} e : (\mathsf{Code}(T^0 \,!\, \xi)^\gamma)^{-1} \,!\, \Delta}{\Gamma \vdash^\gamma_{\mathbf{c}|\mathbf{q}} \$e : T^0 \,!\, \Delta ; \xi}$$

(**s**-QUOTE)
$$\frac{\Gamma \vdash^\gamma_{\mathbf{q}} e : T \,!\, \Delta ; \xi}{\Gamma \vdash_{\mathbf{s}} \langle\langle e \rangle\rangle : (\mathsf{Code}(T^0 \,!\, \xi)^\gamma)^{-1} \,!\, \Delta}$$

(**c**|**q**-SUB)
$$\frac{\Gamma \vdash^\gamma_{\mathbf{c}|\mathbf{q}} \$e : T \,!\, \Delta ; \xi \qquad \Gamma \vDash \gamma \sqsubseteq \gamma'}{\Gamma \vdash^{\gamma'}_{\mathbf{c}|\mathbf{q}} e : T \,!\, \Delta ; \xi}$$

(**s**-SUB)
$$\frac{\Gamma \vdash_{\mathbf{s}} e : \mathsf{Code}(T \,!\, \xi)^\gamma \,!\, \Delta \qquad \Gamma \vDash \gamma \sqsubseteq \gamma'}{\Gamma \vdash_{\mathbf{s}} e : \mathsf{Code}(T \,!\, \xi)^{\gamma'} \,!\, \Delta}$$

Figure 4.3.: Selected typing rules for refined environment classifiers. The **c**|**q**-LAMBDA rule corresponds to C-ABS in the refined environment classifier literature. Following Isoda et al., handlers and continuations are restricted to Code types; However, types and typing rules are simpler than the system by Isoda et al., since there is no polymorphism.

> arbitrary $n' \in Scoped_{\Theta, B^{-1}}$, $\Phi(E[n'])$ *implies* $\Phi(t)$
>
> *Then for all* $t \in Scoped_{\Theta, \tau ! \Delta}$, $\Phi(t)$

The proof additionally relies on a closure lemma [20]

> **Lemma 4.4.6 (Closure under Anti-Reduction)**
> *If* $\langle t; E; U \rangle \to^* \langle t'; E'; U' \rangle$ *and* $E'[t'] \in Scoped_{\Theta, \tau ! \Delta}$ *then* $E[t] \in Scoped_{\Theta, \tau ! \Delta}$

Finally, the proof relies on a notion of closed substitution $\rho \vDash \Gamma$. Care must be taken with substitution of level-0 variables, since these should be in the logical relation for Binders rather than ASTs (note the second clause in Definition 4.4.7).

> **Definition 4.4.7 (Closed substitution)**
> *Given a context* Γ, *and assuming* $\Theta = \pi_\gamma(\Gamma)$, *the set of closed substitutions* $\rho \vDash \Gamma$ *are defined inductively as follows:*
>
> 1. $() \vDash \gamma_\perp$
>
> 2. *If* $\rho \vDash \Gamma$ *and* $n \in Scoped_{\Theta, \underline{T^0(\gamma)}}$ *then* $(\rho, n/x) \vDash \Gamma, (x : T^0)^\gamma$
>
> 3. *If* $\rho \vDash \Gamma$ *and* $n \in Scoped_{\Theta, T^{-1}}$ *then* $(\rho, n/x) \vDash \Gamma, (x : T^{-1})$
>
> 4. *If* $\rho \vDash \Gamma$ *then* $\rho \vDash \Gamma, \gamma$
>
> 5. *If* $\rho \vDash \Gamma$ *then* $\rho \vDash \Gamma, \gamma \sqsubseteq \gamma'$

It is now easy to show the fundamental lemma. Once again, because types are stratified, and typing judgements are indexed by a mode, the fundamental lemma decomposes into many sub-lemmas. One such is stated in Lemma 4.4.8.

> **Lemma 4.4.8 (Fundamental Lemma $[\mathbf{c}, T^0 ! \Delta; \xi]$ of the Scoped Logical Relation)**
> *If* $\Gamma \vdash^\gamma_{\mathbf{c}} e : T^0 ! \Delta; \xi$ *then for* $\Theta = \pi_\gamma(\Gamma)$, *and for all* ρ *such that* $\rho \vDash \Gamma$,
>
> $$\llbracket e \rrbracket_{\mathbf{c}}(\rho) \in Scoped_{\Theta, T^0 ! \Delta; \xi(\gamma)}$$

Proof of Lemma 4.4.8 is by induction on the source $\lambda_{\langle\langle \mathsf{op} \rangle\rangle}$ typing rules. I focus on an interesting case: the **c**-LAMBDA (C-ABS) case, where (handwaving the side-condition on U for clarity) it suffices to show that for some arbitrary ρ, $\rho \vDash \Gamma$,

$$\mathbf{do}\ x \leftarrow \mathtt{mkvar}\ \mathrm{erase}(S^0(\gamma'))\ \mathbf{in}\ \mathbf{do}\ \mathrm{body} \leftarrow \llbracket e \rrbracket_{\mathbf{c}}(\rho)\ \mathbf{in}\ \mathbf{return}\ \mathsf{Lam}(x, \mathrm{body})$$

in $Scoped_{\Theta, (S^0 \xrightarrow{\xi} T^0)^0 ! \Delta(\gamma)}$. It is clear that this reduces to

$$\mathbf{do}\ \mathrm{body} \leftarrow \llbracket e \rrbracket_{\mathbf{c}}(\rho, \alpha_{S\gamma'}/x)\ \mathbf{in}\ \mathbf{return}\ \mathsf{Lam}(\alpha_{S\gamma'}, \mathrm{body})$$

By anti-reduction (Lemma 4.4.6) it suffices to show that the term above is in the logical relation.

By weakening, and the induction hypothesis, $\llbracket e \rrbracket_{\mathbf{c}}(\rho, \alpha_{S\gamma'}/x) \in Scoped_{\Theta', T^0 ! \Delta; \xi(\gamma')}$, where $\Theta' =, \Theta, \gamma', \gamma \sqsubseteq \gamma'$. Applying Scoped-Induction on $\llbracket e \rrbracket_{\mathbf{c}}(\rho, \alpha_{S\gamma'})$:

1. If $\llbracket e \rrbracket_{\mathbf{c}}(\rho, \alpha_{S\gamma'}/x) \in \mathsf{Scoped}_{\Theta', T^0 ! \Delta; \xi(\gamma')}$ reduces to some **return** n, then by the inductive hypothesis it is of AST type and all its free variables are permitted by γ'. The term **do** body $\leftarrow$ **return** n **in** $\mathsf{Lam}(\alpha_{S\gamma'}, \mathsf{body})$ reduces to $\mathsf{Lam}(\alpha_{S\gamma'}, n)$, where $\mathsf{Var}(\alpha_{S\gamma'})$ is bound. By the typing rules, of the free variables, α is the only variable tagged with classifier γ'. So under Θ, we conclude that the free variables of $\mathsf{Lam}(\alpha_{S\gamma'}, n)$ are permitted by γ. The conclusion thus follows from anti-reduction.

2. If $\llbracket e \rrbracket_{\mathbf{c}}(\rho, \alpha_{S\gamma'}/x) \in \mathsf{Scoped}_{\Theta', T^0 ! \Delta; \xi(\gamma')}$ reduces to $E[\mathbf{op}(n)]$, then because the context **do** body $\leftarrow [-]$ **in return** $\mathsf{Lam}(\alpha_{S\gamma'}, \mathsf{body})$ introduces no handlers, the conclusion follows immediately from the inductive hypothesis.

I conjecture that this proof may be extended to support non-termination by incorporating the techniques of step-indexing and biorthogonality, as demonstrated by Biernacki et al. [4].

4.4.2. Expressiveness of Refined Environment Classifiers

The typing rules for refined environment classifiers forbid any program which attempts to extrude some variable x to a handler, *no matter how the handler chooses to use x* (Listing 19).

```
$(handle ⟨⟨ λx. return $( extrude(⟨⟨x⟩⟩) ) ⟩⟩
   with {return(u) ↦ return u; extrude(y, k) ↦ any arbitrary program})
```
$\lambda_{\langle\langle \mathbf{op} \rangle\rangle}$

Listing 19: The typing rules for refined environment classifiers forbid any program which attempts to extrude some variable x to a handler. Even if x is unused, or is resumed safely, this program will not type check.

```
$λz.(handle ⟨⟨ λx. return $( extrude(⟨⟨z⟩⟩) ) ⟩⟩
     with {return(u) ↦ return u; extrude(y, k) ↦ continue k ()})
```
$\lambda_{\langle\langle \mathbf{op} \rangle\rangle}$

Listing 20: Refined environment classifiers allow variables to be passed via effects, so long as the variable can never cause a scope extrusion error. In the program above, performing an effect with z never causes a scope extrusion error.

Thus, even if the handler throws x away, or resumes a continuation with x, the program in Listing 19 does not type-check. Consequently, neither do Listings 13 to 16. Thus, refined environment classifiers are less expressive even than the eager dynamic check.

The only variables that refined environment classifiers permit are those that never cause scope extrusion, for example, the variable z in Listing 20.

4.5. Evaluation of $\lambda_{\langle\langle \mathbf{op} \rangle\rangle}$

$\lambda_{\langle\langle \mathbf{op} \rangle\rangle}$ is an appropriate language in which to encode, and evaluate, scope extrusion checks. Formalising scope extrusion in $\lambda_{\langle\langle \mathbf{op} \rangle\rangle}$ provided clarity, aiding development of

---

The Scoped$_{\Theta,T}$ Logical Relation

Normal Forms

$n \in \mathsf{Scoped}_{\Theta,\mathbb{N}^{-1}}$ $\triangleq$ $n \in \mathbb{N}$

$n \in \mathsf{Scoped}_{\Theta,T^0(\gamma)}$ $\triangleq$ $\cdot \vdash [\![n]\!] \in [\![T^0(\gamma)]\!]$ and $\Theta \vdash \mathsf{FV}^0(n) \subseteq \mathsf{permitted}(\gamma)$
  (*symmetric for* $(Code(T^0)^\gamma)^{-1}$, $T^0 \,!\, \xi(\gamma)$, *etc*)

$n \in \mathsf{Scoped}_{\Theta,\underline{T^0(\gamma)}}$ $\triangleq$ $\mathsf{Var}(n) \in \mathsf{Scoped}_{\Theta,T^0 \,!\, \Delta(\gamma)}$

$n \in \mathsf{Scoped}_{\Theta,(S^{-1}\underline{\Delta}\to T^{-1})^{-1}}$ $\triangleq$ $\forall n' \in \mathsf{Scoped}_{\Theta,S^{-1}}, n\,n' \in \mathsf{Scoped}_{\Theta,T^{-1}\,!\,\Delta}$

$n \in \mathsf{Scoped}_{\Theta,(S^{-1}\underline{\Delta}\twoheadrightarrow T^{-1})^{-1}}$ $\triangleq$ $\forall n' \in \mathsf{Scoped}_{\Theta,S^{-1}}, \mathbf{continue}\,n\,n' \in \mathsf{Scoped}_{\Theta,T^{-1}\,!\,\Delta}$

Handlers

$h \in \mathsf{Scoped}_{\Theta,(S^{-1}\,!\,\Delta_1 \Longrightarrow T^{-1}\,!\,\Delta_2)^{-1}}$ $\triangleq$ if $h = \mathbf{return}(x) \mapsto t_{\mathrm{ret}}$
  $\forall n' \in \mathsf{Scoped}_{\Theta,S^{-1}}, t_{\mathrm{ret}}[n'/x] \in \mathsf{Scoped}_{\Theta,T^{-1}\,!\,\Delta_2}$

  else $h = h'; \mathbf{op}(x,k) \mapsto t_{\mathrm{op}}, \mathrm{op} : A^{-1} \to B^{-1}$
  $h' \in \mathsf{Scoped}_{\Theta,(S^{-1}\,!\,\Delta_1 \Longrightarrow T^{-1}\,!\,\Delta_2)^{-1}}$ and
  $\forall n \in \mathsf{Scoped}_{\Theta,A^{-1}}, n' \in \mathsf{Scoped}_{\Theta,B^{-1}\underline{\Delta_2}\twoheadrightarrow T^{-1}},$
  $t_{\mathrm{op}}[n/x,n'/k] \in \mathsf{Scoped}_{\Theta,T^{-1}\,!\,\Delta_2}$

Terms

In the following, let $\tau\,!\,\Delta$ be shorthand for any of $T^0\,!\,\Delta(\gamma)$, $T^0\,!\,\Delta; \xi(\gamma)$, $(S^0\,!\,\xi_1 \Longrightarrow T^0\,!\,\xi_2)^0\,!\,\Delta(\gamma)$, or $T^{-1}\,!\,\Delta$

$\mathsf{Scoped}_{\Theta,\tau\,!\,\Delta}$ $\triangleq$ The smallest property on terms t such that

1. For arbitrary U consistent with t, exists U' such that $\langle t; [-]; U\rangle \to^* \langle \mathbf{return}\,n; [-]; U'\rangle$, such that U' consistent with n, and $n \in \mathsf{Scoped}_{\Theta,\tau}$

2. For arbitrary U consistent with t, exists U' such that $\langle t; [-]; U\rangle \to^* \langle \mathbf{op}(n); E; U'\rangle \not\to$, U' consistent with $E[\mathbf{op}(n)]$, and

   a) $\mathrm{op} : A^{-1} \to B^{-1}$,

   b) $n \in \mathsf{Scoped}_{\Theta,A^{-1}}$, and

   c) for all $n' \in \mathsf{Scoped}_{\Theta,B^{-1}}, E[n'] \in \mathsf{Scoped}_{\Theta,\tau\,!\,\Delta}$

Where, in this context, consistent with t means that for all $\mathsf{Var}(\alpha_R)$ or $\alpha_R \in t$, $\alpha \in U$. This side condition ensures that we use `mkvar` correctly.

Figure 4.4.: The definition of the Scoped logical relation. Most definitions are standard. The logical relation on terms is defined as a least fixed point, following the definitions by Plotkin and Xie [24] and Kuchta [20], where the well-foundedness of the definition is additionally justified.

a novel best-effort dynamic check, which finds a sweet spot between the eager and dynamic checks. Additionally, unifying checks under a common language allows for comparative evaluation with reference to a bank of $\lambda_{\langle\langle op \rangle\rangle}$ programs, which serve as litmus tests of expressiveness.

The cost of encoding static and dynamic checks into the same language is that reasoning about the correctness of static checks becomes more complicated, since one can no longer prove correctness via progress and preservation. It is difficult to reduce the complexity of reasoning, since dynamic checks (as currently defined) are inserted by elaboration. I conjecture that the added complexity of reasoning is a reasonable cost to pay for a comprehensive and comparative evaluation.

5. Conclusion

This thesis makes significant progress on four fronts.

1. It introduces a novel two-stage calculus, $\lambda_{\langle\langle op \rangle\rangle}$, that allows for effect handlers at both stages: compile-time and run-time.

2. It formally describes and evaluates a range of scope extrusion solutions in $\lambda_{\langle\langle op \rangle\rangle}$, including the existing MetaOCaml check [16] and the refined environment classifiers approach [19]. Such comparison was facilitated by $\lambda_{\langle\langle op \rangle\rangle}$, validating its design.

3. It formally describes and evaluates a novel best-effort dynamic check, which occupies a goldilocks zone between expressiveness and efficiency.

4. It is supported by implementatopms of all three dynamic checks (lazy, eager, and best-effort) in MacoCaml.

5.1. Limitations and Future Work

Let-Insertion
This thesis was primarily concern with the *undesirable* interaction of metaprogramming and effects, rather than their *desirable* interaction: the previously described let-insertion [39].

I conjecture that $\lambda_{\langle\langle op \rangle\rangle}$ is an ideal target in which to study let-insertion. Let-insertion has typically been studied in calculi where only pure programs can be generated [12]. Let-insertion is more interesting when one can generate effectful programs. Since the order of operation becomes more important, it can be more challenging to describe an "optimal" insertion point.

Empirical Studies
I asserted that the dynamic checks differ in efficency, but in the common case, rather than worst case. I would like to verify this with empirical studies.

Kiselyov [16] additionally considers the *usability* of scope extrusion solutions, in terms of the informativeness of error messages. I did not consider this in my evaluation, but would like to perform user studies to more thoroughly evaluate usability.

Formalisation
The proofs in this thesis are pen-and-paper proofs. However, several are quite intricate (for example, the fundamental lemma of the Scoped logical relation). To ensure correctness, these proofs ought to be formalised in a theorem prover. Formalisation would further operationalise $\lambda_{\langle\langle op \rangle\rangle}$ as a testing bed for scope extrusion checks.

Bibliography

[1] D. Abrahams and A. Gurtovoy. *C++ Template Metaprogramming: Concepts, Tools, and Techniques from Boost and Beyond* (*C++ in Depth Series*). Addison-Wesley Professional, 2004. ISBN 0321227255.

[2] A. Bauer and M. Pretnar. An effect system for algebraic effects and handlers. *Logical Methods in Computer Science*, Volume 10, Issue 4, Dec. 2014. ISSN 1860-5974. doi: 10.2168/lmcs-10(4:9)2014. URL http://dx.doi.org/10.2168/LMCS-10(4:9)2014.

[3] N. Benton and C.-K. Hur. Biorthogonality, step-indexing and compiler correctness. In *Proceedings of the 14th ACM SIGPLAN International Conference on Functional Programming*, ICFP '09, page 97–108, New York, NY, USA, 2009. Association for Computing Machinery. ISBN 9781605583327. doi: 10.1145/1596550.1596567. URL https://doi.org/10.1145/1596550.1596567.

[4] D. Biernacki, M. Piróg, P. Polesiuk, and F. Sieczkowski. Handle with care: relational interpretation of algebraic effects and handlers. *Proc. ACM Program. Lang.*, 2(POPL), Dec. 2017. doi: 10.1145/3158096. URL https://doi.org/10.1145/3158096.

[5] C. Calcagno, E. Moggi, and W. Taha. Closed types as a simple approach to safe imperative multi-stage programming. In U. Montanari, J. D. P. Rolim, and E. Welzl, editors, *Automata, Languages and Programming*, pages 25–36, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg. ISBN 978-3-540-45022-1.

[6] C. Calcagno, W. Taha, L. Huang, and X. Leroy. Implementing multi-stage languages using ASTs, gensym, and reflection. In F. Pfenning and Y. Smaragdakis, editors, *Generative Programming and Component Engineering*, pages 57–76, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg. ISBN 978-3-540-39815-8.

[7] T.-J. Chiang, J. Yallop, L. White, and N. Xie. Staged compilation with module functors. *Proc. ACM Program. Lang.*, 8(ICFP), Aug. 2024. doi: 10.1145/3674649. URL https://doi.org/10.1145/3674649.

[8] M. Felleisen and D. P. Friedman. Control operators, the secd-machine, and the λ-calculus. In M. Wirsing, editor, *Formal Description of Programming Concepts - III: Proceedings of the IFIP TC 2/WG 2.2 Working Conference on Formal Description of Programming Concepts - III, Ebberup, Denmark, 25-28 August 1986*, pages 193–222. North-Holland, 1987.

[9] D. Hillerström and S. Lindley. Shallow effect handlers. In S. Ryu, editor, *Programming Languages and Systems*, pages 415–435, Cham, 2018. Springer International Publishing. ISBN 978-3-030-02768-1.

[10] huceke. memcpy.c. https://github.com/huceke/xine-lib-vaapi/blob/master/src/xine-utils/memcpy.c. Accessed: 2025-05-26.

[11] J. Inoue and W. Taha. Reasoning about multi-stage programs. In H. Seidl, editor, *Programming Languages and Systems*, pages 357–376, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. ISBN 978-3-642-28869-2.

[12] K. Isoda, A. Yokoyama, and Y. Kameyama. Type-safe code generation with algebraic effects and handlers. In *Proceedings of the 23rd ACM SIGPLAN International Conference on Generative Programming: Concepts and Experiences*, GPCE '24, page 53–65, New York, NY, USA, 2024. Association for Computing Machinery. ISBN 9798400712111. doi: 10.1145/3689484.3690731. URL https://doi.org/10.1145/3689484.3690731.

[13] Jax-Ml. Using grad on vmap on map on function containing sinc results in error. URL https://github.com/jax-ml/jax/issues/10750.

[14] O. Kammar, S. Lindley, and N. Oury. Handlers in action. In *Proceedings of the 18th ACM SIGPLAN International Conference on Functional Programming*, ICFP '13, page 145–158, New York, NY, USA, 2013. Association for Computing Machinery. ISBN 9781450323260. doi: 10.1145/2500365.2500590. URL https://doi.org/10.1145/2500365.2500590.

[15] O. Kiselyov. Delimited control in OCaml, abstractly and concretely. *Theoretical Computer Science*, 435:56–76, 2012. ISSN 0304-3975. doi: https://doi.org/10.1016/j.tcs.2012.02.025. URL https://www.sciencedirect.com/science/article/pii/S0304397512001661. Functional and Logic Programming.

[16] O. Kiselyov. The design and implementation of BER MetaOCaml. In M. Codish and E. Sumii, editors, *Functional and Logic Programming*, pages 86–102, Cham, 2014. Springer International Publishing. ISBN 978-3-319-07151-0.

[17] O. Kiselyov. Generating C: Heterogeneous metaprogramming system description. *Science of Computer Programming*, 231:103015, 2024. ISSN 0167-6423. doi: https://doi.org/10.1016/j.scico.2023.103015. URL https://www.sciencedirect.com/science/article/pii/S0167642323000977.

[18] O. Kiselyov. MetaOCaml: Ten years later: System description. In *Functional and Logic Programming: 17th International Symposium, FLOPS 2024, Kumamoto, Japan, May 15–17, 2024, Proceedings*, page 219–236, Berlin, Heidelberg, 2024. Springer-Verlag. ISBN 978-981-97-2299-0. doi: 10.1007/978-981-97-2300-3_12. URL https://doi.org/10.1007/978-981-97-2300-3_12.

[19] O. Kiselyov, Y. Kameyama, and Y. Sudo. Refined environment classifiers. In A. Igarashi, editor, *Programming Languages and Systems*, pages 271–291, Cham, 2016. Springer International Publishing. ISBN 978-3-319-47958-3.

[20] W. Kuchta. A proof of normalization for effect handlers, Sept. 2023. URL https://icfp23.sigplan.org/details/hope-2023/4/A-proof-of-normalization-for-effect-handlers. Seattle, Washington, United States.

[21] J. L. Lawall and O. Danvy. Continuation-based partial evaluation. *SIGPLAN Lisp Pointers*, VII(3):227–238, July 1994. ISSN 1045-3563. doi: 10.1145/182590.182483. URL https://doi.org/10.1145/182590.182483.

[22] K. W. Li. Toward mechanized proof of macocaml with staging inference. Mphil thesis, University of Cambridge, 2024.

[23] L. Phipps-Costin, A. Rossberg, A. Guha, D. Leijen, D. Hillerström, K. Sivaramakrishnan, M. Pretnar, and S. Lindley. Continuing WebAssembly with effect handlers. *Proc. ACM Program. Lang.*, 7(OOPSLA2), Oct. 2023. doi: 10.1145/3622814. URL https://doi.org/10.1145/3622814.

[24] G. Plotkin and N. Xie. Handling the selection monad (full version), 2025. URL https://arxiv.org/abs/2504.03890.

[25] M. Pretnar. An introduction to algebraic effects and handlers. invited tutorial paper. *Electronic Notes in Theoretical Computer Science*, 319:19–35, 2015. ISSN 1571-0661. doi: https://doi.org/10.1016/j.entcs.2015.12.003. URL https://www.sciencedirect.com/science/article/pii/S1571066115000705. The 31st Conference on the Mathematical Foundations of Programming Semantics (MFPS XXXI).

[26] H. G. Rice. Classes of Recursively Enumerable sets and their decision problems. *Transactions of the American Mathematical Society*, 74(2):358–366, 1953. ISSN 00029947, 10886850. URL http://www.jstor.org/stable/1990888.

[27] A. D. Robison. Impact of economics on compiler optimization. In *Proceedings of the 2001 Joint ACM-ISCOPE Conference on Java Grande*, JGI '01, page 1–10, New York, NY, USA, 2001. Association for Computing Machinery. ISBN 1581133596. doi: 10.1145/376656.376751. URL https://doi.org/10.1145/376656.376751.

[28] G. Scherer. Deciding equivalence with sums and the empty type. In *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages*, POPL '17, page 374–386, New York, NY, USA, 2017. Association for Computing Machinery. ISBN 9781450346603. doi: 10.1145/3009837.3009901. URL https://doi.org/10.1145/3009837.3009901.

[29] M. Servetto and E. Zucca. A meta-circular language for active libraries. In *Proceedings of the ACM SIGPLAN 2013 Workshop on Partial Evaluation and Program Manipulation*, PEPM '13, page 117–126, New York, NY, USA, 2013. Association for Computing Machinery. ISBN 9781450318426. doi: 10.1145/2426890.2426913. URL https://doi.org/10.1145/2426890.2426913.

[30] T. Sheard and S. P. Jones. Template meta-programming for Haskell. In *Proceedings of the 2002 ACM SIGPLAN Workshop on Haskell*, Haskell '02, page 1–16, New York, NY, USA, 2002. Association for Computing Machinery. ISBN 1581136056. doi: 10.1145/581690.581691. URL https://doi.org/10.1145/581690.581691.

[31] K. Sivaramakrishnan, S. Dolan, L. White, T. Kelly, S. Jaffer, and A. Madhavapeddy. Retrofitting effect handlers onto OCaml. In *Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation*, PLDI 2021, page 206–221, New York, NY, USA, 2021. Association for Computing Machinery. ISBN 9781450383912. doi: 10.1145/3453483.3454039. URL https://doi.org/10.1145/3453483.3454039.

[32] W. W. Tait. Intensional interpretations of functionals of finite type i. *The Journal of Symbolic Logic*, 32(2):198–212, 1967. ISSN 00224812. URL http://www.jstor.org/stable/2271658.

[33] L. Tratt. Domain specific language implementation via compile-time meta-programming. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 30(6):1–40, 2008.

[34] J. Vandebon, J. G. F. Coutinho, W. Luk, and E. Nurvitadhi. Enhancing high-level synthesis using a meta-programming approach. *IEEE Transactions on Computers*, 70(12):2043–2055, 2021. doi: 10.1109/TC.2021.3096429.

[35] T. Walid. Multi-stage programming: Its theory and applications. Technical report, 1999.

[36] H. Wickham. *Advanced R*. Chapman and Hall/CRC, 2019.

[37] N. Xie, Y. Cong, K. Ikemori, and D. Leijen. First-class names for effect handlers. *Proc. ACM Program. Lang.*, 6(OOPSLA2), Oct. 2022. doi: 10.1145/3563289. URL https://doi.org/10.1145/3563289.

[38] N. Xie, L. White, O. Nicole, and J. Yallop. MacoCaml: Staging composable and compilable macros. *Proc. ACM Program. Lang.*, 7(ICFP), Aug. 2023. doi: 10.1145/3607851. URL https://doi.org/10.1145/3607851.

[39] J. Yallop and O. Kiselyov. Generating mutually recursive definitions. In *Proceedings of the 2019 ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation*, PEPM 2019, page 75–81, New York, NY, USA, 2019. Association for Computing Machinery. ISBN 9781450362269. doi: 10.1145/3294032.3294078. URL https://doi.org/10.1145/3294032.3294078.

[40] J. Yallop, N. Xie, and N. Krishnaswami. flap: A deterministic parser with fused lexing. *Proc. ACM Program. Lang.*, 7(PLDI), June 2023. doi: 10.1145/3591269. URL https://doi.org/10.1145/3591269.

A. Auxiliary Definitions

A.1. Erase

The erase function takes a level 0 type and erases all level annotations, and elaborates effect rows. It is defined by straightforward induction on $\lambda_{\langle\langle \text{op} \rangle\rangle}$ types.

$$
\begin{aligned}
\text{erase}(\mathbb{N}^0) &= \mathbb{N} \\
\text{erase}((S^0 \xrightarrow{\xi} T^0)^0) &= \text{erase}(S^0) \xrightarrow{[\![\xi]\!]} \text{erase}(T^0) \\
\text{erase}((S^0 \xrightarrow{\xi} \!\!\!\twoheadrightarrow T^0)^0) &= \text{erase}(S^0) \xrightarrow{[\![\xi]\!]} \!\!\!\twoheadrightarrow \text{erase}(T^0) \\[6pt]
\text{erase}(T^0 \,! \, \xi) &= \text{erase}(T^0) \,! \, [\![\xi]\!] \\
\text{erase}(T^0 \,! \, \Delta) &= \text{erase}(T^0) \,! \, [\![\Delta]\!] \\
\text{erase}(T^0 \,! \, \Delta; \xi) &= \text{erase}(T^0) \,! \, [\![\Delta]\!]; [\![\xi]\!] \\[6pt]
\text{erase}((S^0 \,! \, \xi_1 \Longrightarrow T^0 \,! \, \xi_2)^0 \,! \, \Delta) &= (\text{erase}(S^0) \,! \, [\![\xi_1]\!] \Longrightarrow \text{erase}(T^0) \,! \, [\![\xi_2]\!]) \,! \, [\![\Delta]\!]
\end{aligned}
$$

B. Litmus Tests

B.1. MetaOCaml

This section transcribes Listings 11, 12, 14 and 15 in BER MetaOCaml N153.

To test these programs, as of 05 June 2025, one must first set up MetaOCaml to perform scope extrusion checking.

```MetaOCaml
let () =  Trx.set_with_stack_mark
  {Trx.stackmark_region_fn =
      fun body ->
        let module M = struct type _ Effect.t += E: unit t end in
        try body (fun () -> try perform M.E; true with Unhandled _ -> false)
        with effect M.E, k -> continue k ()}
```

```MetaOCaml
run (let z  = match .<fun x -> .˜(perform (Extrude .<x>.) ) >.
             with u -> .<0>.
                 | effect (Extrude y), k -> y
      in .< .˜z + 1 >.)
```

Listing 21: Listing 11, transcribed in MetaOCaml

```MetaOCaml
let z = run (match .<fun x -> .˜(perform (Extrude .<x>.) ) >.
             with u -> .<0>.
                 | effect (Extrude y), k -> y)
in z + 1
```

Listing 22: Listing 12, transcribed in MetaOCaml

```MetaOCaml
run (match .<fun x -> .˜(perform (Extrude .<x>.) ) >.
             with u -> .<0>.
                 | effect (Extrude y), k -> let _ = y in .<0>. )
```

Listing 23: Listing 14, transcribed in MetaOCaml

```MetaOCaml
run (match .<fun x -> .˜(perform (Extrude .<x>.) ) >.
             with u -> .<0>.
                 | effect (Extrude y), k -> continue k y )
```

Listing 24: Listing 15, transcribed in MetaOCaml

B. Litmus Tests

```MetaOCaml
1  run (match .<fun x -> .˜(perform (Extrude .<x>.) ) >.
2          with u -> .<0>.
3            | effect (Extrude y), k -> continue k .< .˜y + 1>. )
```

Listing 25: Listing 16, transcribed in MetaOCaml