K 1

Conventions

1.1 Languages

The discussion of formal languages requires the use of several different languages simultaneously. The following is a list of the languages used in this work:

- **narrative (informal) language**: The top-level language used to narrate this work in an intuitive prose; English.
- **logical meta-language**: Formalized expressions that make no extra-logical assumptions. Contains expressions such as "The proposition A implies the proposition A."
- **mathematical meta-language**: Mathematical expressions of generalized programs, where terms range more freely than in actual valid programs in the programming language. Relies on a mathematical context not explicit in this work. Contains expressions such as "$f : \alpha \to \beta \to \gamma$."
- **programming language**: Programs that are fully defined by the contents of this work, relying on no external context. Necessarily conforms to the given syntax, and its expressions have no meaning beyond the given rules that apply to them. Contains expressions such as "`term id (α:Type) (a:α) : α := a.`"

1.2 Fonts

The use of many different languages simultaneously, as described by the previous section, has the unfortunate consequence of certain expressions seeming ambiguous to the reader. In order to mitigate this problem, each language and certain kinds of phrases are designated a font. The following fonts are designated in this way:

- **normal font**: narrative language.
- **italic font**: emphasis in narrative language.

- **bold font**: introductory use of new terms in narrative language, and syntactic structures in narrative language.
- **small-caps font**: names in logical meta-language.
- **sans-serif font**: mathematical meta-language.
- **monospace font**: programming language.

1.3 Names

Naming conventions: **TODO**

- **terms**: lower-case english word/phrase.
- **term variables**: lower-case english letter.
- **types**: lower-case english word/phrase.
- **types of higher order**: capitalized english word/phrase.
- **type variables**: lower-case greek letter.
- **type variables of higher order**: capital english letter.

K 2

Introduction

TODO: change `to in` most cases, and have to wrap in $'s **TODO**: change declaration header ‘term‘ and ‘type‘ to just one keyword, say ‘let‘ **TODO**: is this entire chapter, change concrete programs to be entirely monospace font

2.1 Language A

lambda-calculus is a formal language for expressing computation. In this context, a **language** is defined to be a set of expression that are generated by syntactical rules. The lambda-calculus comes in many different variants, and here we will consider a basic variant of the **simply-typed lambda-calculus** in order to considering computation formally. Call our language A.

2.1.1 Syntax for A

In A, there are two forms used for constructing well-formed expressions: **terms** and **types**. They are expressed by the following syntax:

metavariable	constructors	name
«*program*»	`[` «*declaration*» `]`	program
«*declaration*»	`primitive term` «*term-name*» `:` «*type*»`.`	primitive term
	`term` «*term-name*» `:` «*type*» `:=` «*term*»`.`	constructed term
	`primitive type` «*type-name*» `:` «*Type*»`.`	primitive type
	`type` «*type-name*» `:` «*Type*» `:=` «*type*»`.`	constructed type
«*Type*»	`Type`	atom
	`Type ->` «*Type*»	arrow
«*type*»	«*type-name*»	atom
	`(`«*type-param*» `:` «*Type*»`) =>` «*type*»	function
	«*type*» «*type*»	application
«*term*»	«*term-name*»	atom
	`(`«*term-param*» `:` «*type*»`) =>` «*term*»	function
	«*term*» «*term*»	application

(2.1)

Metavariables. The metavariables «*term-name*», «*type-name*», and «*term-param*» range over, for a given program, a fixed and collection of names. There are two kinds of names included in this collection:

- **primitive names**: Included a priori. Terms and types provided this way are provided along with their a priori type or Type respectively, and primitive terms along with a priori reduction rules (if any).
- **constructed names**: Require a definition written in the language.

This syntax schema is formatted as a *generative context-free grammar*, with

- *non-terminals*: The meta-variables «*progam*», «*declaration*», «*Type*», «*type*», «*term*».
- *terminals*: Ranged over by the meta-variables «*term-name*», «*type-name*».
- *repeated*: Expressions of the form `[` «*meta-var*» `]` indicate that any number of «*meta-var*» can be repeated in its place.

The following are some examples of the sorts of formal items that these meta-variables stand range over:

- «*term-name*»: `1`, `12309`, `true`, `false`, `"hello world"`, •.
- «*type-name*»: `natural`, `integer`, `boolean`, `string`, `void`, `unit`.
- «*term-param*»: `x`, `y`, `this-is-an-parameter`.

TODO: include some function terms and (and maybe types?)

A given expression is well-formed with respect to A if it is constructible by a series of applications of these rules. Note that this syntax does not specify any concrete terms or types. In this way, A's syntax is defined so abstractly in order to make the definitions for its typing and semantics as concise as possible. For example, we shall reference to the type `int`, some «*term-name*»s that have type `int` such as $0, 1, -1, 2, -2, 3, -3$, and so on. Such types and terms as these are called **atoms** because they do not have any internal; they are simply posited as primitives in the language.

2.1.2 Syntactical sugar

Syntactical notations that translate definitional into their expansions before semantic processing are referred to as **syntactical sugar** in the programming community. In this way, they are *new* syntactical structures in A, but immediately reduce to the core set of syntactical structures as defined by the previously-outlined syntax of A. Since a few syntactical structures are used very commonly and are more intuitively read in a slightly different form, we shall adopt a few notations specified in the following few paragraphs.

Definition arguments. When a function term or type has multiple parameters, a convenient notation is to accumulate the parameters to the left side of a single => as follows:

$$\begin{array}{c} \texttt{[(}\text{«}\textit{term-param}\text{»}_i\ \texttt{:}\ \text{«}\textit{type}\text{»}_i\texttt{)}\ \texttt{=>]}\ \text{«}\textit{term}\text{»} \\ ::= \\ \texttt{[(}\text{«}\textit{term-param}\text{»}_i\ \texttt{:}\ \text{«}\textit{type}\text{»}_i\texttt{)]}\ \text{«}\textit{term}\text{»} \end{array} \tag{2.2}$$

$$\begin{array}{c} \texttt{[(}\text{«}\textit{type-param}\text{»}_i\ \texttt{:}\ \text{«}\textit{Type}\text{»}_i\texttt{)}\ \texttt{=>]}\ \text{«}\textit{type}\text{»} \\ ::= \\ \texttt{[(}\text{«}\textit{type-param}\text{»}_i\ \texttt{:}\ \text{«}\textit{Type}\text{»}_i\texttt{)]}\ \text{«}\textit{type}\text{»} \end{array} \tag{2.3}$$

When defining a term or type in a declaration it is convenient to write the names of parameters immediately to the right of the name being defined, resembling the syntax for applying the new term or type to its given arguments. The following notations implement this.

$$\begin{array}{c} \texttt{term}\ \text{«}\textit{term-name}\text{»}\ \texttt{[(}\text{«}\textit{type-param}\text{»}\texttt{:}\text{«}\textit{Type}\text{»}\texttt{)]}\ \texttt{[(}\text{«}\textit{term-param}\text{»}\texttt{:}\text{«}\textit{type}\text{»}\texttt{)]}\texttt{:}\text{«}\textit{type}\text{»}\texttt{:=}\text{«}\textit{term}\text{»}\texttt{.} \\ ::= \\ \texttt{term}\ \text{«}\textit{term-name}\text{»}\texttt{:[(}\text{«}\textit{type-param}\text{»}\texttt{:}\text{«}\textit{Type}\text{»}\texttt{)]=>}\text{«}\textit{type}\text{»}\texttt{:=[(}\text{«}\textit{term-param}\text{»}\texttt{:}\text{«}\textit{type}\text{»}\texttt{)]=>}\text{«}\textit{term}\text{»}\texttt{.} \end{array} \tag{2.4}$$

$$\begin{array}{c} \texttt{term}\ \text{«}\textit{type-name}\text{»}\ \texttt{[(}\text{«}\textit{type-param}\text{»}\texttt{:}\text{«}\textit{Type}\text{»}\texttt{)]}\ \texttt{:=}\ \text{«}\textit{type}\text{»}\texttt{.} \\ ::= \\ \texttt{term}\ \text{«}\textit{term-name}\text{»}\ \texttt{:=}\ \texttt{[(}\text{«}\textit{type-param}\text{»}\texttt{:}\text{«}\textit{Type}\text{»}\texttt{)]}\ \texttt{=>}\ \text{«}\textit{type}\text{»}\texttt{.} \end{array} \tag{2.5}$$

Local bindings. These are a core feature in all programming languages, and is expressed in A with this notation:

$$\begin{array}{c} \texttt{let}\ \text{«}\textit{term-name}\text{»} : \text{«}\textit{type}\text{»} \coloneqq \text{«}\textit{term}\text{»}_1\ \texttt{in}\ \text{«}\textit{term}\text{»}_2 \\ \Updownarrow \\ (\text{«}\textit{term-name}\text{»} : \text{«}\textit{type}\text{»} \Rightarrow \text{«}\textit{term}\text{»}_2)\ \text{«}\textit{term}\text{»}_1 \end{array} \tag{2.6}$$

Omitted types. The types of «*term-param*»s may sometimes be omitted when they are unambiguous and obvious from their context. For example, in

```
term twice : α( -> α) -> α -> α :=
  f a =>
    let a' = f a in
    f a'.
```

the types of `f`, `a`, and `a'` are obvious from the immediately-previous type of `twice`.

2.1.3 Primitives for A

TODO: rewrite these with syntax sugar The primitive names for a program are defined by its `primitive term` and `primitive type` declarations, and the constructed names for a program are defined by its `construct term` and `constructed type` declarations. There are two particularly useful primitive types, along with some accompanying primitive terms, to have defined as part of the core of A. The first of these is the `sum` type, where `sum` α β is the type of either α or β. To reflect this, a term x : `sum` α β is constructed with either a term of type α or a term of type β. These properties are specified by the following declarations:

```
primitive type sum : Type -> Type -> Type.

// constructors
primitive term left  α( β : Type) : α -> sum α b.
primitive term right α( β : Type) : β -> sum α b.

// destructor
primitive term split α( β γ : Type)
  : sum α β -> α( -> γ) -> β( -> γ) -> γ.
```

Notation 2.1.1. Case of sum. **TODO**: review this notation. We also introduce the

following syntax sugar for `split` — the following `case` notation:

$$\begin{aligned}&\texttt{case } \langle\!\langle \textit{term} \rangle\!\rangle \texttt{ to } \langle\!\langle \textit{type} \rangle\!\rangle \\ &\quad \texttt{\{ left (}\langle\!\langle \textit{term-param} \rangle\!\rangle_1 \texttt{:}\langle\!\langle \textit{type} \rangle\!\rangle_1 \texttt{) => } \langle\!\langle \textit{term} \rangle\!\rangle_1 \\ &\quad \texttt{| right (}\langle\!\langle \textit{term-param} \rangle\!\rangle_2 \texttt{:}\langle\!\langle \textit{type} \rangle\!\rangle_2 \texttt{) => } \langle\!\langle \textit{term} \rangle\!\rangle_2 \texttt{ \}} \\ &\qquad\qquad ::= \\ &\quad \texttt{split } \langle\!\langle \textit{type} \rangle\!\rangle_1 \ \langle\!\langle \textit{type} \rangle\!\rangle_2 \ \langle\!\langle \textit{type} \rangle\!\rangle \\ &\quad\ \texttt{((}\langle\!\langle \textit{term-param} \rangle\!\rangle_1 \texttt{:}\langle\!\langle \textit{type} \rangle\!\rangle_1 \texttt{) => } \langle\!\langle \textit{term} \rangle\!\rangle_1 \texttt{)} \\ &\quad\ \texttt{((}\langle\!\langle \textit{term-param} \rangle\!\rangle_2 \texttt{:}\langle\!\langle \textit{type} \rangle\!\rangle_2 \texttt{) => } \langle\!\langle \textit{term} \rangle\!\rangle_2 \texttt{)}\end{aligned} \tag{2.7}$$

The next notable primitive type to define here is the `product` type, where `product` α β is the type of both α and β. To reflect this, a term x : `product` α β is constructed with both a term of type α and a term of type β. These properties are reflected by the following declarations:

```
primitive type product : Type -> Type -> Type.

// constructor
primitive term pair α( β : Type) : α -> β -> product α β.

// destructors
primitive term first α( β : Type) : product α β -> α.
primitive term second α( β : Type) : product α β -> β.
```

TODO: mention other common primitives that will not be explicitly defined, based on the following:

- integer
- natural
- boolean
- unit

TODO: note that primitive terms need to have reduction rules defined outside of A (if they have any reductions), and that these are not guaranteed to not break the rest of A. So separate proofs need to be provided for complicated primitive stuff.

Notation 2.1.2. Infix arrow, sum, and product. The arrow, sum, and product types have a usual infixed notation to enhance the readability as they are immensely common and intentionally intuitive. These notations are as follows:

$$\langle\!\langle \textit{type} \rangle\!\rangle_1 \to \langle\!\langle \textit{type} \rangle\!\rangle_2 ::= \texttt{arrow } \langle\!\langle \textit{type} \rangle\!\rangle_1 \ \langle\!\langle \textit{type} \rangle\!\rangle_2 \tag{2.8}$$

$$\langle\!\langle \textit{type} \rangle\!\rangle_1 + \langle\!\langle \textit{type} \rangle\!\rangle_2 ::= \texttt{sum } \langle\!\langle \textit{type} \rangle\!\rangle_1 \ \langle\!\langle \textit{type} \rangle\!\rangle_2 \tag{2.9}$$

$$\langle\!\langle \textit{type} \rangle\!\rangle_1 \times \langle\!\langle \textit{type} \rangle\!\rangle_2 ::= \texttt{product } \langle\!\langle \textit{type} \rangle\!\rangle \ \langle\!\langle \textit{type} \rangle\!\rangle \tag{2.10}$$

Each of these infixed notations are right-associative. So, the type $\alpha \to \beta \to \gamma$ implicitly expands to $\alpha \to (\beta \to \gamma)$, matching a Curry-oriented[1] intuition.

Additionally, having multiple infixed notations for «*type*»s introduce inter-notational ambiguity. For example, the type $\alpha \to \beta \times \gamma + \delta$ could be associated in many different ways. We adopt the following precedence order of increasing tightness:

$$\to, +, \times.$$

According to this order, the type $\alpha \to \beta \times \gamma + \delta$ expands to the proper association $\alpha \to ((\beta \times \gamma) + \delta)$.

2.1.4 Typing Rules for A

TODO: fix fonts, if need be **TODO**: write Typing rules for types

Terms and types are related by a **typing judgement**, by which a term is stated to have a type. The judgement that a has type α is written as $a : \alpha$. In order to build typed terms using the constructors presented in **??**, the types of complex terms are inferred from their sub-terms using inference rules making use of judgement contexts (i.e. collections of judgements). A statement of the form $\Gamma \vdash a : \alpha$ asserts that the context Γ entails that $a : \alpha$. The notation $\Gamma, J \vdash J'$ abbreviates $\Gamma \cup \{J\} \vdash J'$. Keep in mind that these propositions (e.g. judgements) and inferences are in an explicitly-defined language that has no implicit rules. The terms "inference" and "judgement" are called such in order to have an intuitive sense, but rules about judgement and inference in general (outside of this context) are not implied to also apply here.

With judgements, we now can state **typing inferences rules**. Such inference rules have the form

$$\frac{P_1 \qquad \cdots \qquad P_n}{Q},$$

which asserts that the premises $P_1, \ldots, P_n$ entail the conclusion Q. For example,

$$\frac{\Gamma \text{ is a judgement context} \qquad a \text{ is a term} \qquad \alpha \text{ is a type} \qquad \Gamma \vdash a : \alpha}{\Gamma \vdash a : \alpha}$$

could be a particularly uninteresting inference rule. Explicitly stating the domain of each variable as premises is cumbersome however, so the following are conventions for variable domains based on their name:

- $\Gamma, \Gamma_i, \ldots$ each range over judgement con texts,
- $a, b, c, \ldots$ each range over terms,
- $\alpha, \beta, \gamma, \ldots$ each range over types.

[1] TODO: Citation needed?

The following typing rules are given for A:

$$\textbf{TODO}\quad \Gamma, a : \alpha \vdash a : \alpha$$

$$\textsc{Function-Abstraction}\quad \frac{\Gamma, a : \alpha \vdash b : \beta}{\Gamma \vdash a : \alpha \Rightarrow b : \alpha \to \beta}$$

$$\textsc{Function-Concretization}\quad \frac{\Gamma \vdash a : \alpha \to \beta \qquad \Gamma \vdash b : \alpha}{\Gamma \vdash a\ b : \beta}$$

$$\textsc{Destruct-Sum}\quad \frac{\Gamma \vdash x : (\alpha + \beta) \qquad \Gamma, a : \alpha \vdash c_1 : \gamma \qquad \Gamma, b : \beta \vdash c_2 : \gamma}{\Gamma \vdash (\texttt{case}\ x\ \{\ \texttt{left}\ a \Rightarrow c_1\ \mid\ \texttt{right}\ b \Rightarrow c_2\ \}) : \gamma} \tag{2.11}$$

2.1.5 Reduction Rules for A

Finally, the last step is to introduce **reduction rules**. So far we have outlined syntax and inference rules for building expressions in A, but all these expressions are inert. Reduction rules describe how terms can be transformed, step by step, in a way that models computation. A series of these simple reductions may end in a term for which no reduction rule can apply. Call these terms **values**, and notate "v is a value" as "value v." The following reduction rules are given for A:

$$\begin{aligned}
\beta\textsc{-Reduce}\quad & \frac{\text{value } v}{(\texttt{(}a\texttt{:}\alpha\texttt{)}\ \texttt{=>}\ b)\ v \twoheadrightarrow [v/a]b} \\
\textsc{Split-Left}\quad & \texttt{split}\ \alpha\ \beta\ \gamma\ \texttt{(left}\ a\texttt{)}\ f\ g \twoheadrightarrow f\ a \\
\textsc{Split-Right}\quad & \texttt{split}\ \alpha\ \beta\ \gamma\ \texttt{(right}\ a\texttt{)}\ f\ g \twoheadrightarrow f\ b \\
\textsc{Project-First}\quad & \texttt{first}\ \alpha\ \beta\ \texttt{(a, b)} \twoheadrightarrow \texttt{a} \\
\textsc{Project-Second}\quad & \texttt{first}\ \alpha\ \beta\ \texttt{(a, b)} \twoheadrightarrow \texttt{b}
\end{aligned} \tag{2.12}$$

The most fundamental of these rules is β-Reduction, which is the way that function applications are resolved to the represented computation's output. The substitution notation $[v/a]b$ indicates to "replace with v each appearance of a in b." In this way, for a function $a : \alpha \Rightarrow b : (\alpha \to \beta)$ and an input $v : \alpha$, β-Reduction **substitutes** the input v for the appearances of the function parameter a in the function body b.

For example, consider the following terms: **TODO**: enlightening example of a series of β-reductions for some simple computation.

2.1.6 Properties of A

With the syntax, typing rules, and reduction rules for A, we now have a completed definition of the language. However, some of the design desicions may seem arbitrary even if intuitive. This particular framework is good because it maintains a few nice properties that make reasoning about A intuitive and extendable.
TODOdefine these properties in English; want to keep prog-language and meta-language separate.

Theorem 2.1.1. (Type-Preserving Substitution in A). If $\Gamma, a : \alpha \vdash b : \beta$, $\Gamma \vdash v : \alpha$, and $\mathsf{value}\ v$, then $\Gamma \vdash [v/a]b : \beta$.

Theorem 2.1.2. (Reduction Progress in A). If $\{\} \vdash a : \alpha$, then either $\mathsf{value}\ a$ or $\exists a' : a \twoheadrightarrow a'$.

Theorem 2.1.3. (Type Soundness in A). If $\Gamma \vdash a : \alpha$ and $a \twoheadrightarrow a'$, then either $\mathsf{value}\ a'$ or $\exists a'' : \alpha \twoheadrightarrow a''$.

Theorem 2.1.4. (Type Preservation in A). If $\Gamma \vdash a : \alpha$ and $a \twoheadrightarrow a'$, then $\Gamma \vdash a' : \alpha$.

Theorem 2.1.5. (Strong Normalization in A). For any term a, either $\mathsf{value}\ a$ or there is a sequence of reductions that ends in a term a' such that $\mathsf{value}\ a$.

2.2 Computation with Effects

TODO: describe actual state of programming with effects i.e. writing C code (imperative).

The definition of A in section **??** embodies a good flavor for many similar functional programming languages. In terms of the such language's reductions from term to term, all the information relevant for deciding such reductions is explicit within the term itself and the explicit context built up during reduction. In other words, there is no **implicit activity** that influences what a term's reduction will look like. The path of reductions is exactly the computation a term corresponds to, so this yields that the computation has the same property of not having access to or being affected by any implicit activity.

However nice a formalization of computation this is, it is immediately unrealistic. Actual computers, for which programming languages are abstractions of their activities, host multitudes of implicit processes while running a program. Even if a programming language modelled all such processes and incorporated them into the language so that each activity was made perfectly explicit as a term (a task that is certainly infeasable and likely impossible), the result would be an unuseful and inefficient language. The point of having layers of abstraction, in the form of high-and-higher level programming language, is to avoid this situtation in the first place. So there appears to be a dilemma:

The Dilemma of Implicit Activities

(1) Require fully explicit terms and reductions. This grants reasoning about programs is fully formalized and abstracted from the annoyances of hardware and lower-level-implementations, but restricts such programs from being applicable in almost all useful circumstances.

(2) Allow implicit activities that affect reductions. This grants many useful program applications and maintains some formal nature to the language's behavior, but reasoning about programs is now inescapably tainted by implicit activities.

A resolution to this apparent dilemma is to either choose one horn or to reject the dilemma. But first, let us consider what kinds of implicit activities are being considered here — in particular, what are computational **effects**.

2.2.1 Effects

The definition of an **effect** in the context of programming language is frequently debated, and there is no majority standard answer[2]. For the purposes of this thesis, the following definition is adopted.

Definition 2.2.1. A computational **effect** is a capability in a program that depends on factors outside of that capability's normal scope.

The definition of **normal scope** will be left to intuitive interpretation, with the intent that what is the normal scope of a capability depends on many theoretical, design, and implementation factors.

Now for example, suppose we have a program P that computes the sum of two integers given as input. If P is designed and implemented exactly to this specification, then P has no effects; none of P's cabapilities depend on factors outside of their usual scope. The only scope that P's capabilities depend on is that of the two inputs. No other factors influence what the correctly computed sum of the two integers is. Such a program with no effects is called a **pure** program.

Definition 2.2.2. A program is **pure** if it has no effects.

But if P is run, as abstractly as it is defined, not much use comes from it. P does not display its results, write the results to some P-specified memory, or give you an error if there is an overflow. These capabilities depend on factors outside of P's normal scope, per its specification, and so are examples of effects.

So as another example, let us consider a modified version of P that is effectual. Suppose that program P' takes as input two integers, computes the sum of the integers, throws an error if there is an overflow, writes the result into RAM, and prints the result to the console from which P' was run. These capabilities are examples of effects, since their behavior depends on factors outside of the normal scope of P' (the same scope as P). Such a program with effects is called an **impure** program.

[2] **TODO**: source

Definition 2.2.3. A program is **impure** if it has effects.

There are a variety of common effects that are available in almost every programming language. These include:

- **input/output (IO),** e.g. printing to the console, accepting input from use, interfacing with other peripherals.
- **mutable data**, e.g. mutable variables, in-place arrays.
- **exception**, e.g. division by `0`, out-of-bounds index of array.
- **nondeterminism**, e.g. **TODO**: what would be good examples for this…
- **partiality**, e.g. **TODO**
- **continuation**, e.g. **TODO**

TODO: go into detail here, or till after I've talked about comparing functional/imperative approaches to effects?

According to definition **??**, there is an easy method for transforming an impure program into a pure program: add the factors depended upon by the program's effects to the program's scope. Using this intuition, we can reformulate the Dilemma of Implicit Activities with the new formal notion of computational effects:

The Dilemma of Effectual Purity

(1) Require only pure programs. This grants reasoning about programs to depend only on the normal scope of the program.

(2) Allow impure as well as pure programs. This grants many useful programs, where the behavior of the programs depends on factors not entirely encapsulated by the program's normal scope.

The goal of resolving this dilemma is to make a choice about how programming languages should be designed. Are computational effects a feature to be avoided as much as possible? Or are they actually so necessary that it would be a mistake to restrict them? Unsurprisingly, no widely-adopted languages have chosen horn (1). But even in more generality, almost all languages have chosen horn (2), but with many varied approaches to incorporating effects. Overally languages have clustered into two groups.

- **Functional** programming language treat computation as the evaluation of mathematical functions. Such languages put varying degrees of emphasis on restricting effects, but in general much more emphasis than imperative languages. E.g. Scheme, Lisp, Standard ML, Clojure, Scala, Haskell, Agda, Gallina.

- **Imperative** programming languages treat computation as a sequence of commands. E.g. the C family, Bash, Java, Python. Such languages put very little (if any) emphasis on restricting effects.

The perspective on effects is not the only way in which these groups differ, but nevertheless it is an important one. Among functional programming languages, we shall consider two in particular: Standard ML and Haskell. Standard ML takes a very relaxed approach to effects, and Haskell takes a more restrictive approach.

TODO: summarize a small history lesson of how there were two camps in the approach to effects: C code (systems-level programming) and PL people (type theory e.g. ML). For most of history, C code has won out, but more recently the advantages of structures in the lambda-calculus and type theory have started making their way into industry languages (e.g. Java has generics and lambdas, Haskell is getting mode industry use).

K 3

A Simple Approach to Effects

The Standard ML (Standard Meta Language) language is most commonly used in academic settings for teaching about programming languages. However here, I shall avoid introducing an entire new syntax and language semantics. Instead, the Standard ML effect design strategy will be demonstrated using B. B extends A with the following new features:

- **Sequence**. A collection of terms is arranged in the sequence of desired resolution. Reducing the sequence term will reduce the terms in order.
- **Mutable**. A new type that indicates mutable data. It must be explicitly read from and wrote to, rather than handled like the normal (immutable) value.
- **Exception**. A collection of new term constructs, allowing for programs to **throw** and **catch** exceptions that interrupt usual reduction.
- **Input/Ouput (IO)** A collection of new primitive terms that, when evaluated, yield effects in the evaluation context not reflected in their types.

3.1 Definition of B

3.1.1 Primitives for B

TODO: write English to encompass this

Sequencing. **TODO**: describe

```
primitive term sequence α( β : Type) : α -> β -> β.
```

Notation 3.1.1. Infix sequence.

$$(\text{«}term\text{»}_1 \ : \ \text{«}type\text{»}_1) \ ; \ (\text{«}term\text{»}_2 \ : \ \text{«}type\text{»}_2)$$
$$::=$$
$$\texttt{sequence} \ \text{«}type\text{»}_1 \ \text{«}type\text{»}_2 \ \text{«}term\text{»}_1 \ \text{«}term\text{»}_2.$$

Mutable. **TODO**: describe

```
primitive type mutable : Type -> Type.

primitive term new-mutable α( : Type) : α -> unit.
primitive term read α( : Type) : mutable α -> α.
primitive term write α( : Type) : mutable α -> α -> unit.
```

Notation 3.1.2. Infix and prefix mutable operations.

*(«term» : «type») ::= new-mutable «type» «term»
!(«term» : «type») ::= read «type» «term»
«term»$_1$ <- («term»$_2$: «type») ::= write «type» «term»$_1$ «term»$_2$

Exceptions. **TODO**: describe

```
primitive type exception : Type -> Type.

primitive term throw α( β : Type) : exception α -> α -> β.
primitive term catching α( β : Type)
  : (exception α -> α -> β) -> β -> β.
```

TODO: or, with dependent types. Maybe if I introduce dependent types in A, I could use them here. But not sure if that's a good idea. Perhaps I could introduce very simple dependent types, requiring positivity and totality and all that.

```
// dependent type, since has term-parameter.
primitive type exception α( : Type) : α -> Type.

primitive term throw α( : Type) (a : α) : exception α a.
primitive term catching α( β : Type) (e : exception α a)
  : (exception α a -> β) -> β -> β.
```

Notation 3.1.3.

catch { «term» («term-param»$_1$:«type»$_1$) => («term»$_2$:«type»$_2$) }
in «term»$_3$
::=
catching «type»$_1$ «type»$_2$ ((«term-param»$_1$:«type»$_1$) => «term»$_2$) «term»$_3$

TODO: describe how, in addition to these primitives for `exception`, there is also a collection of primitives of the form `primitive term` «*exception-name*» `: exception` «*type*». These define the kinds of exceptions that can be thrown.

IO. **TODO**: describe

```
primitive type mutable : Type -> Type.

primitive term input : unit -> string.
primitive term output : string -> unit.
```

3.1.2 Reduction Rules for B

TODO: formally explain how evaluation contexts work ($\mathcal{S}, \ldots \parallel a$). Should that go in this section, or the definition of A? If I put it in A, that would make defining let expressions much easier.
TODO: explain how S and E are handled when not included in inference rule (stay same)
TODO: define `new-uid(`$\mathcal{S}$`)`

Reduction Rules for Sequences

$$\textsc{Sequence}\quad \frac{\mathsf{value}\ a}{\mathcal{S};\mathcal{E} \parallel (a\ ;\ b) \twoheadrightarrow \mathcal{S};\mathcal{E} \parallel b} \tag{3.1}$$

Reduction Rules for Mutables

$$\textsc{Initialize}\quad \frac{\mathsf{value}\ v}{\mathcal{S} \parallel *v \twoheadrightarrow \mathcal{S}[\![\mathfrak{i} \mapsto v]\!] \parallel \mathfrak{i}} \quad \text{where } \mathfrak{i} = \texttt{new-uid}(\mathcal{S})$$

$$\textsc{Read}\quad \mathcal{S}[\![\mathfrak{i} \mapsto v]\!] \parallel !\mathfrak{i} \twoheadrightarrow \mathcal{S}[\![\mathfrak{i} \mapsto v]\!] \parallel v \tag{3.2}$$

$$\textsc{Write}\quad \frac{\mathsf{value}\ v'}{\mathcal{S}[\![\mathfrak{i} \mapsto v]\!] \parallel \mathfrak{i} \leftarrow v' \twoheadrightarrow \mathcal{S}[\![\mathfrak{i} \mapsto v']\!] \parallel \bullet}$$

TODO: Define what $\mathcal{S}$ looks like mathematically (a mapping, where indices form a set that can be looked at). **TODO**: Define

Reduction Rules for Exceptions **TODO**: Note the there must be a priority order to these reduction rules, because it matters which are applied in what order (as opposed to other rules).
TODO: use append operation for adding things to top of stack

$$\textsc{Throw}\ \frac{e : \texttt{exception}\ \alpha \qquad v : \alpha \qquad \mathsf{value}\ v}{\mathcal{E} \parallel \texttt{throw}\ e\ v \twoheadrightarrow (\texttt{throw}\ e\ v), \mathcal{E} \parallel \texttt{throw}\ e\ v}$$

$$\textsc{Raise}\ \frac{e : \texttt{exception}\ \alpha \qquad v : \alpha \qquad \mathsf{value}\ v}{(\texttt{throw}\ e\ v), \mathcal{E} \parallel a \twoheadrightarrow (\texttt{throw}\ e\ v), \mathcal{E} \parallel \texttt{throw}\ e\ v} \tag{3.3}$$

$$\textsc{Catch}\ \frac{e : \texttt{exception}\ \alpha \qquad v : \alpha \qquad \mathsf{value}\ v}{(\texttt{throw}\ e\ v), \mathcal{E} \parallel \texttt{catching}\ \alpha\ \beta\ e\ b \twoheadrightarrow \mathcal{E} \parallel}$$

Reduction Rules for IO

$$\begin{gathered}\textsc{Input}\ \ \mathcal{O} \parallel \texttt{input}\ \bullet \twoheadrightarrow \mathcal{O} \parallel \mathcal{O}(\texttt{input}\ \bullet) \\ \textsc{Output}\ \ \mathcal{O} \parallel \texttt{output}\ s \twoheadrightarrow \mathcal{O}(\texttt{output}\ s) \parallel \bullet\end{gathered} \tag{3.4}$$

These rules interact with the IO context, $\mathcal{O}$, by using it as an interface to an external IO-environment that handles the IO effects. This organization makes semantically explicit the division between B's model and an external world of effectual computations. For example, which $\mathcal{O}$ may be thought of as stateful, this is not expressed in the reduction rules as showing any stateful update of $\mathcal{O}$ to $\mathcal{O}'$ when its capabilities are used. An external implementation of $\mathcal{O}$ that could be compatible with B must satisfy the following specifications:

Specification of $\mathcal{O}$ **TODO**: should $\mathcal{O}(\texttt{output}\ )$ be specified as anything?

- $\mathcal{O}(\texttt{input}\ \bullet)$ returns a `string`.
- $\mathcal{O}(\texttt{output}\ s)$ returns nothing, and resolves to $\mathcal{O}$.

TODO: come up with running IO example

At this point, we can express the familiar Hello World program.

Listing 3.1: Hello World

```
output "hello world"
```

But as far as the definition of B is concerned, this term is treated just like any other term that evaluates to $\bullet$. The implementation for $\mathcal{O}$ used for running this program decides its effectual behavior (within the constraints of the specification of $\mathcal{O}$ of course). An informal but satisfactory implementation is the following:

Implementation 1 of $\mathcal{O}$:

- $\mathcal{O}$(`input` •):
  1. Prompt the console for user text input.
  2. Interpret the user text input as a string, then return the string.
- $\mathcal{O}$(`output` *s*):
  1. Write *s* to the console.
  2. Resolve to $\mathcal{O}$.

As intended by B's design, this implementation will facilitate Hello World appropriately: the text "hello world" is displayed on the console. Beyond the requirements enumerated by the specification of $\mathcal{O}$ however, B does not guarantee anything about how $\mathcal{O}$ behaves. Consider, for example, this alternative implementation:

Implementation 2 of $\mathcal{O}$:

- $\mathcal{O}$(`input` •):
  1. Set the toaster periphery's mode to **currently toasting**.
- $\mathcal{O}$(`output` *s*):
  1. Interpret *s* as a ABH routing number, and route $1000 from the user's bank account to 123456789.
  2. Set the toaster periphery's mode to **done toasting**.
  3. Resolve to $\mathcal{O}$.

This implementation does not seem to reflect the design of B, though unfortunately it is still compatible. In the way that B is defined, it is difficult to formally specify any more detail about the behavior of IO-like effects, since its semantics all but ignore the workings of $\mathcal{O}$.

3.2 Motivations

This chapter has introduced the concept of effects in programming languages, and presented B as a simple approach to extending a simple lambda calculus, A, with a sample of effects (mutable data, exceptions, IO). But such a simple approach leaves a lot to be desired.

Each effect is implemented by pushing effectual computation to the reduction context:

- Mutable data is managed by a mutable mapping between identifiers and values.
- Exceptions are thrown to and caught from an exception stack.

- IO is performed through an interface to an external IO implementation.

TODO: describe problem with this kind of approach:

- mutable data is global and stored outside language objects
- exceptions bypass type checking; exceptable programs aren't reflected in types
- IO is a black-box which is not reflected in types, so cannot be modularly reasoned about in programs (similar to exceptions)

K 4

Monadic Effects

4.1 Outline

1. Definition and context for monads in category theory and computer science

2. Explanation of how monads can model effects in general

3. Demonstration of constructing and using the stateful monad, building it up from scratch in Haskell or Haskell-like psuedocode

   ( ) Explain the Functor, Applicative, and Monad typeclasses, and how they build up the mathematical definition of a monad

4. Outline some problems with monadic effects

   ( ) different effects are not composable

   ( ) paper: *The Awkward Squad*

4.2 Introduction to Monads

TODO: introduce in programmer-friendly way first, mention category only for like a sentence if at all. give examples of writing code in Java/C/etc. and how we want to be able to do something similar but in a functional way

The concept of *monad* originates in the branch of mathematics by the name of Category Theory. As highly abstract as monads are, they turn out to be a very convenient structure for formalizing implicit contexts within functional programming languages. Though a background in the Categorical approach to monads and monad-related structures probably cannot hurt one's understanding of computational monads, this section will follow a more programmer-friendly path.

The Stateful Monad

One particularly general effect is the **stateful** effect, where an implicit, mutable state is accessible within a stateful computation. This effect was implemented by B by the introduction of a globally-accessible, mutable table of variables. This impl required, however, several new syntactical structures and reduction rules. Is there a way to implement something similar in just A?

It turns out there is — with a certain tradeoff. Since A is pure, such an impl cannot provide true mutability. However, we can model mutability in A as a function from the initial state to the modified state. Call a σ-computation of α to be a stateful computation where the state is of type σ and the result is of type α. To describe the type of such computations purely, consider the following:

```
type stateful σ( a : Type) : Type := σ -> σ × α.
```

Relating to the description of the stateful effect, `stateful` σ α is the type of functions from an initial σ-state to a pair of the affected σ-state and the α-result. So if given a term m : `stateful` σ α, one can purely compute the affected state and result by providing m with an initial state.

For `stateful` to truly be an effect, it needs to implicitly facilitate the stateful effect to some sort of internal context. So let us see how we can construct terms that work with `stateful`. In B's impl of this effect, it posited two primitive terms: `read` and `write`. Using `stateful` we can define these terms in A as:

```
term read σ{ : Type}
  : stateful σ σ
  := (s : σ) => (s, s).

term write σ{ : Type} (s' : σ)
  : stateful σ σ
  := (s : σ) => (s', •).
```

Observe that `read` is a σ-computation that does not modify the state and returns the state, `write` is a σ-computation that replaces the state with a given s' : σ and returns $\bullet$. In this way, using `read` and `write` in A fills exactly the same role as a simple B stateful effect of one mutable variable.

Since the stateful effect is in fact an effect, we should also be able to *sequence* stateful computations to produce one big stateful computation that does performs the computations in sequence. It is sufficient to define the sequencing of just two effects, since any number of effects can be sequenced one step at a time. So, given two σ-computations m : `stateful` σ α and m' : `stateful` σ β the sequenced σ-computation should first compute the m-affected state and then pass it to m'.

```
term stateful-sequence
      σ( α : Type)
      (m : stateful σ α) (m' : stateful σ β) :
  : stateful σ β
  := (s : σ) =>
      let (s', a) : σ × α := m s in
      m' s'.
```

However, in this form it becomes clear that `sequence` throws away some information — the α-result of the first stateful computation. To avoid this amounts to allowing m' to reference m's result, and can be modeled by typing m' instead as $\alpha \to$ `stateful` $\sigma\ \beta$. A sequence that allows this is called a *binding-sequence*, since it sequences m, m' and also *binds* the first parameter of m' to the result of m.

```
term stateful-bind
      (m : stateful σ α)
      (fm : α -> stateful σ β)
  : stateful σ β
  := (s : σ) =>
      let (s', a) : σ × α := m s in
      fm a s'.
```

Additionally, one may notice that one of `stateful-sequence` and `stateful-bind` is superfluous i.e. can be defined in terms of the other. Consider the following re-definition of `sequence`:

```
term stateful-sequence
      σ( α β : Type)
      (m : stateful σ α) (m' : stateful σ β)
  : stateful σ β
  := stateful-bind m ((a : α) => m')
```

This construction demonstrates how `sequence` can be thought of as a trivial binding-sequence, where the bound result of m is ignored by m'.

So far, we have defined all of the *special* operations that B provides for stateful computations. The key difference between B and our new A impl of the stateful effect is that B treats stateful computations just like any other kind of pure computation, whereas A "wraps" σ-stateful computations of α using the `stateful` $\sigma\ \alpha$ type rather than just pure α. What is still missing in our A impl is the ability to use non-stateful computations within or on stateful computations. In other words, we should be able to *lift* non-stateful computations to stateful computations that internally don't actually end up having stateful effects. There are two such computations to consider:

- **return**: The non-stateful computation, with parameter $a : \alpha$, that results in the same $a : \alpha$. In other words, the computation that does nothing and results in a.
- **lift**: The computation, with parameter non-stateful computation $f : \alpha \to \beta$ and stateful computation $m :$ `state` $\sigma\ \alpha$, that results in f applied to the result of m. In other words, the function the lifts $f : \alpha \to \beta$ to a function `stateful` $\sigma\ \beta \to$ `stateful` $\sigma\ \beta$.

These computations are implemented in A as follows:

```
term stateful-return (a : α)
  : stateful σ a
  := (s : σ) => (s, a)
```

```
term stateful-lift
    (f : α -> β) (m : stateful σ α)
  : stateful σ β
  := (s : σ) =>
      let (s', a) : σ × α := m s in
      (s', f a)
```

4.2.1 Definition of Monad

Now we have implemented a concrete approach to the stateful effect using pure terms in A. However, only the `read` and `write` terms were meant for exclusive use with `stateful`. The other necessary terms, as they correspond to use the impure impl in B, are intended to interoperate with all effects and interchangeably. To summarize, the capabilities the terms implement are

- **lift**
- **return**
- **binding-sequence**

With these in mind, the definition of monad is as follows:

Definition 4.2.1. A type $M : Type \to Type$ is a **monad** if there exist terms of the following types:

- `lift : (α -> β) -> M α -> M β`
- `return : α -> M α`
- `bind : M α -> (α -> M β) -> M β`

However, within A we currently have no type-oriented way to assert that a type M is associated with the expected constructions for qualifying as a monad. In order to formally and generally reference monads in A, we first need to introduce the concept type-classes.

4.3 Type-classes

4.3.1 Concept of Classes

The concept of a *class* is used in many different forms among many different programming languages. In object-oriented programming languages, classes define "blueprints" for creating objects that are instances of the class. Such a class defines an *interface* that each instance object of the class must implement. For example, the following Java code defines the abstract `Animal` class as the class of objects that have a `name` and implement the `eat` and `sleep` functions:

```
abstract class Animal {

  public String name;
  public Animal(String name) {
    this.name = name
  }

  abstract public void eat();
  abstract public void sleep();

}
```

```
class Animal {

  public void eat() {
    System.out.println(this.name + " eats.");
  }

  public void sleep() {
    System.out.println(this.name + " sleeps.");
  }

}
```

The motivation for the classes is to allow a parameter to range over a collection of different types of structures given that all of these structures meet some requirements. Then the parameter can be assumed to meet those requirements, regardless of the specific argument structure ends up being provided.

As is commonly known, both cats and dogs are examples of animals, so we can create respective objects that are instances of the `Animal` class:

```
class Cat extends Animal {

  public Cat() {
    super("Cat");
  }

  @Override
  public void eat() {
    System.out.println(this.name + " eats kibble.");
  }

  @Override
  public void sleep() {
    System.out.println(this.name + " naps.");
  }

  public void hunt() {
    System.out.println(this.name + " hunts for some mice and birds.");
  }

}

class Dog extends Animal {

  public Dog() {
    super("Dog");
  }

  @Override
  public void eat() {
    System.out.println(this.name + " eats steak.");
  }

  @Override
  public void sleep() {
    System.out.println(this.name + " sleeps wrestlessly.");
  }

  public void walk() {
    System.out.println(this.name + " goes on a walk with its owner.");
  }
```

```
}
```

Finally, and most importantly, we can write functions that take `Animal` parameters and only assume of these parameters what is specified by the `Animal` class — even though `Cat` and `Dog` are different structures.

```
void simple_simulate_animal(Animal a, int steps) {
  for (int i = 0; i < steps; i++) {
    a.eat();
    a.sleep();
  }
}
```

4.3.2 Definition of type-classes

Now back to the realm of strictly-typed functional programming languages. Our motivation at the moment is to devise a structure, describable in A, that allows for the formal specification of the monad and other type-class.

It turns out that we can model the monad type-class as a parametrized type, with the type `Monad (M:Type) : Type` of terms that implement the monad requirements for M. In other words, a term of type `Monad` M "contains" in some way (i.e. *implements*) terms with the types of `lift`, `return`, and `bind` as defined in section **??**. The simplest way to represent such an *implementation* of a type-class instance in this way is to represent the implementation as a type-product of the types of the required terms. Concretely, for the `Monad` type-class, we specify the `Monad` type as

```
type Monad (M : Type -> Type) : Type
  := α(( -> β) -> M α -> M β) ×
     α( -> M α) ×
     (M α -> α( -> M β) -> M β).
```

This allows working with monads (and other type-classes) using the following intuition: given a term of type `Monad` M, the terms required to be constructed in order for M to be a monad are available by projecting the from `Monad` M as the product of those types. Thus we can define `lift`, `return`, and `bind` for monads in general as follows:

```
term lift (M : Type -> Type) α( β : Type) (impl : Monad M)
  : α( β : Type) => α( -> β) -> M α -> M β
  := first impl

term return (M : Type -> Type) α( : Type) (impl : Monad M)
  : α( : Type) => α -> M α;
```

```
  := second impl

term bind (M : Type -> Type) α(, β : Type) (impl : Monad M)
  : α(, β : Type) => M α -> α( -> M β) -> M β
  := third impl
```

Finally, in order to use these functions with `Stateful σ`, we need to construct a term of type `Monad (Stateful σ)`. This term is the `Monad` type-class *implementation* for `Stateful σ`.

```
term Stateful-Monad
  : σ( : Type) => Monad (Stateful σ)
  := ( // lift
       α( β : Type) (f : α -> β) (m : M α) =>
         (s : σ) =>
           let (s', a) := m s in
           (s', f a)
       // return
     , α( : Type) (a : α) =>
         (s : σ) => (s, a)
       // bind
     , α( β : Type) (m : M α) (fm : α -> M β) =>
         (s : σ) =>
           let (s', a) := m s in
           a s' ).
```

This term can be passed as the first term argument to `lift`, `return`, and `bind` to yield terms that are concretely compatible with the `Stateful σ` instance of the `Monad` type-class.

Notations for type-classes

So far, the code that we have ended up writing to define a type-class and implement an instance of that type-class has contained a lot of boilerplate and is hard to follow on its own. For example, the types of `lift`, `return`, and `bind` had to be specified twice: once in the specification of `Monad`, and once again in their `Monad`-general constructions. To make the definition and instantiation of type-classes easier to read and write, we introduce the following notations.

Notation 4.3.1. Type-class definition. Defining a type-class requires specifying the terms that must be implemented for each instance of the type-class. The following notation allows concise specification, as well as additionally generating the terms, generalized to all

instances of the type-class, that are specified.

```
class «class-name» («type-param» : «Type») : «Type»
 { [ «term-name»_i : «type» ; ] }.
                    ::=
type «class-name» («type-param» : «Type») : «Type»
 := [ «type»_i × ].
[ term «term-name»_i («type-param» : «Type»)
    : (impl : «class-name» «type-param») -> «type»_i
    := i-th impl. ]
```
(4.1)

Using this notation, the definition of the `Monad` type-class is written more aesthetically as:

```
class Monad (M : Type) : Type
  { lift   : α(, β : Type) => α( -> β) -> M α -> M β
  ; return : α( : Type)    => α -> M α
  ; bind   : α(, β : Type) => M α -> α( -> M β) -> M β }.
```

Notation 4.3.2. Type-class instantiation. Instantiating the a type A as an instance of a type-class C requires implementing the terms specified by C where A is supplied as the argument to C's first type parameter. The following notation conveniently names this implementation and makes explicit C's intended names for each component.

```
instance [(«type-param»_i : «Type»_i) => ] «class-name» «type»
 { [ «term-name»_j : «type»_j := «term»_j ; ] }.
                    ::=
  term «class-name»-«type»
   : [(«type-param»_i : «Type»_i)] => «class-name» «type»
   := [ «term»_j × ].
```
(4.2)

TODO: explain how the way this notation works is a little tricky, since «*type*» may not be in a valid term-name format.

Using this notation, the implementation for the `Monad` instance of `(σ : Type) => State σ` is written more cleanly as:

```
instance σ( : Type) => Monad (Stateful σ)
  { lift α(, β : Type) (f : α -> β) (m : M α) : M β :=
      (s : σ) =>
        let (s', a) := m s in
        (s', f a)
  ; return α( : Type) (a : α) : M α :=
```

```
      (s : σ) => (s, a)
  ; bind α(, β : Type) (m : M α) (fm : α -> M β) : M β :=
      (s : σ) =>
        let (s', a) := m s in
        fm a s' }.
```

Notation 4.3.3. Type-class passive status. **TODO**: checking passively for type-class instances, providing them implicitly when necessary? This is kind of a larger change though.

TODO: Justify how monads are a good model for thinking about computation being pushed into an implicit context (cite Notions by Moggi).
TODO: Give definitions of other monads that implement other effects, such as exception and IO (and maybe others?)

K 5

Algebraic Effect Handlers

5.1 Outline

1. Introduction to continuations in general, and delimeted control.
2. Definition and context for algebraic effect handlers.
3. Explanation of the Eff programming languages approach to implementation
   - ( ) subset of semantics
   - ( ) examples
4. Comparison of algebraic effect handlers to monadic effects approach
   - ( ) alebraic effect handlers allow for effects and handlers to be defined separately
   - ( ) algebraic effect handlers and generally composable, however they must be carefully handled to match their internal composition
   - ( ) Eff does not expressively type the effect system, and many features are untyped

5.2 Definition of C