Do-it-yourself Module Systems

Extending Dependently-Typed Languages to Implement Module System Features In The Core Language

Department of Computing and Software

McMaster University

Musa Al-hassy

June 12, 2020

PhD Thesis

-- *Supervisors* | -- *Emails*
Jacques Carette | carette@mcmaster.ca
Wolfram Kahl | kahl@cas.mcmaster.ca

Chapter 1

Introduction

The construction of programming libraries is managed by decomposing ideas into self-contained units called 'packages' whose relationships are then formalised as transformations that reorganise representations of data. Depending on the *expressivity* of a language, packages may serve to avoid having different ideas share the same name —which is usually their *only* use— but they may additionally serve as silos of source definitions from which interfaces and types may be *extracted*. Figure 1 exemplifies the idea for monoids —which themselves model a notion of composition. In general, such derived constructions are *out of reach* from *within* a language and have to be extracted *by hand* by users who have the time and training to do so. Unfortunately, this is the standard approach; even though it is error-prone and disguises mechanical *library methods* (that are written *once* and proven correct) as *design patterns* (which need to be carefully implemented for *each* use and argued to be correct). The goal of this thesis is to show that sufficiently expressive languages make packages an interesting *and* central programming concept by extending their common use as silos of data with the ability for *users* to *mechanically* derive related ideas (programming constructs) as well as the relationships between them.

The framework developed in this thesis is motivated by the following concerns when developing libraries in the dependently-typed language (DTL) Agda, such as [Kah18].

1. **Practical$_1$: Renaming** There is excessive repetition in the simplest of tasks when working with packages; e.g., to *uniformly* decorate the names in a package with subscripts $_0$, $_1$, $_2$ requires the package's contents be listed thrice. It would be more economical to *apply* a renaming *function* to a package.

2. **Practical$_2$: Unbundling** In general, in a DTL, *packages behave like functions* in that they may have a subset of their contents designated as *parameters exposed at the type-level* which users can *instantiate*. Unfortunately, library developers generally provide only a few *variations* on *a* package; such as having no parameters or having only *functional symbols* as parameters —c.f., the carrier `C` and operation $\oplus$ in figure 1. Whereas functions can *bundle-up* or *unbundle* their parameters using currying and

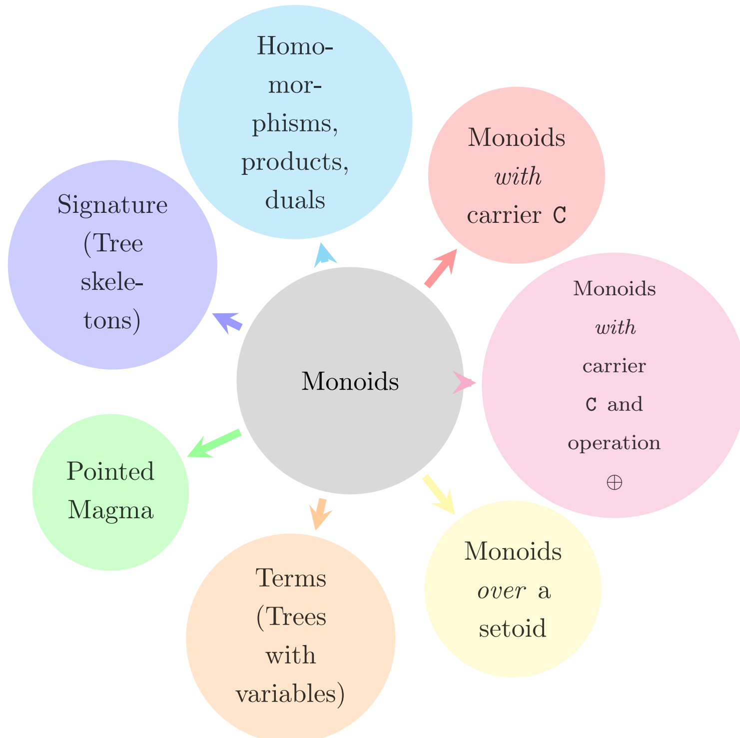


Figure 1.1: Deriving related *types* from *the* definition of monoids

uncurrying, only the latter is generally supported and, even then, not in an elegant fashion. Rather than provide *several variations* on a package, it would be more economical to provide one singular fully-bundled package and have an operator that allows users to *declaratively*, "on the fly", expose package constituents as parameters.

3. **Theoretical$_1$: Exceptionality** DTLs blur the distinguish between expressions and types, treating them as the same thing: *Terms*. This collapses a number of seemingly different language constructs into the same thing —e.g., programs and proofs are essentially the same thing. Unfortunately, packages are treated as *exceptional* values that differ from *usual* values —such as functions and numbers— in that the former are 'second-class citizens' which only serve to collect the latter 'first-class citizens'. This forces users to learn two families of 'sub-languages' —one for each citizen class. There is essentially no *theoretical* reason why packages do not deserve first-class citizenship, and so receive the same treatment as other *unexceptional* values. Another advantage of giving packages equal treatment is that we are inexorably led to wonder what **computable algebraic structure** they have and how they relate to other constructs in a language; e.g., packages are essentially record-valued functions.

4. **Theoretical$_2$: Syntax** It is well known that sequences of declarations may be grouped together within a *package*. If any declarations are opaque, not fully undefined, they become *parameters* of the package —which may then be identified as a *record type* with the opaque declarations called *fields*. However, when a declaration is *intentionally*

opaque not because it is missing an implementation, but rather it acts as a value construction itself then one uses *algebraic data types*, or 'termtypes'. Such types share the general structure of a package, and so it would be interesting to illuminate the exact difference between the concepts —*if any*. In practice, one forms a record type to model an interface, instances of which are actual implementations, and forms an *associated* termtype to *describe computations* over that record type, thereby making available a syntactic treatment of the interface —textual substitution, simplification / optimisation, evaluators, canonical forms. For example, as shown in figure 1, the record type of monoids models composition whereas the (tremendously useful) termtype of binary trees acts as a description language for monoids. The *problem of maintenance* now arises: Whenever the record type is altered, one must mechanically update the associated termtype. It would be more economical to extract *both* record types and termtypes from a single package declaration.

In this thesis, we aim to mitigate the above concerns with a focus on **practicality**. A theoretical framework may address the concerns, but it would be incapable of accommodating *real-world use-cases* when it cannot be applied to real-world code. For instance, one may speak of 'amalgamating packages', which can always "be made disjoint", but in practice the union of two packages would likely result in name clashes which could be avoided in a number of ways but the *user-defined names* are important and so a result that is "unique up to isomorphism" is not practical. As such, we will implement a framework to show that the above concerns can be addressed in a way that **actually works**.

1.1 Thesis Overview

The remainder of the thesis is organised as follows.

- ◇ Chapter 2 consists of preliminaries, to make the thesis self-contained, and contributions of the thesis.

  A review of dependently-typed programming with Agda is presented, with a focus on its packaging constructs: Namespacing with `module`, record types with `record`, and as contexts with Σ-padding. The interdefinability of the aforementioned three packaging constructs is demonstrated. After-which is a quick review of other DTLs that shows the idea of a unified notion of package is promising —Agda is only a presentation language, but the ideas transfer to other DTLs.

  With sufficient preliminaries reviewed, the reader is in a position to appreciate a survey of package systems in DTLs and the contributions of this thesis. The contributions listed will then act as a guide for the remainder of the thesis.

- ◇ Chapter 3 consists of real world examples of problems encountered with the existing package system of Agda.

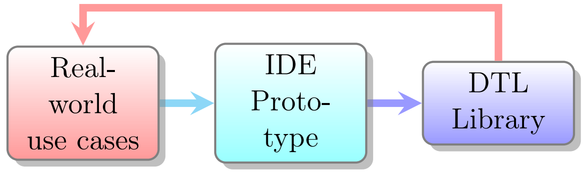


Figure 1.2: Approach for a **practical** framework

Along the way, we identify a set of *DTL design patterns* that users repeatedly implement. An indicator of the **practicality** of our resulting framework is the ability to actually implement such patterns as library methods.

- ◇ Chapter 4 discusses a prototype that addresses *nearly* all of our concerns.

  Unfortunately, the prototype introduces a new sublanguage for users to learn. Packages are *nearly* first-class citizens: Their manipulation must be specified in Lisp rather than in the host language, Agda. However, the ability to rapidly, textually, manipulate a package makes the prototype an extremely useful tool to test ideas and implementations of package combinators. In particular, the aforementioned example of forming unions of packages is implemented in such a way that the amount of input required —such as *along* what interface should a given pair of packages be *glued* and *how* name clashes should be handled— can be 'inferred' when not provided by making use of Lisp's support for keyword arguments. Moreover, the union operation is a *user-defined* combinator: It is a *possible* implementation by a user of the prototype, built upon the prototype's "package meta-primitives".

- ◇ Chapter 5 takes the lessons learned from the prototype to show that *DTLs can have a unified package system within the host language.*

  The prototype is given semantics as Agda types and functions by forming a **practical** library within Agda that achieves the core features of the prototype. The switch to a DTL is nontrivial due to the type system; e.g., fresh names cannot be arbitrarily introduced nor can syntactic shuffling happen without a bit of overhead. The resulting library is both usable and practical, but lacks the immense power of the prototype due to the limitations of the existing implementation of Agda's metaprogramming facility.

  We conclude with the observation that ubiquitous data structures in computing arise *mechanically* as termtypes of simple 'mathematical theories' —i.e., packages.

- ◇ Chapter 6 concludes with a discussion about the results presented in the thesis.

The underlying motivation for the research is the conviction that packages play *the* crucial role for forming compound computations, subsuming *both* record types and termtypes. The approach followed is summarised in figure 1.1.

Chapter 2

Packages and Their Parts

The purpose of language is to communicate ideas that ‘live’ in our minds. In particular, written text captures ideas independently of the person who initially thought of them. To understand the idea *behind* a written sentence, people agree on **how** sentences may be organised and **what** content they denote from their parts. For example, in English, a sentence is considered ‘well-formed’ if it is in the order subject-verb-object —such as *“Jim ate the apple”*— and it is considered ‘meaningful’ if the subject and object are noun phrases that *denote things in the world that **could exist*** and the verb is a **possible action** by the subject on the object. For instance, in the previous example, there *could* be a person named *Jim* who *could* eat an apple, and so the sentence is meaningful. In contrast the phrase *“the colourless green apple kissed Jim”* is well-formed *but not* meaningful: The indicated action **could happen**, say, *in a world* of sentient apples; however, the subject —*the colourless green apple*— **cannot possibly exist** since a thing cannot be both lacking colour but also having colour at the same time. Moreover, *depending on who you ask*, the action of the previous example —*the [...] apple **kissed** Jim*—, may be ludicrous *on the basis* that kissing is ‘classified’ as a verb whose subject, in the ‘real’ world, has the ability to kiss. As such, ‘meaningfulness’ is not necessarily fixed, but may vary. Likewise, as there is no one universal language spoken by all people, written text is also not fixed but varies; e.g., a translation tool may convert an idea *captured in* Arabic to a related idea *captured in* French. It is with the observations that we will discuss the concepts required to have a formal theory of packages, as summarised in Figure 2.

Syntax	Written text; a sequence of symbols
Well-formed	Adherence to a particular organisation
Types	Classifications of the relationships between words
Semantics	An idea, or thing, “possible in some world”
Package	A language consisting of a vocabulary and sentences
Combinator	A translation of ideas in one language (package) into another

The contents of Table 2 may be intimidating to the uninitiated; so we reach for a gameplay based analogy to further make the concepts accessible.

Programming, as is the case with all of mathematics, is the manipulation of symbols according to specific *rules*. Moreover, like a game, when one plays —i.e., shuffles symbols around— one may interpret the game pieces and the actions to *denote* some meaning, such as reflecting aspects of the players or of reality. Many play because it is fun to do so; there are only pieces (mathematical symbols or *terms*) and rules to be followed, and nothing more. Complex games may involve a number of pieces (terms) which are classified by the *types* of roles they serve, and the rules of play allow us to make observations or *judgements* about them; such as, “in the stage Γ of the game, game piece x serves the role τ” and this is denoted $\Gamma \vdash x : \tau$ mathematically. Games which allow such observations are called *type theories* in mathematics. When games are played, they may override concepts in reality; e.g., in Chess, the phrase *Knight’s move* refers to a particular set of possible plays and has nothing to do with knights in the real-world. As such, one calls the collection of specific game words, and what they mean, within a game (*type theory*) the *object-language* and uses the phrase *meta-language* to refer to the ambient language of the real-world. As it happens, some games have localised interactions between players where the rules may be changed temporarily and so we have *games within games*, then the object-language of the main game becomes the meta-language of the inner game. The rules of the game are its *syntax* and what the game means is its *semantics*. To say that a game piece (term) denotes some idea **I**, we need to be able to *express* that idea which may only be possible in the meta-language; e.g., pieces in a mini-game within a game may themselves denote pieces within the primary game —more concretely, a game may require a roll of a die whose numbers *denote*, or *refer to*, players in the main game which are not expressible in the mini-game. A *model* of a game (type theory) is an interpretation of the game's pieces in way that the rules are true under the interpretation.

Consider the following real-world examples. First, suppose you have a machine whose actions you cannot see, but you have a control panel before you that shows a starting screen, `start`, and the panel has one button, `next`, that forces the machine to act which updates the screen. Moreover, there is a screen capture called `thrice` *which happens* to be the result of pressing `next` three times after starting the machine. Second, suppose you are an artist mixing colours together.

A dynamical system – Machine

```
State  : Type
start  : State
next   : State → State
thrice : State
thrice = next (next (next start))
```

A dynamical system – Colours

```
Colour : Type
red    : Colour
green  : Colour
blue   : Colour
mix    : Colour × Colour → Colour
violet : Colour
violet = mix green blue
dark   : Colour → Colour
dark c = mix c blue
```

Each of these is a **package**: A sequence of 'declarations' of operations; wherein elements may be 'parameters' in the declarations of others. A **declaration** is a "name : classification" pair of words, *optionally* with another "name = definition" pair of words that shows how the new word *name* can be obtained from the vocabulary already declared thus far. For example, in these packages (languages) `thrice` and `violet` are aliases for expressions (sentences) constructed from other words. A **parameter** —also known as a **field**— is a declaration that is not an alias; i.e., it has no associated =-pair. Parameters are essentially the building blocks of a language; they cannot be expressed in terms of other words. A non-parameter is essentially *fully defined, implemented,* as an alias of a mixture of earlier words; whereas parameters are 'opaque' —*not yet implemented*. In particular, in the colours example above, `dark` *defines* a function that uses the *symbolic name* `mix` in its definition. There is an important subtlety between `mix` and `dark`: The latter, `dark`, is an *actual function* that is fully determined when an *implementation* of the *symbolic name* `mix` is provided. The (parameter) name `mix` is said to be a *function symbol* rather than a function: It is the *name* of a function, but it lacks any implementation and is thus not actually a function. A *function symbol* is to a function, like a name is to a person: Your name does not fully determine who you are as a person.

This sections aims to present a mathematical formalisation of packages. For brevity, we only consider parameters in the first few sections then accommodate non-parameters after a working definition is established. As discussed in the introduction, there are a number of 'sub-languages' one must be familiar with in any setting —e.g., function symbols and types (classifications) and their respective operations— and so a prime goal of our discussions will be to *reduce* the number of distinctions so that we have a *uniform* approach to different aspects of a language. The goals of the subsections are as follows.

◇ Provide a formalism of the above `Colour` package.

1. **What is a language?** Sketch out the English sentences example from above, introducing the notation used for declaring grammars of languages, along with typing contexts.
2. **Signatures** Attempt to extrapolate the key ideas of the previous section; concluding with a a discussion of when contexts constitute packages.
3. **Presentations of Signatures —Π and Σ** The desire to present packages (signatures) *practically* in a uniform notation leads to types that *vary* according to other types and so the constructor Π; then the **(un)bundling problem** is used to motivate the introduction of the Σ type constructor.
4. **Permitting Optional Definitions** Round-up the discovery of a formal definition of packages by returning to the `Colour` example above.
5. **The Definition of *Generalised Signatures*** Summarise the final definition of packages as generalised signatures; a theory related to *sketches*.

◇ Demonstrate the interdefinability of structuring mechanisms.

6. **A Whirlwind Tour of Agda** Tersely review the Agda language as a tool supporting the ideas of the previous subsections. In particular, the usual structuring mechanisms found in most settings are discussed —they are records, namespacing modules, and "algebraic datatypes" (grammars in a new setting).
7. **Facets of Structuring Mechanisms** Demonstrate three possible ways to define monoids in Agda and argue their equivalence; thereby, showing that structuring mechanisms are in effect accomplishing the same goal in different ways: They package data along with a particular *usage interface*. As such, it is not unreasonable to seek out a unified notion of **package** —namely, the aforementioned generalised signatures.

◇ Take inspiration from how other DTLs handle packages.

8. **Contexts are Promising** Discuss how other dependently-typed languages (DTLs) view contexts and signatures.
9. **Coq Modules as Generalised Signatures** Argue that the notion of generalised signature is promising as the underlying formal definition of packages.

◇ Contributions of the thesis.

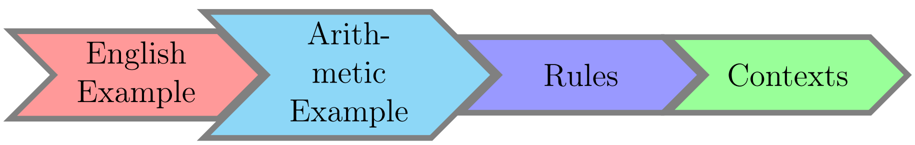
10. What is the primary problem the thesis aims to address.
11. What are the outcomes of the thesis effort.

```
Subject  ::= Jim | He | Apple
Verb     ::= Ate | Kissed
Object   ::= The Subject | Subject
Sentence ::= Subject Verb Object
```

Figure 2.1: Madlips Grammar

2.1 What is a language?

In this section, we introduce two languages in preparation for the terminology and ideas of the next section. The first language, *Madlips*, will only be discussed briefly and is mentioned due to its inherit accessibility, thereby avoiding unnecessary domain specific clutter and making definitions clearer. The plan for this section is summarised in the following diagram.



Madlips[1] Simple English sentences have the form subject-verb-object such as *"Jim ate the apple"*. To *mindlessly* produce such sentences, one must produce a subject, then a verb, then an object —all from given lists of possibilities. A convenient notation to describe a language is its *grammar* [Cho59a; Cho59b] presented in *Backus-Naur Form* [CCH73; GDF02; Lar+11; Knu64] as in Figure 2.1.

The notation τ `::=` $\texttt{c}_0$ `|` $\texttt{c}_1$ `|` … `|` $\texttt{c}_n$ defines the name τ as an alias for the collection of words —also called *strings* or *constructors*— $\texttt{c}_0$ or $\texttt{c}_1$ or … or $\texttt{c}_n$; that is the bar '|' is read 'or'. The name τ is also known as a *syntactic category*. For example, in the Madlips grammar, `Subject` is the name of the collection of words *Jim, He,* and *Apple*. A constructor may be followed by words of another collection, which are called *the arguments of the constructor*. For example, the `Object` collection above has a 'The' constructor which must be followed by a word of the `Subject` collection; e.g, `The Apple` is a valid *value* of the `Object` collection, whereas `The` is just an incomplete construction of `Object` words. The last clause of `Object` is just `Subject`: An invisible (unwritten) constructor that takes a value of `Subject` as its argument; e.g., `He` and all other values of `Subject` are also values of the `Object` collection. Similarly, the `Sentence` collection consists of one invisible (unwritten) constructor that takes 3 arguments —a subject, a verb, and an object. Below is an example *derivation* of a *sentence* in the *language generated by this grammar*; at each '$\to$' step, one of the collection names is replaced by one of its constructors until there are no more possible replacements.

[1]This is a collection of English sentences that may result from the *lips* of a person who is *mad*. Example phrases include `He Ate The Apple, He Ate Jim,` and `Apple Kissed The Jim` —whereas the first is reasonable, the second is worrisome, and the final phrase is confusing.

Example Derivation

```
  Sentence
→ Subject Verb Object
→ Jim     Verb Object
→ Jim     Ate  Object
→ Jim     Ate  The Subject
→ Jim     Ate  The Apple
```

Similarly, one may form `He Kissed Jim` as well as the meaningless sentence `Apple Kissed He`.

- ◇ The first is vague, the pronoun 'He' does not designate a known person but instead "stands in" for a *variable*, yet unknown, person. As such, the first sentence can be assigned a meaning once we have a *context* of which pronouns refer to which people.
- ◇ The second just doesn't make sense. Sometimes nonsensical sentences can be avoided by restructuring the grammar, say, by introducing auxiliary syntactic categories. A more general solution is to introduce *judgement rules* that characterise the subset of sentences that are sensible.

We will return to the notions of *context* and *judgement* after the next example language.

Freshmen Introductory computing classes are generally interested in arithmetic that involves both numeric and truth values —also known as *Boolean values*. We can capture some of their ideas with the following grammar.

Freshmen Grammar

```
Term ::= Zero | Succ Term | Term + Term | True | False | Term ≈ Term
```

- ◇ Unlike the previous grammar, instead of `+ Term Term` to declare a constructor '+' that takes two `Term` values, we write the operation `_+_` *infix*[2], in the middle, since that is a common convention for such an operation. Likewise, `Term ≈ Term` specifies a constructor `_≈_` that takes two term values.

Example terms include the numbers `Zero, Succ Zero,` and `Succ Succ Zero` —which denote 0, 1 (the successor of zero), and 2 (the successor of the successor of zero). The sensible Booleans terms `True ≈ False` and `True` are also possible —regardless of *how true*

[2]It is common to use underscores "_" to denote the *position* of arguments to constructions that do not appear first in a term. For example, one writes `if_then_else_` to indicate that we have a construction that takes *three* arguments, as indicated by the number of underscores; whence in a term such as `if` x `then` y `else` z it is understood that we have the construction `if_then_else_` applied to the arguments x, y, and z.

they may be. However, the nonsensical terms `True + False` and `Zero ≈ True` are also possible. As mentioned earlier, judgement rules can be used to characterise the sensible terms: The relationship "term t is an element of kind τ", written `t` : τ is defined by (1) introducing a new syntactic category (called "types") to 'tag' terms with the kind of elements they denote, and (2) declaring the conditions under which the relationship is true.

Types for Freshmen

```
Type ::= Number | Boolean
```

$$\frac{}{\texttt{Zero} : \texttt{Number}} \qquad \frac{t : \texttt{Number}}{\texttt{Succ}\, t : \texttt{Number}} \qquad \frac{s : \texttt{Number} \quad t : \texttt{Number}}{s + t : \texttt{Number}} \qquad \frac{}{\texttt{True} : \texttt{Boolean}}$$

$$\frac{}{\texttt{False} : \texttt{Boolean}} \qquad \frac{s : \texttt{Number} \quad t : \texttt{Number}}{s \approx t : \texttt{Boolean}} \qquad \frac{s : \texttt{Boolean} \quad t : \texttt{Boolean}}{s \approx t : \texttt{Boolean}}$$

A rule $\frac{\textit{premises}}{\textit{conclusion}}$ means "if the top parts are all true, then the bottom part is also true"; some rules have no premises and are their conclusions are unconditionally true. That these are *judgement rules* means that a particular instance of the relationship `t` : τ is true if and only if it is the conclusion of 'repeatedly stacking' these rules on each other. For example, below we have a *derivation tree* that allows us to conclude the sentence `Zero ≈ Succ Zero` is a Boolean term —regardless of *how true* the equality may be. Such trees are both read and written from the *bottom to the top*, where each horizontal line is an invocation of one of the judgement rules from above, until there are no more possible rules to apply.

$$\dfrac{\dfrac{}{\texttt{Zero} : \texttt{Number}} \qquad \dfrac{\dfrac{}{\texttt{Zero} : \texttt{Number}}}{\texttt{Succ}\,\texttt{Zero} : \texttt{Number}}}{\texttt{Zero} \approx (\texttt{Succ}\,\texttt{Zero}) : \texttt{Boolean}}$$

This solves the problem of nonsensical terms; for example, `True + Zero` *cannot be assigned* a type since the judgement rule involving `+` requires both its arguments to be numbers. As such, **consideration is moved from raw terms, to typeable terms.** The types can be interpreted as *well-definedness constraints* on the constructions of terms. Alternatively, types can be considered as **abstract interpreters** in that, say, we may not know the exact *value* of `s + t` but we know that it is a `Number` *provided* both `s` and `t` are numbers; whereas we know nothing about `Zero + False`.

Concept	Intended Interpretation
type	a collection of things
term	a particular one of those things
$x : \tau$	the declaration that x is indeed within collection τ

There is one remaining ingredient we have yet to transfer over from the Madlips setting: Pronouns, or *variables*, which "stand in" for "yet unknown" values of a particular type. Since a variable, say, x, is a stand-in value, a term such as x `+ Zero` has the `Number` type *provided* the variable x is known, in a *context*, to be of type `Number` as well. As such, in the presence of variables, the typing relation `_:_` must be extended to, say, `_⊢_:_` so that we have **typed terms in a context**.

$$\Gamma \vdash t : \tau \qquad \equiv \qquad \text{"}\textit{In the context } \Gamma\textit{, term } t \textit{ has type } \tau\text{"}$$

A *context*, denoted Γ, is simply a list of associations: In Madlips, a context associates pronouns with the names of people they refer to; in Freshmen, a context associates variables with their types. For example, $\Gamma : \texttt{Variable} \to \texttt{Type}; \Gamma(x) = \texttt{Number}$ associates the `Number` type to every variable. In general, a context only needs to mention the pronouns (variables) used in a sentence (term) for the sentence (term) to be understood, and so it may be **presented** as a set of pairs $\Gamma = \{(x_1, \tau_1), \ldots, (x_n, \tau_n)\}$ *with* the understanding that $\Gamma(x_i) = \tau_i$. However, since we want to *treat* each association (x_i, τ_i) as saying "x_i has type τ_i", it is common to present the **tuples** in the form $x_i : \tau_i$ —that is, the colon ':' is **overloaded** for denoting tuples in contexts and for denoting typing relationships.

Extending Freshmen with Variables

```
Term     ::= ··· | Variable
Variable ::= x | y | z
```

We have one new rule to type variables, which makes use of the underlying context.

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

All previous rules now must now additionally keep track of the context; e.g., the `'+'` rule becomes:

$$\frac{\Gamma \vdash s : \texttt{Number} \quad \Gamma \vdash t : \texttt{Number}}{\Gamma \vdash s \texttt{ + } t : \texttt{Number}}$$

We may now derive x `: Number ⊢` x `+ Zero : Number` but cannot complete the senseless phrase x `: Boolean ⊢` x `+ Zero : ???`. *That is, the same terms may be typeable in some contexts but not in others.*

Before we move on, it is interesting to note that contexts can themselves be presented with a grammar —as shown below, where constructors ',' and ':' each take two arguments and are written infix; i.e., instead of the usual `,` $\texttt{arg}_1$ $\texttt{arg}_1$ we write $\texttt{arg}_1$ `,` $\texttt{arg}_2$. Contexts are *well-formed* when variables are associated at most one type; i.e., when contexts *represent* 'partial functions'.

Grammar for Contexts

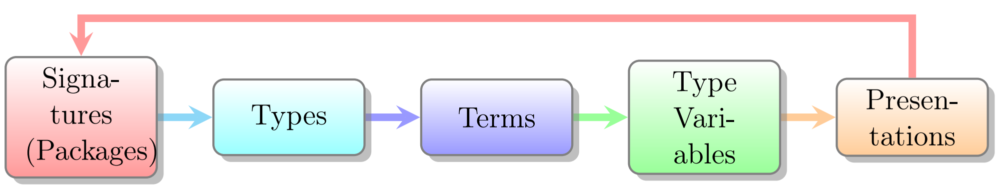
```
Context     ::= ∅ | Association, Context
Association ::= Variable : Type
```

Finally, it is interesting to observe that the addition of variables results in a an interesting correspondence: **Terms in context are functions of their variables**. More precisely, if there is a method $[\![\_]\!]$ that *interprets* type names τ as actual sets $[\![\tau]\!]$ and terms $\texttt{t} : \tau$ as *values* of those sets $[\![\texttt{t}]\!] : [\![\tau]\!]$, then a **term** in context $\texttt{x}_1 : \tau_1\texttt{,}\ \ldots\texttt{,}\ \texttt{x}_n : \tau_n \vdash \texttt{t} : \tau$ corresponds to the **function** $f : [\![\tau_1]\!] \times \cdots \times [\![\tau_n]\!] \to [\![\tau]\!]; f(x_1, \ldots, x_n) = [\![t]\!]$. *That is, terms in context model parameterisation* ***without*** *speaking of sets and functions.* (Conversely, *functions* $A \to B$ "are" *elements* of B *in a context* A.)

As mentioned in the introduction, we want to treat packages as the central structure for compound computations. To this aim, we have the approximation: **Parameterised packages are terms in context.**

2.2 Signatures

The languages of the previous section can be organised into *signatures*, which define interfaces in computing since they consist of the *names* of the types of data as well as the *names* of operations on the types —there are only symbolic names, not implementations. The purpose of this section is to organise the ideas presented in the previous section —shown again in the figure below— in a refinement-style so that the resulting formal definition permits the presentation of packages given in the first subsection above.



Signatures are tuples $\Sigma = (\mathcal{S},\ \mathcal{F},\ src,\ tgt)$ consisting of

- a set $\mathcal{S}$ of *sorts* —the names of types—,
- a set $\mathcal{F}$ of *function symbols*, and
- two mappings $\texttt{src} : \mathcal{F} \to \texttt{List}\,\mathcal{S}$ and $\texttt{tgt} : \mathcal{F} \to \mathcal{S}$ that associate a list[3] of *source sorts* and a *target sort* with a given function symbol.

Unary Signatures have only one source sort for each function symbol —i.e., the length of $\texttt{src}\ f$ is always 1— and so are just graphs. The ontology is captured in Figure 2.2.

[3] We write `List X` for the type of lists with values from `X`. The empty list is written `[]` and $\texttt{[x}_1\texttt{, x}_2\texttt{, ...,}$ $\texttt{x}_n\texttt{]}$ denotes the list of n elements $\texttt{x}_i$ from `X`; one says n is the *length* of the list.

Signatures	$\approx$	Graphs
Sorts		Nodes, Vertices
Function symbols		Edges, Tentacles

$$\frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau} \qquad \frac{\Gamma \vdash t_1 : \tau_n \quad \ldots \quad \Gamma \vdash t_n : \tau_n \qquad f : \tau_1 \times \cdots \times \tau_n \to \tau}{\Gamma \vdash \mathtt{f}\, t_1\, t_2\, \ldots\, t_n : \tau}$$

Typing the symbols of a signature as follows[4] lets us treat signatures as general forms of 'type theories' since we may speak of 'typed terms'.

$$f : s_1 \times \cdots \times s_n \to t \qquad \equiv \qquad \mathtt{src}\, f = [s_1, \ldots, s_n] \;\wedge\; \mathtt{tgt}\, f = t$$

Moreover, we regain the *typing judgements* of the previous section by introducing a grammar for *terms* which the above typing relation —i.e., `_⊢_:_` is definable using the above definition of ':'. Given a set $\mathcal{V}$ of **variables**, we may define **terms** with the following grammar.

Grammar for Arbitrary Terms

```
Term ::= x               {- A variable; an element of 𝒱            -}
       | f t₁ t₂ ... tₙ  {- A function symbol f of ℱ taking n sorts
                            where each tᵢ is a Term                -}
```

As discussed in the previous section, variables are *not* necessary and if they are *not* permitted, we omit the first clause of `Term` and only use the second typing rule —we also drop the contexts since there would be no variables for which variable-type associations must be remembered. Without variables, the resulting terms are called *ground terms*. Since terms are defined recursively, inductively, the set of ground terms is non-empty precisely when at least one function symbol `c` needs no arguments, in which case we say `c` is a *constant symbol* and make the following abbreviation:

$$c : \tau \qquad \equiv \qquad \mathtt{src}\, c = [] \;\wedge\; \mathtt{tgt}\, c = \tau$$

Alternatively, the abbreviation $\tau_1 \times \cdots \times \tau_n \to \tau$ is written as just τ *when* $n = 0$.

How do we actually **present** a signature?

Brute force Recall the Freshmen language, we can present an *approximation*[5] of it as signature by providing the necessary components $\mathcal{S}$, $\mathcal{F}$, `src`, and `tgt` with

```
𝒮 = {Number, Boolean}
ℱ = {Zero, Succ, Plus, True, False, Equal}
```

[4] The wedge symbol '$\wedge$' is read "and"; e.g., $p \wedge q$ is read "*p and q are true*".

[5] This is an approximation since we have constrained the equality construction, '$\approx$', to take *only* numeric arguments; whereas the original Freshmen allowed both numbers and Booleans as arguments to equality *provided* the arguments have the *same type*. We shall return to this issue later when discussing *type variables*.

op	`Zero`	`Succ`	`True`	`False`	`_+_`	`_≈_`
`src` op	`[]`	`[Number]`	`[]`	`[]`	`[Number, Number]`	`[Number, Number]`
`tgt` op	`Number`	`Number`	`Boolean`	`Boolean`	`Number`	`Boolean`

This is however rather **clumsy** and not that clear. We may collapse the `src, tgt` definitions into the `_:_→_` relation defined above; i.e., replacing *two* definition declarations `src Zero = []` $\land$ `tgt Zero = Number` by *one* definition declaration `Zero : Number`. However, function symbol names are still repeated twice: Once in the definition of $\mathcal{F}$ and once in the definition of `_:_→_`; the latter mentions all the names of $\mathcal{F}$ and so $\mathcal{F}$ may be inferred from the typing relationship. We are left with two declarations: The sorts $\mathcal{S}$ and the typing declarations. However, the set $\mathcal{S}$ only serves to declare its elements as sort symbols; if we use the relationship `_: Type` defined by τ `: Type` $\equiv \tau \in \mathcal{S}$, then the sort symbols can also be introduced by seemingly similar 'typing declarations'. With this approach, Freshmen can be introduced more naturally[6] as follows.

Freshmen as a Generalised Signature

```
Number  : Type
Boolean : Type

Zero : Number
Succ : Number → Number
Plus : Number × Number → Number

True  : Boolean
False : Boolean
Equal : Number × Number → Boolean
```

What a twist: **Generalised signatures are contexts!** That is, a sequence of name-type associations. More precisely, with the relation `package_` defined below, we can characterise packages as the contexts whose earlier elements allow their later elements to be typeable. For example, the context `S : Type; x : S` can be proven to be package whereas the context `S : Type; x : Q` cannot —it has the 'global name' Q.

$$\frac{}{\texttt{package}\,\emptyset} \qquad \frac{\texttt{package}\,\Gamma \qquad \tau \in \mathit{Name}}{\texttt{package}\,(\Gamma, \tau : \texttt{Type})}$$

$$\frac{\text{For } i : 1..n+1, \Gamma \vdash \tau_i : \texttt{Type} \qquad f \in \mathit{Name} \qquad \texttt{package}\,\Gamma}{\texttt{package}\,(\Gamma, f : \tau_1 \times \cdots \times \tau_n \to \tau_{n+1})}$$

Of-course these rules require contexts to be well-formed: Names are declared at most once in a context. Below is an example derivation demonstrating that the context $\mathcal{N}$ `: Type,`

[6] It is important to note that there are three relations here with ':' in their name —`_:Type`, `_:_→_`, and `_:_` for constant-typing. See Table ??.

$\mathcal{B}$: `Type`, `z` : $\mathcal{N}$, `s` : $\mathcal{N} \to \mathcal{N}$ (an initial segment of Freshmen) is actually a package by taking $Name = \{\mathcal{N}, \mathcal{B}, s, z\}$.

$$\dfrac{\dfrac{}{\emptyset, \mathcal{N} : \mathtt{Type}, \mathcal{B} : \mathtt{Type}, z : \mathcal{N} \vdash \mathcal{N} : \mathtt{Type}} \qquad \dfrac{}{s \in Name} \qquad \dfrac{\dfrac{}{\emptyset, \mathcal{N} : \mathtt{Type}, \mathcal{B} : \mathtt{Type} \vdash \mathcal{N} : \mathtt{Type}} \quad \dfrac{}{z \in Name} \quad \dfrac{\dfrac{\dfrac{}{\mathsf{package}\ \emptyset}}{\mathsf{package}\ (\emptyset, \mathcal{N} : \mathtt{Type})}}{\mathsf{package}\ (\emptyset, \mathcal{N} : \mathtt{Type}, \mathcal{B} : \mathtt{Type})}}{\mathsf{package}\ (\emptyset, \mathcal{N} : \mathtt{Type}, \mathcal{B} : \mathtt{Type}, z : \mathcal{N})}}{\mathsf{package}\ (\emptyset, \mathcal{N} : \mathtt{Type}, \mathcal{B} : \mathtt{Type}, z : \mathcal{N}, s : \mathcal{N} \to \mathcal{N})}$$

It is important to pause and realise that there are **three relations with ':' in their name** —which may include spaces as part of their names.

Function symbol to sort *adjacency*	$f : s_1 \times \cdots \times s_n \to t$	$\equiv$	`src f = [`s_1`, ..., `s_n`]` $\wedge$ `tgt f = t`
Sort symbol *membership*	$s : \text{Type}$	$\equiv$	`s` $\in \mathcal{S}$
Pair formation within contexts Γ	$x : t$	$\equiv$	`(x , t)`

Table 2.1: Three "typing" relations

Consequently, we have stumbled upon a grammar `TYPE` for types —called the *types for signature* Σ over a collection of names $\mathcal{V}$.

Induced Grammar for Types

```
TYPE ::= Type              {- An opaque symbol; "the type of types" -}
       | τ                 {- τ is a sort symbol; a value of 𝒮 -}
       | x                 {- A variable; an element of 𝒱 -}
       | TYPE → TYPE        {- '→' takes two TYPE arguments -}
       | TYPE × TYPE |  𝟙 {-- "product types" -}
```

Where the type $\mathbb{1}$ is used for constants: With this grammar a constant $c : \tau$ would have type `c` : $\mathbb{1} \to \tau$. The symbol $\mathbb{1}$ is used simply to indicate that the function symbol `c` takes no arguments. The introduction of $\mathbb{1}$ saves us from having to include the constant-typing relationship defined above —namely, `c` : τ $\equiv$ `src c = []` $\wedge$ `tgt c =` τ.

We may now form types $\alpha \to \beta$ and $\alpha \times \beta$ but there is no way for the type β to depend on the type α. In particular, recall that in Freshmen we wanted to have `s` $\approx$ `t` to be a well-formed term of type `Boolean` *provided* `s` and `t` have the *same* type, either `Number` or `Boolean`. That is, '_≈_' wants to have *both* `Number` $\times$ `Number` $\to$ `Boolean` *and* `Boolean` $\times$ `Boolean` $\to$ `Boolean` as types —since it is reasonable to compare either numbers of truth values for equality. But a function symbol can have only *one* type —since `src` and `tgt` are (deterministic) functions. If we had access to variables which stand-in for types, we could type equality as α $\times$ α $\to$ `Boolean` *for any type* α.

$$\dfrac{}{\alpha : \mathtt{Type} \quad \vdash \quad \_ \approx \_ : \alpha \times \alpha \to \mathtt{Boolean}}$$

Even though types *constrain* terms, there seems to be a subtle repetition: The `TYPE` grammar resembles the `Term` grammar. In fact, if we pretend `Type`, $\mathbb{1}$, $\times$, $\to$ *are* function symbols, then `TYPE` is subsumed by `Term`. Hence, we may conflate the two into one declaration —a concern which we will return to at a later time.

2.3 Presentations of Signatures —Π and Σ

Since a signature's types also have a grammar, we can present a signature in the natural style of "name : type-term" pairs. That is, a signature may be presented as a context; i.e., sequence of declarations δ_0; δ_1; ...; δ_n *such that* each δ_i is of the form $\mathtt{name}_i$: $\mathtt{type}_i$ where $name_i$ are unique names but $type_i$ are terms from the `TYPE` grammar. For example, the above presentation of Freshmen is a context from which we regain a signature $\Sigma = (\mathcal{S}, \mathcal{F}, src, tgt)$ where:

- $\mathcal{S}$ is all of the $name_i$ where $type_i$ is `Type`;
- $\mathcal{F}$ is the remaining $name_i$ symbols;
- `src, tgt` are defined by the following equations, where the right side, involving `_:_→_` and `_:_`, are given in the context of δ_i.

  $$\begin{array}{llll} \mathtt{src}\, f = [\tau_1, \ldots, \tau_n] & \wedge \quad \mathtt{tgt}\, f = \tau & \equiv & f : \tau_1 \times \cdots \times \tau_n \to \tau \\ \mathtt{src}\, f = [] & \wedge \quad \mathtt{tgt}\, f = \tau & \equiv & f : \tau \end{array}$$

  These equations ensure `src, tgt` are functions *provided* each name occurs at most once as the name part of a declaration.

This is one of the first instances of a syntax-semantics relationship: **A context is a syntactic representation of a (generalised) signature**. However, with a bit of experimentation one quickly finds that the syntax is "too powerful": There are contexts that do *not* denote signatures. Consider the following grammar which models 'smart' people and their phone numbers. Observe that the 'smartness' of a person *varies* according to their location; for example, in, say, a school setting we have 'book smart' people whereas in the city we have 'street smart' people and, say, in front of a television we have 'no smart' people. Moreover, the function symbol `call` for obtaining the phone number of a 'smart person' must necessarily have a variable that accounts for how the smart type *depends* on location. However, if variables are not permitted, then `call` cannot have a type which is unreasonable. It is a well-defined context, but it does not denote a signature.

Calling-smart-people Grammar

```
Location : Type

School   : Location
Street   : Location
TV       : Location

Smart    : Location → Type

Phone    : Type
call     : Smart α → Phone   -- A variable?!
```

The first problem, the type of `Smart`, is easily rectified: The sorts $\mathcal{S}$ are now *all* names in the context that *conclude* with `Type` or that *conclude* with some τ that has type `Type`. Sorts now may *vary* or *depend* on other sorts.

The second problem, the type of `call`, requires the introduction of a new[7] type operation. The operation $\Pi\_:\_\bullet\_$ will permit us to type operations that have variables in their types even when there is no variable collection $\mathcal{V}$.

Dependent Function Type

$$\Pi\, a : A \;\bullet\; B\, a \qquad \equiv \qquad \text{“Values of } \textit{type } B\, a\text{, for each value } a \text{ of type } A\text{”}$$

An element of $\Pi\, a : A \bullet B\, a$ is a function f which assigns to each $a : A$ an element of $B\, a$. Such methods f are *choice functions*: For every a, there is a collection $B\, a$, and $f\, a$ picks out a particular b in a's associated collection.

The type of `call` is now Π ℓ `: Location •  (Smart` ℓ `→ Phone)`. That is, *given* any location ℓ, `call` ℓ specialises to a function symbol of type `Smart` ℓ `→ Phone`, then given any “smart person s in location ℓ”, `call` ℓ `s` would be their phone number. Interestingly, if s is a street-smart person then `call School s` is *ill-typed*: The type of `s` must be `Smart School` not `Smart Street`. Hence, later inputs may be constrained by earlier inputs. This is a new feature that simple signatures did not have.

Before extending the previous definition of signatures, there is a practical subtlety to consider. Suppose we want to talk about smart people *regardless* of their location, how would you express such a type? The type of `call : (`Π l `: Location • Smart` l `→ Phone)` reads: *After picking a particular location ℓ, you may get the phone numbers of the smart people at that location.* In particular, Π ℓ `: Location • Smart` ℓ is the type of smart people **at a**

[7]Those familiar with set theory may remark that dependent types are not *necessary* in the presence of power sets. Even though power sets are not present in our setting, dependent types provide a natural and elegant approach to *indexed types* in lieu of an encoding in terms of *families of sets or operations*. Moreover, an encoding *hides* essential features of an idea such as dual concepts: Σ and Π are ‘adjoint functors’. Even more surprising, working with Σ and Π leads one to interpret “propositions as types” with predicate logic quantifiers $\forall/\exists$ encoded via dependent types Π/Σ; whence the slogan “Programming $\approx$ Proving”.

particular location ℓ. Since, in this case, we do not care about locations, we would like to simply pick a person who is located **somewhere**. The ability to "bundle away" a varying feature of a type, instead of fixing it as a particular value, is known as the **(un)bundling problem**[8]. It is addressed by introducing a new[9] type operator $\Sigma\_:\_ \bullet \_$ —the symbol 'Σ' is conventionally used both for the name of signatures and for this new type operator.

$\Pi\ \ell$: `Location` $\bullet$ `Smart` ℓ	Pick a location, then pick a person
$\Sigma\ \ell$: `Location` $\bullet$ `Smart` ℓ	Pick a person, who is located *somewhere*
Π `a : A` $\bullet$ `B a`	Pick a value `a : A`, to get `B a` values
Σ `a : A` $\bullet$ `B a`	Values are pairs `(a, b)` with `a : A` and `b : B a`

Dependent Product Type

$\Sigma\, a : A \bullet B\, a \quad \equiv \quad$ "The type of pairs (a, b) where $a : A$ and b is a value of *type* $B\, a$"

An element of $\Sigma\, a : A \bullet B\, a$ is a pair (a, b) of an element $a : A$ along with an element $b : B\, a$. Such pairs are *tagged values*: We have values b which are 'tagged' by the collection-*index* a with which they are associated.

The type operator `_→_` did not accommodate dependence but Π does; indeed if B does not depend on values of type A, then $\Pi a : A \bullet B$ is just `A → B`. Likewise, Σ generalises `_×_`.

Abbreviations

Provided B is a type that does not vary,

$$\begin{aligned} A \to B \quad &\equiv \quad \Pi\, x : A \bullet B \\ A \times B \quad &\equiv \quad \Sigma\, x : A \bullet B \end{aligned}$$

Before returning to the task of defining signatures, let us present a number of examples to showcase the differences between dependent and non-dependent types.

1. Let `Birthday` : `Weekday` → `Type` denote the collection of all people who have a birthday on a given weekday. One says, `Birthday` *is the collection of all people,* ***indexed*** *by their birth day of the week.* Moreover, let `People` denote the collection of all people in the world.

   $\underline{\Pi\, d : \texttt{Weekday} \bullet \texttt{Birthday}\, d}$ is the type of *functions* that given any weekday d, yield a person whose birthday is on that weekday.

[8]The initiated may recognise this problem as identifying the relationship between *slice categories* $\mathcal{C}/A$ whose objects are A-indexed families and *arrow categories* $\mathcal{C}^{\to}$ whose objects are *all* the A-indexed families *for all* possible A. In particular, identifying the relationship between the categorial transformations $\_/A$ and $\_^{\to}$ —for which there is a non-full inclusion from the former to the latter, which we call "Σ-padding".

[9]The Σ-types denote disjoint unions and are sometimes written as $\coprod$ —the 'dual' symbol to Π.

Example functions in this type are f and g below...

```
f Monday  = Jim
f Tuesday = Alice

g Monday  = Mark
g Tuesday = Alice
```

... *provided* we live in a tiny world consisting of three people and only two weekdays.

Person	Birthday
Jim	Monday
Alice	Tuesday
Mark	Monday

In contrast, `Weekday` $\to$ `People` is the collection of functions associating people to weekdays —no constraints whatsoever. E.g., `f d = Jim` is the function that associates `Jim` to every weekday `d`.

$\underline{\Sigma\, d : \texttt{Weekday} \bullet \texttt{Birthday}\, d}$ is the type of *pairs* (d, p) of a weekday d and a person whose birthday is that weekday.

Below are two values of this type (✓) and a non-value (×). The third one is a pair (d, p) where d is the weekday `Tuesday` and so the p must be *some* person born on that day, and `Mark` is not such a person in our tiny world.

```
✓ (Monday, Jim)
✓ (Tuesday, Alice)
× (Tuesday, Mark)
```

In contrast, `Weekday` × `People` is the collection of pairs (w, p) of weekdays and people —no constraints whatsoever. E.g., `(Tuesday, Mark)` is a valid such value.

2. Let $\texttt{English}_{\leq n}$ denote the collection of all English worlds that have at most n letters; let `English` denote *all* English words.

   $\underline{\Pi\, n : \mathbb{N} \bullet \texttt{English}_{\leq n}}$ is the type of *functions* that given a length n, yield a word of that length. Below is part of a such a function `f`.

```
f 0 = ""   -- The empty word
f 1 = "a"  -- The indefinite article
f 2 = "to"
f 3 = "the"
f 4 = "more"
...
```

   In contrast, an $f : \mathbb{N} \to \texttt{English}$ is just a list of English words with the i-th element in the list being $f\, i$.

   $\underline{\Sigma\, n : \mathbb{N} \bullet \texttt{English}_{\leq n}}$ is the type of *values* (n, w) where n is a number and w is an English word of that length. E.g., `(5, "hello")` is an example such value; whereas `(2, "height")` is not since the length of `"height"` is *not* 2.

   In contrast, $\mathbb{N} \times$ `English` is any number-word pair, such as `(12, "hi")`.

   Notice that dependent types may ***encode properties*** *of values.*

3. (**"All errors are type errors"**) Suppose `get i xs` is the i-th element in a list `xs = [`x_0`, `x_1`, ..., `x_n`]`, what is the type of such a method `get`?

   Using `get : Lists → ℕ → Value` will allow us to write `get [`x_1`, `x_2`] 44` which makes no sense: There is no 44-th element in that 2-element list! Hence, the `get` operation must constrain its numeric argument to be at most the length of its list argument. That is, `get : (Π (xs : Lists) • ℕ< (length xs) → Value)` where `ℕ< n` is the collection of numbers less than n. *Now the previous call, `get [`x_1`, `x_2`] 44` does not need to make sense since it is /ill-typed*: The second argument does not match the required constraining type.

   In fact, when we speak of lists we implicitly have a notion of the kind of value type they contain. As such, we should write `List X` for the type of lists with elements drawn from type `X`. Then what is the type of `List`? It is simply `Type → Type`. With this form, `get` has the type `Π X : Type • Π xs : List X • ℕ< (length xs) → X`.

   Interestingly, lists of a particular length are known as *vectors*. The type of which is denoted `Vec X n`; this is a type that is *indexed* by *both* another *type* `X` and an *expression* `n`. Of-course `Vec : Type → ℕ → Type` and, with vectors, `get` may be typed `Π X : Type • Π n : ℕ • Vec X n → ℕ< n → X`; in-particular notice that the *external computation* `length xs` in the previous typing of `get` is replaced by the *intrinsic index* `n`; that is, **dependent types allow us to encode properties of elements at the type level!**

Anyhow, back to the task as hand —defining signatures (packages).

Given two collections of names $\mathcal{V}$ and $\mathcal{B}$ where each name in $\mathcal{B}$ has an associated *arity*, a number, we may form the collection of generalised terms as follows.

Generalised Terms

```
Term ::= x                -- A "variable"; a value of 𝒱
      | β t₁ t₂ ... tₙ   -- A "base symbol of arity n"; a value of ℬ
      | Π a : τ • τ'     -- For previously constructed types τ and τ'
      | Σ a : τ • τ'     --      and variable "a"
      | 𝟙                -- "unit type"
```

Since this collection constructs a number of different kinds of things:

- ◇ The term `Type` is usually called a ***kind***;
- ◇ the terms τ of type `Type` are called ***types***;
- ◇ all other terms, those `t : `τ for τ` : Type`, are called ***expressions***.

The rules below classify the well-formed generalised terms. The rules for Π and Σ show that they are *families* of types 'indexed' by the first type. The rules only allow the construction of types and variable values, to construct *values of types* we will need some starting base types, whence the upcoming definition.

$$\frac{}{\Gamma \;\vdash\; \mathtt{Type} : \mathtt{Type}}[\textsc{Type-in-Type}]$$

$$\frac{\Gamma(x) = \tau}{\Gamma \;\vdash\; x : \tau}[\textsc{Variables}] \qquad \frac{\Gamma, a : \tau \;\vdash\; \tau' : \mathtt{Type}}{\Gamma \vdash (\Pi\, a : \tau \bullet \tau') : \mathtt{Type}}[\textsc{Dependent Function Type}]$$

$$\frac{}{\Gamma \;\vdash\; \mathbb{1} : \mathtt{Type}}[\textsc{Unit Type}] \qquad \frac{\Gamma, a : \tau \;\vdash\; \tau' : \mathtt{Type}}{\Gamma \;\vdash\; (\Sigma a : \tau \bullet \tau') : \mathtt{Type}}[\textsc{Dependent Product Type}]$$

A **Generalised Signature** is a tuple *($\mathcal{B}$, arity, type)* where $\mathcal{B}$ = *[β_0, β_1, …, β_n]* is an *ordered* list of "base symbols", $\mathtt{arity} : \mathcal{B} \to \mathbb{N}$ associates a number to each base symbol, and $\mathtt{type} : \mathcal{B} \to \mathtt{Term}$ associates a generalised term to each base symbol such that $\Gamma_{k-1} \vdash \mathtt{type}\, \beta_k : \mathtt{Type}$ for each k *: 0..n*, where $\Gamma_k = (\beta_0 : \tau_0, \ldots, \beta_k : \tau_k)$ and $\tau_i = \mathtt{type}\, \beta_i$. That is `type` associates to each base symbol a type-term that is well-defined according to the typing rules above for generalised terms and *possibly* making use of previous symbols in the listing. We may now augment the above rule listing so that we can form well-typed *expressions* as well as *terms* using the symbols of $\mathcal{B}$ —for now we are ignoring Σ for brevity.

$$\frac{\mathtt{type}\, \beta \;=\; \tau}{\Gamma \;\vdash\; \beta : \tau}[\textsc{Base Symbol}]$$

$$\frac{\Gamma \;\vdash\; \beta : (\Pi\, x : \tau \bullet \tau') \qquad \Gamma \;\vdash\; t : \tau}{\Gamma \;\vdash\; \beta\, t \;:\; \tau'[x \coloneqq t]}[\textsc{Symbol Introduction}]$$

(The notation $E[x := F]$ means "replace every occurrence of the name x within term E by the term F.")

Crucially, generalised signatures may be presented as a sequence of "symbol : type" pairs where the symbols are unique names and each type is a generalised term. Below is an example similar to Calling-smart-people. In this example, `A` denotes a collection that each member `a : A` of which determines a collection `B a` which each have a 'selected point' `it a : B a`. More concretely, think of `A` as the countries in the world from which `B` are the households in each country, and `it` selects a representative member of a household `B a` for each country `a : A`.

Pointed Families

```
A  : Type
B  : A → Type
it : Π a : A • B a
```

This is a generalised signature *($\mathcal{B}$, arity, type)* where:

$\mathcal{B}$	`A`	`B`	`it`
`arity`	0	1	1
`type`	`Type`	`A → Type`	`Π a : A • B a`

The $\Gamma_{k-1} \;\vdash\; \mathtt{type}\;\; \beta_k \;:\; \mathtt{Type}$ obligations for this example become:

1. $\vdash$ `Type : Type`,
2. `A : Type` $\vdash$ `(A → Type) : Type`, and
3. `A : Type, B : A → Type` $\vdash$ `(Π a : A • B a) : Type`.

The first is just the TYPE-IN-TYPE rule, the second is a mixture of the ABBREVIATION and DEPENDENT FUNCTION TYPE rules; the third one is a mixture of the DEPENDENT FUNCTION TYPE and SYMBOL INTRODUCTION rules. Moreover, notice that `it a` is a valid term *provided* `a : A` as shown in the following derivation.

$$\dfrac{\dfrac{}{a : A \;\vdash\; \texttt{it} : (\Pi\, x : A \bullet Bx)}[\textsc{Base Symbol}] \qquad \dfrac{}{a : A \;\vdash\; a : A}[\textsc{Variables}]}{a : A \;\vdash\; \texttt{it}\, a : Ba}[\textsc{Symbol Introduction}]$$

Signatures are a staple of computing science since they formalise interfaces and generalise graphs and type theories. Our generalised signatures have been formalised "after the fact" from the creation of the prototype for packages. In the literature, our definition of generalised signatures is essentially a streamlined presentation of Cartmell's *Generalised Algebraic Theories* [Car86] expect that we do not allow arbitrary equational 'axioms' instead using "name = term" rather than "term = term" axioms which serve as *default implementations* of names. The notion of optional definitions is explored in the next section.

2.4 Permitting Optional Definitions

The examples packages from this chapter's introduction, one of which is shown below for convenience, can *almost* be understood as presentations of generalised signatures. What is lacking is the ability for *optional* definitions, as is the case with `violet` and `dark` below.

A dynamical system – Colours

```
Colour : Type
red    : Colour
green  : Colour
blue   : Colour
mix    : Colour × Colour → Colour
violet : Colour
violet = mix green blue
dark   : Colour → Colour
dark c = mix c blue
```

The first step in **amend** the definition of generalised signatures is to introduce a new syntactic representation for functional definitions. The `Term` obtains a new clause.

Augmenting The Grammar for Generalised Terms

```
Term ::= ...
      | λ x : τ • e {- For variable x, and terms τ, e -}
```

The usages of this new string of symbols is governed by the following well-definedness rule. Essentially, one treats $\lambda\ x : \tau\ \bullet\ e$ as the function that on input x of type τ it yields e.

$$\frac{\Gamma, x : \tau \vdash e : \tau'}{\Gamma \vdash (\lambda x : \tau \bullet e) : (\Pi x : \tau \bullet \tau')}\text{[}\Pi\text{-Introduction]}$$

A **Generalised Signature** is now defined to be a tuple *($\mathcal{B}$, arity, type, definition)* where $\mathcal{B}$ = $[\beta_0,\ \beta_1,\ \ldots,\ \beta_n]$ is an *ordered* list of "base symbols", `arity` : $\mathcal{B} \to \mathbb{N}$ associates a number to each base symbol, and `type` : $\mathcal{B} \to$ `Term` associates a generalised term to each base symbol such that $\Gamma_{k-1} \vdash \tau_k :$ `Type` for each k : $0..n$, where $\Gamma_k = (\beta_0 : \tau_0, \ldots, \beta_k : \tau_k)$ and $\tau_i =$ `type` β_i; and `definition` : $\mathcal{B} \to$ `Term` is a partial function associating a term to each symbol name such that the types agree: $\Gamma_{k-1} \vdash$ `definition` β_k : `type` β_k.

Crucially, a generalised signature may be presented as a sequence of declarations $\delta_1, \ldots, \delta_n$ where each δ_i is of the form *name* : *term* = *term* where the "= *term*" portion is optional and the names are unique.

- ◇ When presented with multiple lines, with one declaration δ_i on each line, we omit the commas and split "*name* : *type* = *definition*" into two lines: The first being "*name* : *type*" and the second, if any, being *name* = *definition*.
  - ○ Moreover, `name = (λ x : τ • e)` is instead simplified to `name x = e`.

For example, the Colours context above is a generalised signature, as follows —where, for brevity, we write **C** in place of `Colour`.

$\mathcal{B}$	**C**	Red	green	blue	mix	violet	dark
arity	0	0	0	0	2	0	1
type	Type	**C**	**C**	**C**	**C** × **C** → **C**	**C**	**C** → **C**
definition	-	-	-	-	-	mix green blue	λ c : **C** • mix c blue

As another example, we show how disjoint sums can be defined.

Sums from Σ and 𝔹

```
𝔹              : Type
True           : 𝔹
False          : 𝔹
if_then_else_ : Π A : Type • 𝔹 → A → A → A

_+_ : Type → Type → Type
_+_ X Y  =  Σ tag : 𝔹 • if tag then X else Y

inl : Π X : Type • X → 𝔹 × X
inl x = (True, x)

inr : Π X : Type • X → 𝔹 × X
inr y = (False, y)
```

The type `X + Y` denotes the collection of values of the form "in left" `inl x` or "in right" `inr y` for all `x : X` and `y : Y`. That is, `X + Y` is the disjoint union of collections `X` and `Y`. Above are "default implementations" for `_+_`, `inl`, `inr`; however, there are other ways to encode sum types.

2.5 The Definition of *Generalised Signatures*

For reference, we collect the necessary pieces to formulate the definition of Generalised Signatures. Moreover, we extend the grammar for terms with additional useful constructs.

Review of Inteded Interpretations of Symbols

Symbols	Intended Interpretation
`Type`	The type of all types
𝟙	The type with one element
`Π a : A • B a`	Values of *type* `B a`, for each value `a` of type `A`
`Σ a : A • B a`	Pairs `(a, b)` where `a : A` and `b` is a value of *type* `B a`
`λ x : τ • e`	The function that takes input `x : τ` and yields output `e`

Abbreviations: Provided B is a type that does not vary,

Symbol		Elaboration	Inteded Interpretation
$A \to B$	$\equiv$	$\Pi\, x : A \bullet B$	The functions from A to B
$A \times B$	$\equiv$	$\Sigma\, x : A \bullet B$	Pairs of values *(a, b)* with *a : A* and *b : B*

Given two collections of names $\mathcal{V}$ and $\mathcal{B}$ where each name in $\mathcal{B}$ has an associated *arity*, a number, we may form the collection of generalised terms as follows.

Generalised Terms

```
Term ::= x                  -- A "variable"; a value of 𝒱
       | β t₁ t₂ ... tₙ      -- A "base symbol of arity n"; a value of ℬ
       | Π a : τ • τ'        -- For previously constructed types τ and τ'
       | Σ a : τ • τ'        --      and variable "a"
       | (λ a : τ • τ')      -- "Lambdas"; i.e., functional expressions
       | (τ, τ')             -- "Pairs"
       | 𝟙                   -- "unit type"
       | tt                  -- The only value in the unit type
       | τ ≡ τ'              -- "Propositional equality" type
       | refl x              -- "Reflexivity proofs"
```

If $\texttt{t} : \tau$ and $\tau : \texttt{Type}$ we refer to `t` as an **expression**, to τ as a **type**, and to `Type` as a **kind**. The rules below classify the well-formed generalised terms. The rules for Π and Σ show that they are *families* of types 'indexed' by the first type.

$$\frac{}{\Gamma \vdash \texttt{Type} : \texttt{Type}}[\textsc{Type-in-Type}] \qquad \frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau}[\textsc{Variables}]$$

$$\frac{}{\Gamma \vdash \mathbb{1} : \texttt{Type}}[\textsc{Unit Type}] \qquad \frac{\Gamma, a : \tau \vdash \tau' : \texttt{Type}}{\Gamma \vdash (\Pi\, a : \tau \bullet \tau') : \texttt{Type}}[\textsc{Dependent Function Type}]$$

$$\frac{}{\Gamma \vdash \texttt{tt} : \mathbb{1}}[\mathbb{1}\textsc{-Intro}] \qquad \frac{\Gamma, a : \tau \vdash e : \tau'}{\Gamma \vdash (\lambda\, a : \tau \bullet e) : (\Pi\, a : \tau \bullet \tau')}[\Pi\textsc{-Intro}]$$

$$\frac{\Gamma, a : \tau \vdash \tau' : \texttt{Type}}{\Gamma \vdash (\Sigma\, a : \tau \bullet \tau') : \texttt{Type}}[\textsc{Dependent Product Type}]$$

$$\frac{\Gamma \vdash e : \tau \qquad \Gamma \vdash p : \tau'[a \coloneqq e]}{\Gamma \vdash (e, p) : (\Sigma a : \tau \bullet \tau')}[\Sigma\textsc{-Intro}]$$

$$\frac{\Gamma \vdash l : \tau \qquad \Gamma \vdash r : \tau}{\Gamma \vdash (l \equiv r) : \texttt{Type}}[\textsc{Propositional Equality Type}]$$

$$\frac{\Gamma \vdash x : \tau}{\Gamma \vdash \texttt{refl}_x : (x \equiv x)}[\textsc{Equality Introduction}]$$

A **Generalised Signature** is a tuple *($\mathcal{B}$, arity, type, definition)* where $\mathcal{B}$ = *[*β_0, β_1, …, β_n*]* is an *ordered* list of "base symbols", $\texttt{arity} : \mathcal{B} \to \mathbb{N}$ associates a number to each base symbol, and $\texttt{type} : \mathcal{B} \to \texttt{Term}$ associates a generalised term to each base symbol such that $\Gamma_{k-1} \vdash \tau_k : \texttt{Type}$ for each k *: 0..n*, where $\Gamma_k = (\beta_0 : \tau_0, \ldots, \beta_k : \tau_k)$ and $\tau_i = \texttt{type}\, \beta_i$; and $\texttt{definition} : \mathcal{B} \to \texttt{Term}$ is a partial function associating a term to each symbol name such that the types agree: $\Gamma_{k-1} \vdash \texttt{definition}\, \beta_k : \texttt{type}\, \beta_k$.

That is `type` associates to each base symbol a type-term that is well-defined according to the typing rules above for generalised terms and *possibly* making use of previous symbols in the listing. Then $\texttt{definition}\,\beta_k$ *may* provide a description of a value of $\texttt{type}\,\beta_k$.

$$\frac{\texttt{type}\,\beta \;=\; \tau}{\Gamma \;\vdash\; \beta : \tau}[\textsc{Base Symbol}]$$

$$\frac{\Gamma \;\vdash\; \beta : (\Pi\, x : \tau \,\bullet\, \tau') \qquad \Gamma \;\vdash\; t : \tau}{\Gamma \;\vdash\; \beta\, t \;:\; \tau'[x \coloneqq t]}[\textsc{Symbol Introduction}]$$

Equivalently, a Generalised Signature is an ordered list of 'declarations' $\delta_1, \ldots, \delta_n$ where each δ_i is a tuple from $Name \times Term \times (Term \cup \{-\})$ —for an inferred set $Name$— with the following constraints:

- ◇ Each tuple $\delta_i = (\eta_i, \tau_i, d_i)$ is written as $\eta_i : \tau_i \coloneqq d_i$ or as $\eta_i : \tau_i$ when d_i is the special symbols "-".
  - ◦ We refer to η_i, τ_i, d_i as the *name, type*, and *definition* of δ_i, respectively.
- ◇ Declaration names must be unique.
- ◇ $\delta_1, \ldots, \delta_{k-1} \vdash \delta_k$ for all $k : 1..n$.

Of course contexts now associate *both* a type and an optional definition with a given name, and so $\Gamma : Name \to Term \times (Term \cup -)$ where "-" denotes "no definition". We augment our rules with the following two to accomodate this extended capability.

$$\frac{\Gamma(\eta) = (\tau, d) \qquad d \;\neq\; -}{\Gamma \;\vdash\; \eta : \tau \coloneqq d}[\coloneqq\text{-}\textsc{Introduction}] \qquad \frac{\Gamma(\eta) = (\tau, -)}{\Gamma \;\vdash\; \eta : \tau}[:\text{-}\textsc{Introduction}]$$

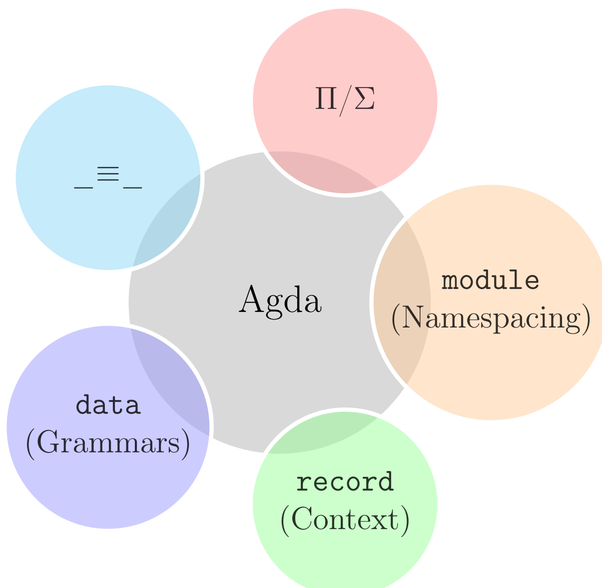
$$\frac{\Gamma \;\vdash\; \eta : \tau \qquad \Gamma \;\vdash\; d : \tau}{\Gamma \;\vdash\; \eta : \tau \coloneqq d}[\coloneqq\text{-}\textsc{Formation}]$$

We refer to the second definition as a **contextual presentation** of Generalised Signatures. In practice, we replace the separating commas of $\delta_1, \ldots, \delta_n$ with line breaks, and write $\eta : \tau \coloneqq d$ as two lines: One with $\eta : \tau$ and another with $\eta = d$, if d is not the opaqueness-value "-". Moreover, in the case of $\eta = (\lambda x : \alpha \,\bullet\, e)$ we elide this as $\eta\, x = e$.

Readers familiar with elementary computing may note that our contextual presentations, when omitting types, are essentially "JSON objects"; i.e., sequences of key-value pairs where the keys are operation names and the values are term descriptions, possibly the "null" description '-'.

2.6 A Whirlwind Tour of Agda

We have introduced a number of concepts and it can be difficult to keep track of when relationships $\Gamma \vdash t : \tau$ are in-fact derivable. The Agda McKinna [McK06], McBride [McB00], Bove and Dybjer [BD08], and Wadler and Kokke [WK18] programming language will allow us to the expressivity of generalised signatures and it will keep track of contexts Γ for us. This section recasts many ideas of the previous sections using Agda notation, and introduces some new ideas. In particular, the 'type of types' `Type` is now cast as a hierarchy of types which can contain types at a 'smaller' level: One writes $\texttt{Set}_i$ to denote the type of types at *level* $i : \mathbb{N}$. This is a technical subtlety and may be ignored; instead treating every occurrence of $\texttt{Set}_i$ as an alias for `Type`.



2.6.1 Dependent Functions

A *Dependent Function type* has those functions whose result *type* depends on the *value* of the argument. If `B` is a type depending on a type `A`, then `(a : A) → B a` is the type of functions `f` mapping arguments `a : A` to values `f a : B a`. Vectors, matrices, sorted lists, and trees of a particular height are all examples of dependent types. One also sees the notations `∀ (a : A) → B a` and `Π a : A • B a` to denote dependent types.

For example, *the* generic identity function takes as *input* a type `X` and returns as *output* a function `X → X`. Here are a number of ways to write it in Agda.

The Identity Function

```
id₀ : (X : Set) → X → X
id₀ X x = x

id₁ id₂ id₃ : (X : Set) → X → X

id₁ X = λ x → x
id₂   = λ X x → x
id₃   = λ (X : Set) (x : X) → x
```

All these functions explicitly require the type `X` when we use them, which is silly since it can be inferred from the element `x`. Curly braces make an argument *implicitly inferred* and so it may be omitted. E.g., the `{X : Set}` $\rightarrow \cdots$ below lets us make a polymorphic function since `X` can be inferred by inspecting the given arguments. This is akin to informally writing id_X versus id.

Inferring Arguments...

```
id : {X : Set} → X → X
id x = x

sad : ℕ
sad = id₀ ℕ 3

nice : ℕ
nice = id 3
```

...and Explicitly Passsing Implicits

```
explicit : ℕ
explicit = id {ℕ} 3

explicit' : ℕ
explicit' = id₀ _ 3


.
```

Notice that we may provide an implicit argument *explicitly* by enclosing the value in braces in its expected position. Values can also be inferred when the `_` pattern is supplied in a value position. Essentially wherever the typechecker can figure out a value —or a type—, we may use `_`. In type declarations, we have a contracted form via ∀ —which is **not** recommended since it slows down typechecking and, more importantly, types *document* our understanding and it's useful to have them explicitly.

In a type, `(a : A)` is called a *telescope* and they can be combined for convenience.

```
  {x : _} {y : _} (z : _) → ⋯
≈  ∀ {x y} z → ⋯
```

```
  (a₁ : A) → (a₂ : A) → (b : B) → ⋯
≈  (a₁ a₂ : A) (b : B) → ⋯
```

2.6.2 Dependent Datatypes

Algebraic datatypes are introduced with a `data` declaration, giving the name, arguments, and type of the datatype as well as the constructors and their types. Below we define the datatype of lists of a particular length.

Vectors —ℕ-indexed Lists

```
data Vec {ℓ : Level} (A : Set ℓ) : ℕ → Set ℓ where
  []  : Vec A 0
  _::_ : {n : ℕ} → A → Vec A n → Vec A (1 + n)
```

Notice that, for a given type `A`, the type of `Vec A` is `ℕ → Set`. This means that `Vec A` is a family of types indexed by natural numbers: For each number `n`, we have a type `Vec A n`. One says `Vec` is *parameterised* by `A` (and ℓ), and *indexed* by `n`. They have different roles: `A` is the type of elements in the vectors, whereas `n` determines the 'shape' —length— of the vectors and so needs to be more 'flexible' than a parameter.

Notice that the indices say that the only way to make an element of `Vec A 0` is to use `[]` and the only way to make an element of `Vec A (1 + n)` is to use `_::_`. Whence, we can write the following safe function since `Vec A (1 + n)` denotes non-empty lists and so the pattern `[]` is impossible.

Safe Head

```
head : {A : Set} {n : ℕ} → Vec A (1 + n) → A
head (x :: xs) = x
```

The ℓ argument means the `Vec` type operator is *universe polymorphic*: We can make vectors of, say, numbers but also vectors of types. Levels are essentially natural numbers: We have `lzero` and `lsuc` for making them, and `_⊔_` for taking the maximum of two levels. *There is no universe of all universes:* $\texttt{Set}_n$ has type $\texttt{Set}_{n+1}$ *for any* n, however the *type* `(n : Level) → Set n` is *not* itself typeable —i.e., is not in $\texttt{Set}_l$ for any `l`— and Agda errors saying it is a value of $\texttt{Set}\omega$.

Functions are defined by pattern matching, and must cover all possible cases. Moreover, they must be terminating and so recursive calls must be made on structurally smaller arguments; e.g., `xs` is a sub-term of `x :: xs` below and catenation is defined recursively on the first argument. Firstly, we declare a *precedence rule* so we may omit parenthesis in seemingly ambiguous expressions.

Catenation is a $++\!\longrightarrow\!+$ Homomorphism

```
infixr 40 _++_

_++_ : {A : Set} {n m : ℕ} → Vec A n → Vec A m → Vec A (n + m)
[]        ++ ys  =  ys
(x :: xs) ++ ys  =  x :: (xs ++ ys)
```

Notice that the **type encodes a useful property**: The length of the catenation is the sum of the lengths of the arguments.

2.6.3 Propositional Equality

An example of propositions-as-types is a definition of the identity relation —the least reflexive relation. For a type `A` and an element `x` of `A`, we define the family of proofs of "being equal to x" by declaring only one inhabitant at index `x`.

Propositional Equality

```
data _≡_ {A : Set} : A → A → Set
  where
    refl : {x : A} → x ≡ x
```

This states that `refl {x}` is a proof of `l ≡ r` whenever `l` and `r` simplify, by definition chasing only, to `x` —i.e., both `l` and `r` have `x` as their normal form.

This definition makes it easy to prove Leibniz's substitutivity rule, "equals for equals":

Transport along proofs

```
subst : {A : Set} {P : A → Set} {l r : A} → l ≡ r → P l → P r
subst refl it = it
```

Why does this work? An element of `l ≡ r` must be of the form `refl {x}` for some canonical form `x`; but if `l` and `r` are both `x`, then `P l` and `P r` are the *same type*. Pattern matching on a proof of `l ≡ r` gave us information about the rest of the program's type.

One says $l \equiv r$ is *definitionally equal* when both sides are indistinguishable after all possible definitions in the terms l and r have been used. In contrast, the equality is «</propositionally equal/»> when one must perform actual work, such as using inductive reasoning. In general, if there are no variables in $l \equiv r$ then we have definitional equality —i.e., simplify as much as possible then compare— otherwise we have propositional equality —real work to do. Below is an example about the types of vectors.

Examples of Propositional and Definitional Equality

```
definitional : ∀ {A} → Vec A 5 ≡ Vec A (2 + 3)
definitional = refl

propositional : ∀ {A m n} → Vec A (m + n) ≡ Vec A (n + m)
propositional = {!!}
```

2.6.4 Calculational Proofs —Making Use of Unicode Mixfix Lexemes

School math classes show calculations as follows.

```
  p
≡⟨ reason why p ≡ q ⟩
  q
≡⟨ reason why q ≡ r ⟩
  r
□
```

Calculational Proof Syntax Embedded As Proof Forming Functions

```
infixr 5 _≡⟨_⟩_
infix  6 _□

_□ : {A : Set} (a : A) → a ≡ a
_ □ = refl

_≡⟨_⟩_ : {A : Set} (p {q r} : A)
   → p ≡ q → q ≡ r → p ≡ r
_ ≡⟨ refl ⟩ refl = refl
```

We can treat these pieces as Agda *mixfix* identifiers and associate to the right to obtain: `p ≡⟨ reason`$_1$ `⟩ (q ≡⟨ reason`$_2$ `⟩ (r □))`. We can code this up, as show above on the right.

2.6.5 Modules —Namespace Management

Agda modules are not a first-class construct, yet.

- Within a module, we may have nested module declarations.
- All names in a module are public, unless declared `private`.

A Simple Module

```
module M where

  𝒩 : Set
  𝒩 = ℕ

  private
    x : ℕ
    x = 3

  y : 𝒩
  y = x + 1
```

Using It

```
use₀ : M.𝒩
use₀ = M.y

use₁ : ℕ
use₁ = y
  where open M

open M

use₂ : ℕ
use₂ = y
```

Parameterised Modules

```
module M’ (x :
 ↪  ℕ)
  where
    y : ℕ
    y = x + 1
```

Names=Functions

```
exposed : (x :
 ↪  ℕ)
        → ℕ
exposed = M’.y
```

Using Them

```
use’₀ : ℕ
use’₀ = M’.y 3

module M’’ = M’
 ↪   3

use’’ : ℕ
use’’ = M’’.y

use’₁ : ℕ
use’₁ = y
  where
    open M’ 3
```

- Public names may be accessed by qualification or by opening them locally or globally.
- Modules may be parameterised by arbitrarily many values and types —but not by other modules.

Modules are essentially implemented as syntactic sugar: Their declarations are treated as top-level functions that take the parameters of the module as extra arguments. In particular, it may appear that module arguments are 'shared' among their declarations, but this is not so.

"Using Them":

- ◇ This explains how names in parameterised modules are used: They are treated as functions.
- ◇ We may prefer to instantiate some parameters and name the resulting module.
- ◇ However, we can still `open` them as usual.

When opening a module, we can control which names are brought into scope with the `using`, `hiding`, and `renaming` keywords.

`open M hiding` (n_0`;` ...`;` n_k)	Essentially treat n_i as private
`open M using` (n_0`;` ...`;` n_k)	Essentially treat *only* n_i as public
`open M renaming` (n_0 `to` m_0`;` ...`;` n_k `to` m_k)	Use names m_i instead of n_i

Table 2.2: Module combinators supported in the current implementation of Agda

Splitting a program over several files will improve type checking performance, since when you are making changes the type checker only has to check the files that are influenced by the change.

- ◇ `import X.Y.Z`: Use the definitions of module `Z` which lives in file `./X/Y/Z.agda`.
- ◇ `open M public`: Treat the contents of `M` as if they were public contents of the current module.

So much for Agda modules.

2.6.6 Records

A record type is declared much like a datatype where the fields are indicated by the `field` keyword. The nature of records is summarised by the following equation.

$$\texttt{record} \quad \approx \quad \texttt{module} + \texttt{data} \text{ with one constructor}$$

The class of types along with a value picked out

```
record PointedSet : Set₁ where
  constructor MkIt  {- Optional -}
  field
    Carrier : Set
    point   : Carrier

  {- It’s like a module,
  we can add derived definitions -}
  blind : {A : Set} → A → Carrier
  blind = λ a → point
```

Defining Instances

```
ex₀ : PointedSet
ex₀ = record {Carrier = ℕ; point = 3}

ex₁ : PointedSet
ex₁ = MkIt ℕ 3

open PointedSet

ex₂ : PointedSet
Carrier ex₂ = ℕ
point   ex₂ = 3
```

Within the Emacs interface, start with `ex₂ = ?`, then in the hole enter `C-c C-c RET` to obtain the *co-pattern* setup. Two tuples are the same when they have the same components, likewise a record is defined by its projections, whence *co-patterns*. If you are using many local definitions, you likely want to use co-patterns.

To allow projection of the fields from a record, each record type comes with a module of the same name. This module is parameterised by an element of the record type and contains projection functions for the fields.

Simple Uses

```
use⁰ : ℕ
use⁰ = PointedSet.point ex₀

use¹ : ℕ
use¹ = point where open PointedSet ex₀

open PointedSet

use² : ℕ
use² = blind ex₀ true
```

You can even pattern match on records —they’re just `data` after all!

Pattern Matching on Records

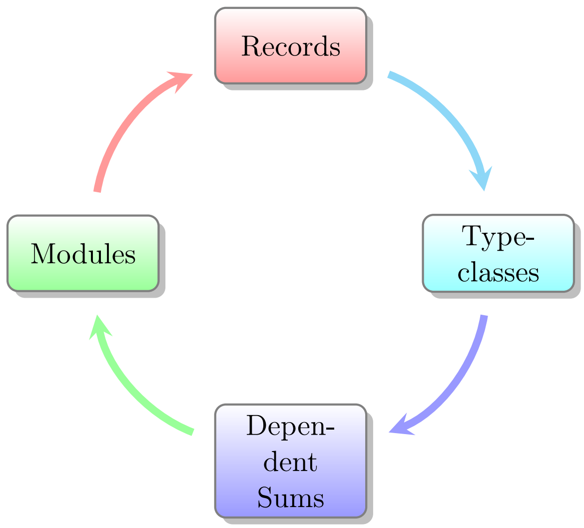
```
use³ : (P : PointedSet) → Carrier P
use³ record {Carrier = C; point = x}
  = x

use⁴ : (P : PointedSet) → Carrier P
use⁴ (MkIt C x)
  = x
```

So much for records.

2.7 Facets of Structuring Mechanisms

In this section we provide a demonstration that with dependent-types we can show records, direct dependent types, and contexts —which in Agda may be thought of as parameters to a module— are interdefinable. Consequently, we observe that the structuring mechanisms provided by the current implementation of Agda —and other DTLs— have no real differences aside from those imposed by the language and how they are generally utilised. More importantly, this demonstration indicates our proposed direction of identifying notions of packages is on the right track.

Our example will be implementing a monoidal interface in each format, then presenting *views* between each format and that of the `record` format. Furthermore, we shall also construe each as a typeclass, thereby demonstrating that typeclasses are, essentially, not only a selected record but also a selected *value* of a dependent type —incidentally this follows from the previous claim that records and direct dependent types are essentially the same.



2.7.1 Three Ways to Define Monoids

Recall that the signature of a monoid consists of a type `Carrier` with a method `_ ; _` that composes values and an `Id`-entity value. With Agda's lack of type-proof discrimination, i.e., its support for the Curry-Howard Correspondence, the "propositions as types" interpretation, we can encode the signature as well as the axioms of monoids to yield their theory presentation in the following two ways. Additionally, we have the derived result: `Id`-entity can be popped-in and out as desired.

The following code blocks contain essentially the same content, but presented using different notions of packaging. Even though both use the `record` keyword, the latter is treated as a typeclass since the carrier of the monoid is given 'statically' and instance search is used to invoke such instances.

Monoids as Agda Records

```
record Monoid-Record : Set₁ where
  infixl 5 _ ; _
  field
    -- Interface
    Carrier  : Set
    Id       : Carrier
    _ ; _       : Carrier → Carrier → Carrier

    -- Constraints
    lid   : ∀{x}    → (Id  ;  x) ≡ x
    rid   : ∀{x}    → (x  ;  Id) ≡ x
    assoc : ∀ x y z → (x  ;  y)  ;  z  ≡  x  ;  (y  ;  z)

  -- derived result
  pop-Idᵣ : ∀ x y  →  x  ;  Id  ;  y  ≡  x  ;  y
  pop-Idᵣ x y = cong (_  ;  y) rid

open Monoid-Record {{...}} using (pop-Idᵣ)
```

Monoids as Typeclasses

```
record HasMonoid (Carrier : Set) : Set₁ where
  infixl 5 _ ; _
  field
    Id    : Carrier
    _ ; _    : Carrier → Carrier → Carrier
    lid   : ∀{x} → (Id  ;  x) ≡ x
    rid   : ∀{x} → (x  ;  Id) ≡ x
    assoc : ∀ x y z → (x  ;  y)  ;  z ≡ x  ;  (y  ;  z)

  pop-Id-tc : ∀ x y →  x  ;  Id  ;  y  ≡  x  ;  y
  pop-Id-tc x y = cong (_  ;  y) rid

open HasMonoid {{...}} using (pop-Id-tc)
```

The double curly-braces `{{...}}` serve to indicate that the given argument is to be found by instance resolution: The derived results for `Monoid-Record` and `HasMonoid` can be invoked without having to mention a monoid on a particular carrier, provided there exists one unique record value having it as carrier —otherwise one must use named instances Kahl and Scheffczyk [KS01]. Notice that the carrier argument in the typeclasses approach, "structure on a carrier", is an (undeclared) implicit argument to the `pop-Id-tc` operation.

Alternatively, in a DTL we may encode the monoidal interface using dependent products **directly** rather than use the syntactic sugar of records. The notation `Σ x : A • B x` denotes the type of pairs `(x , pf)` where `x : A` and `pf : B x` —i.e., a record consisting of two fields. It may be thought of as a constructive analogue to the classical set comprehension `{x : A | B x}`.

Monoids as Dependent Sums

```
-- Type alias
Monoid-Σ  :  Set₁
Monoid-Σ  =    Σ Carrier : Set
             • Σ Id : Carrier
             • Σ _ ; _ : (Carrier → Carrier → Carrier)
             • Σ lid : (∀{x} → Id   ;   x ≡ x)
             • Σ rid : (∀{x} → x   ;   Id ≡ x)
             • (∀ x y z → (x   ;   y)   ;   z ≡ x   ;   (y   ;   z))

pop-Id-Σ : ∀ {{M : Monoid-Σ}}
               (let Id  = proj₁ (proj₂ M))
               (let _ ; _ = proj₁ (proj₂ (proj₂ M)))
           →  ∀ (x y : proj₁ M)  →  (x   ;   Id)   ;   y  ≡  x   ;   y
pop-Id-Σ {{M}} x y = cong (_  ;   y) (rid {x})
             where  _ ; _    = proj₁ (proj₂ (proj₂ M))
                    rid    = proj₁ (proj₂ (proj₂ (proj₂ (proj₂ M))))
```

Observe the lack of informational difference between the presentations, yet there is a *Utility Difference: Records give us the power to name our projections* *directly* *with possibly meaningful names.* Of course this could be achieved indirectly by declaring extra functions; e.g.,

Agda

```
Carrierₜ : Monoid-Σ → Set
Carrierₜ = proj₁
```

We will refrain from creating such boiler plate —that is, *records allow us to omit such mechanical boilerplate.*

Of the renditions thus far, the Σ rendering makes it clear that a monoid could have any subpart as a record with the rest being dependent upon said record. For example, if we had a semigroup type, we could have declared

```
Monoid-Σ = Σ S : Semigroup • Σ Id : Semigroup.Carrier S • ···
```

There are a large number of such hyper-graphs, we have only presented a stratified view for brevity. In particular, `Monoid-Σ` is the extreme unbundled version, whereas `Monoid-Record` is the other extreme, and there is a large spectrum in between —all of which are somehow isomorphic; e.g., `Monoid-Record ≅ Σ C : Set • HasMonoid C`. Our envisioned system would be able to derive any such view at will Astesiano et al. [Ast+02] and so programs may be written according to one view, but easily repurposed for other view with little human intervention.

2.7.2 Instances and Their Use

Instances of the monoid types are declared by providing implementations for the necessary fields. Moreover, as mentioned earlier, to support instance search, we place the declarations in an `instance` clause.

Instance Declarations

```
instance
   ℕ-record = record { Carrier = ℕ ; Id = 0 ; _ ⨾ _ = _+_
            ; lid =  +-identityˡ _  ; rid = +-identityʳ _ ; assoc = +-assoc }

   ℕ-tc : HasMonoid ℕ
   ℕ-tc = record { Id = 0; _ ⨾ _ = _+_
        ; lid = +-identityˡ _ ; rid = +-identityʳ _ ; assoc = +-assoc }

   ℕ-Σ : Monoid-Σ
   ℕ-Σ = ℕ , 0 , _+_ , +-identityˡ _ , +-identityʳ _ , +-assoc
```

Interestingly, notice that the grouping in ℕ-Σ is just an unlabelled (dependent) product, and so when it is used below in `pop-Id-Σ` we project to the desired components. Whereas in the `Monoid-Record` case we could have projected the carrier by `Carrier M`, now we would write `proj₁ M`.

No Monoids Mentioned at Use Sites

```
ℕ-pop-0ᵣ : ∀ (x y : ℕ) → x + 0 + y  ≡  x + y
ℕ-pop-0ᵣ = pop-Idᵣ

ℕ-pop-0-tc : ∀ (x y : ℕ) → x + 0 + y  ≡  x + y
ℕ-pop-0-tc = pop-Id-tc

ℕ-pop-0ₜ : ∀ (x y : ℕ) → x + 0 + y  ≡  x + y
ℕ-pop-0ₜ = pop-Id-Σ
```

One may realise that `pop-0` proofs as a form of polymorphism —the result is independent of the particular packaging mechanism; record, typeclass, Σ, it does not matter.

Finally, let us exhibit views between the Σ form and the `record` form.

Agda

```
{- Essentially moved from record{⋯} to product listing -}
from-record-to-usual-type : Monoid-Record → Monoid-Σ
from-record-to-usual-type M  =  Carrier , Id , _ ; _ , lid , rid , assoc
                                where open Monoid-Record M

{- Organise a tuple componenets as implementing named fields -}
to-record-from-usual-type : Monoid-Σ → Monoid-Record
to-record-from-usual-type (c , id , op , lid , rid , assoc)
    = record { Carrier = c
             ; Id      = id
             ; _ ; _    = op
             ; lid     = lid
             ; rid     = rid
             ; assoc   = assoc
             } -- Term construed by ‘Agsy’,
               -- Agda’s mechanical proof search.
```

Furthermore, by definition chasing, `refl`-exivity, these operations are seen to be inverse of each other. Hence we have two faithful non-lossy protocols for reshaping our grouped data.

2.7.3 A Fourth Definition —Contexts

In our final presentation, we construe the grouping of the monoidal interface as a sequence of *variable* : *type* declarations —i.e., a context or ‘telescope’. Since these are not top level items by themselves, in Agda, we take a purely syntactic route by positioning them in a `module` declaration as follows.

Monoids as Telescopes

```
module Monoid-Telescope-User
  (Carrier : Set)
  (Id      : Carrier)
  (_ ; _    : Carrier → Carrier → Carrier)
  (lid     : ∀{x} → Id  ;  x ≡ x)
  (rid     : ∀{x} → x  ;  Id ≡ x)
  (assoc   : ∀ x y z → (x  ;  y)  ;  z ≡ x  ;  (y  ;  z))
  where

  pop-Id_m : ∀(x y : Carrier)  →  (x  ;  Id)  ;  y  ≡  x  ;  y
  pop-Id_m x y = cong (_ ;  y) (rid {x})
```

Notice that this is nothing more than the named fields of `Monoid-Record` but not[10] bundled. Additionally, if we insert a Σ before each name we essentially regain the `Monoid-Σ`

[10]Records let us put things in a bag and run around with them, whereas telescopes amount to us running around with all of our things in our hands —hoping we don’t drop (forget) any of them.

formulation. It seems contexts, at least superficially, are a nice middle ground between the previous two formulations. For instance, if we *syntactically*, visually, move the `Carrier : Set` declaration one line above, the resulting setup looks eerily similar to the typeclass formulation of records.

As promised earlier, we can regard the above telescope as a record:

Agda

```
  {- No more running around with things in our hands. -}
  {- Place the telescope parameters into a nice bag to hold. -}
  record-from-telescope : Monoid-Record
  record-from-telescope
    = record { Carrier = Carrier
             ; Id      = Id
             ; _ ; _     = _ ; _
             ; lid     = lid
             ; rid     = rid
             ; assoc   = assoc
             }
```

The structuring mechanism `module` is not a first class citizen in Agda. As such, to obtain the converse view, we work in a parameterised module.

Agda

```
module record-to-telescope (M : Monoid-Record) where

  open Monoid-Record M
  -- Treat record type as if it were a parameterised module type,
  -- instantiated with M.

  open Monoid-Telescope-User Carrier Id _ ; _ lid rid assoc
```

Notice that we just listed the components out —rather reminiscent of the formulation `Monoid-Σ`. This observation only increases confidence in our thesis that there is no real distinctions of packaging mechanisms in DTLs.

Undeniably instantiating the telescope approach to monoids for the natural number is nothing more than listing the required components.

Agda

```
open Monoid-Telescope-User ℕ 0 _+_ (+-identityˡ _) (+-identityʳ _) +-assoc
```

C.f., the definition of ℕ-Σ: This is nearly the same instantiation with the primary syntactical difference being that this form had its arguments separated by spaces rather than commas!

```
Agda
ℕ-pop_m  : ∀(x y : ℕ) → x + 0 + y ≡ x + y
ℕ-pop_m  = pop-Id_m
```

Notice how this presentation makes it explicitly clear why we cannot have multiple instances: There would be name clashes. Even if the data we used had distinct names, the derived result may utilise data having the same name thereby admitting name clashes elsewhere. —This could be avoided in Agda by qualifying names and/or renaming.

It is interesting to note that this presentation is akin to that of `class`-es in C#/Java languages: The interface is declared in one place, monolithic-ly, as well as all derived operations there; if we want additional operations, we create another module that takes that given module as an argument in the same way we create a class that inherits from that given class.

Demonstrating the interdefinablity of different notions of packaging cements our thesis that it is essentially *utility* that distinguishes packages more than anything else. In particular, explicit distinctions have lead to a duplication of work where the same structure is formalised using different notions of packaging. In chapter **??** we will show how to avoid duplication by coding against a particular 'package former' rather than a particular variation thereof —this is akin to a type former.

2.8 Contexts are Promising

The current implementation of the Agda language Bove, Dybjer, and Norell [BDN09] and Norell [Nor07] has a notion of second-class modules which may contain sub-modules along with declarations and definitions of first-class citizens. The intimate relationship between records and modules is perhaps best exemplified here since the current implementation provides a declaration to construe a record as if it were a module. This observation is not specific to Agda, which is only a presentation language. Indeed, other DTLs (dependently-typed languages) reassure our hypothesis; the existence of a unified notion of package:

- **The centrality of contexts**

  The **Beluga** language has the distinctive feature of direct support for first-class contexts Pientka [Pie10]. A term `t(x)` may have free variables and so whether it is well-formed, or what its type could be, depends on the types of its free variables, necessitating one to either declare them before hand or to write, in Beluga,
  `[ x : T |- t(x) ]` for example. As argued in the previous section, contexts are essentially dependent sums. In contrast to Beluga, **Isabelle** is a full-featured language and logical framework that also provides support for named contexts in the form of 'locales'

Ballarin [Bal03] and Kammüller, Wenzel, and Paulson [KWP99]; unfortunately it is not a dependently-typed language.

- **Signatures as an underlying formalism**

  Twelf Pfenning and Team [PT15] is a logic programming language implementing Edinburgh's Logical Framework Urban, Cheney, and Berghofer [UCB08], Rabe [Rab10], and Stump and Dill [SD02] and has been used to prove safety properties of 'real languages' such as SML. A notable practical module system Rabe and Schürmann [RS09] for Twelf has been implemented using signatures and signature morphisms.

- **Packages (modules) have their own useful language**

  The current implementation of Coq Paulin-Mohring [Pau] and Gross, Chlipala, and Spivak [GCS14] provides a "copy and paste" operation for modules using the `include` keyword. Consequently it provides a number of module combinators, such as `<+` which is the infix form of module inclusion Coq Development Team [Coq18]. Since Coq module types are essentially contexts, the module type `X <+ Y <+ Z` is really the catenation of contexts, where later items may depend on former items. The Maude Clavel et al. [Cla+07] and Durán and Meseguer [DM07] framework contains a similar yet more comprehensive algebra of modules and how they work with Maude theories.

It is important to consider other languages so as to see their communities treat module systems and what uses cases they are interested in. In the next section, we shall see a glimpse of how the Coq community works with packages, and, to make the discussion accessible, we shall provide Agda translations of Coq code.

2.9 Coq Modules as Generalised Signatures

Module Systems parameterise programs, proofs, and tactics over structures. In this section, we shall form a library of simple graphs to showcase how Coq's approach to packages is essentially the proposed definition of generalised signatures: A sequence of name-type-definition tuples where the definition may be omitted. To make the Coq accessible to readers, we will provide an Agda translation that only uses the `record` construct in Agda —completely ignoring the `data` and `module` forms which would otherwise be more natural in certain scenarios below— in order to demonstrate that *all packaging concepts essentially coincide in a DTL.*

(Along the way, we refer to aspects of Agda that we found convenient and desirable that we chose it as a presentation language instead Coq and other equally appropriate DTLs.)

In Coq, a `Module Type` contains the signature of the abstract structure to work from; it lists the `Parameter` and `Axiom` values we want to use, possibly along with notation declaration to make the syntax easier.

Graphs —Coq

```
Module Type Graph.
  Parameter Vertex : Type.
  Parameter Edges : Vertex -> Vertex -> Prop.

  Infix "<=" := Edges : order_scope.
  Open Scope order_scope.

  Axiom loops : forall e, e <= e.
  Parameter decidable : forall x y, {x <= y} + {not (x <= y)}.
  Parameter connected : forall x y, {x <= y} + {y <= x}.
End Graph.
```

Graphs —Agda

```
record Graph : Set₁ where
  field
    Vertex : Set
    _⟶_  : Vertex → Vertex → Set
    loops  : ∀ {e} → e ⟶ e
    decidable : ∀ x y → Dec (x ⟶ y)
    connected : ∀ x y → (x ⟶ y) ⊎ (y ⟶ x)
```

Notice that due to Agda's support for mixfix Unicode lexemes, we are able to use the evocative arrow notation _⟶_ for edges directly. In contrast, Coq uses ASCII order notation *after* the type of edges is declared. Even worse, conventional Coq distinguishes between value parameters and proofs, whereas Agda does not.

In Coq, to form an instance of the graph module type, we define a module that satisfies the module type signature. The _<:_ declaration requires us to have definitions and theorems with the same names and types as those listed in the module type's signature. In contrast, the Agda form below explicitly ties the signature's named fields with their implementations, rather than inferring it.

Booleans are Graphs —Coq

```
Module BoolGraph <: Graph.
  Definition Vertex := bool.
  Definition Edges  := fun x => fun y => leb x y.

  Infix "<=" := Edges : order_scope.
  Open Scope order_scope.

  Theorem loops: forall x : Vertex, x <= x.
    Proof.
    intros; unfold Edges, leb; destruct x; tauto.
    Qed.

  Theorem decidable: forall x y, {Edges x y} + {not (Edges x y)}.
    Proof.
      intros; unfold Edges, leb; destruct x, y.
      all: (right; discriminate) || (left; trivial).
  Qed.

  Theorem connected: forall x y, {Edges x y} + {Edges y x}.
    Proof.
      intros; unfold Edges, leb. destruct x, y.
      all: (right; trivial; fail) || left; trivial.
  Qed.
End BoolGraph.
```

Booleans are Graphs —Agda

```
BoolGraph : Graph
BoolGraph = record
              { Vertex = Bool
              ; _⟶_ = leb
              ; loops = b≤b
              {- I only did the case analysis, the rest was “auto”. -}
              ; decidable = λ{ true  true  → yes b≤b
                             ; true  false → no (λ ())
                             ; false true  → yes f≤t
                             ; false false → yes b≤b }
              {- I only did the case analysis, the rest was “auto”. -}
              ; connected = λ{ true true   → inj₁ b≤b
                             ; true false  → inj₂ f≤t
                             ; false true  → inj₁ f≤t
                             ; false false → inj₁ b≤b }
              }
```

We are now in a position to write a “module functor”: A module that takes some `Module`

`Type` parameters and results in a module that is inferred from the definitions and parameters in the new module; i.e., a parameterised module. E.g., here is a module that defines a minimum function.

Minimisation as a function on modules —Coq

```
Module Min (G : Graph).
  Import G. (* I.e., open it so we can use names in unquantifed form. *)
  Definition min a b : Vertex := if (decidable a b) then a else b.
  Theorem case_analysis: forall P : Vertex -> Type, forall x y,
        (x <= y -> P x) -> (y <= x -> P y) -> P (min x y).
  Proof.
    intros. (* P, x, y, and hypothesises H₀, H₁ now in scope*)
    (* Goal: P (min x y) *)
    unfold min. (* Rewrite "min" according to its definition. *)
    (* Goal: P (if decidable x y then x else y) *)
    destruct (decidable x y). (* Case on the result of decidable *)
    (* Subgoal 1: P x  ---along with new hypothesis H₃ : x ≤ y *)
    tauto. (* i.e., modus ponens using H₁ and H₃ *)
    (* Subgoal 2: P y  ---along with new hypothesis H₃ : ¬ x ≤ y *)
    destruct (connected x y).
    (* Subgoal 2.1: P y ---along with new hypothesis H₄ : x ≤ y *)
    absurd (x <= y); assumption.
    (* Subgoal 2.2: P y ---along with new hypothesis H₄ : y ≤ x *)
    tauto. (* i.e., modus ponens using H₂ and H₄ *)
  Qed.
End Min.
```

`Min` is a function-on-modules; the input type is a `Graph` value and the output module's type is inferred to be `Sig Definition min : ⋯. Parameter case_analysis: ⋯. End`. This is similar to JavaScript's approach. In contrast, Agda has no notion of signature, and so the declaration below only serves as a *namespacing* mechanism that has a parameter over-which new programs and proofs are abstracted —the primary purpose of module systems mentioned earlier.

Minimisation as a function on modules —Agda

```
record Min (G : Graph) : Set where
  open Graph G

  min : Vertex → Vertex → Vertex
  min x y with decidable x y
  ...| yes _  = x
  ...| no  _  = y

  case-analysis : ∀ {P : Vertex → Set} {x y}
                → (x ⟶ y  →  P x)
                → (y ⟶ x  →  P y)
                → P (min x y)
  case-analysis {P} {x} {y} H₀ H₁ with decidable x y | connected x y
  ... | yes x⟶y | _          = H₀ x⟶y
  ... | no ¬x⟶y | inj₁ x⟶y = ⊥-elim (¬x⟶y x⟶y)
  ... | no ¬x⟶y | inj₂ y⟶x = H₁ y⟶x

open Min
```

Let's apply the so called module functor. The `min` function, as shown in the comment below, now specialises to the carrier of the Boolean graph.

Applying module-to-module functions (part I) —Coq

```
Module Conjunction := Min BoolGraph.
Export Conjunction.
Print min.
(*
min =
fun a b : BoolGraph.Vertex => if BoolGraph.decidable a b then a else b
      : BoolGraph.Vertex -> BoolGraph.Vertex -> BoolGraph.Vertex
 *)
```

In the Agda setting, we can prove the aforementioned observation: The module is for namespacing *only* and so it has no non-trivial implementations.

Applying module-to-module functions (part I) —Agda

```
Conjunction = Min BoolGraph

uep : ∀ (p q : Conjunction) → p ≡ q
uep record {} record {} = refl

{- "min I" is the specialisation of "min" to the Boolean graph -}
_ : Bool → Bool → Bool
_ = min I where I : Conjunction; I = record {}
```

Unlike the previous functor, which had its return type inferred, we may explicitly declare a return type. E.g., the following functor is a `Graph → Graph` function.

A module-to-module function —Coq

```
Module Dual (G : Graph) <: Graph.
  Definition Vertex := G.Vertex.
  Definition Edges  x y : Prop := G.Edges y x.
  Definition loops := G.loops.
  Infix "<=" := Edges : order_scope.
  Open Scope order_scope.
  Theorem decidable: forall x y, {x <= y} + {not (x <= y)}.
    Proof.
      unfold Edges. pose (H := G.decidable). auto.
  Qed.
  Theorem connected: forall x y, {Edges x y} + {Edges y x}.
    Proof.
      unfold Edges.  pose (H := G.connected). auto.
  Qed.
End Dual.
```

Agda makes it clearer that this is a module-to-module function.

A module-to-module function —Agda

```
Dual : Graph → Graph
Dual G = let open Graph G in record
           { Vertex     = Vertex
           ; _⟶_         = λ x y →  y ⟶ x
           ; loops      = loops
           ; decidable = λ x y → decidable y x
           ; connected = λ x y → connected y x
           }
```

An example use would be renaming "min ↦ max" —e.g., to obtain meets from joins.

Applying module-to-module functions (part II) —Coq

```
Module Max (G : Graph).
  (* Module applications cannot be chained;
     intermediate modules must be named. *)
  Module DualG   := Dual G.
  Module Flipped := Min DualG.
  Import G.
  Definition max := Flipped.min.
  Definition max_case_analysis:
        forall P : Vertex -> Type, forall x y,
        (y <= x -> P x) -> (x <= y -> P y) -> P (max x y)
        := Flipped.case_analysis.
End Max.
```

Applying module-to-module functions (part II) —Agda

```
record Max (G : Graph) : Set where
  open Graph G
  private
    Flipped = Min (Dual G)
    I : Flipped
    I = record {}

  max : Vertex → Vertex → Vertex
  max = min I

  max-case-analysis : ∀ {P : Vertex → Set} {x y}
                → (y ⟶ x  →  P x)
                → (x ⟶ y  →  P y)
                → P (max x y)
  max-case-analysis = case-analysis I
```

Here is a table summarising the two languages' features, along with JavaScript as a position of reference.

	Signature	Structure
Coq	≈ module type	≈ module
Agda	≈ record type	≈ record value
JavaScript	≈ prototype	≈ JSON object

Table 2.3: Signatures and structures in Coq, Agda, and JavaScript

It is perhaps seen most easily in the last entry in the table, that modules and modules types are essentially the same thing: They are just partially defined record types. Again there is a difference in the usage intent:

Concept	Intent
Module types	Any name may be opaque, undefined.
Modules	All names must be fully defined.

Table 2.4: Modules and module types only differ in intended utility

2.10 Problem Statement, Objectives, and Methodology

This section provides a statement of the problem that is addressed in this thesis. It also outlines the objectives of this thesis and discusses the methodology used to achieve those objectives.

2.10.1 Problem Statement

Currently, first-class module systems for dependently-typed languages are poorly *supported*. Modules $\mathcal{X}$ consisting of functions symbols, properties, and derived results are currently presented in the form `Is`$\mathcal{X}$: A module parameterised by function symbols and exposing derived results possibly with further, uninstantiated, proof obligations. This is understandable: Function symbols generally vary more often than proof obligations. (This is discussed in detail in Section **??**.) However, when users do not yet have the necessary parameters, they need to use a curried form of the module and so library developers also provide a module $\mathcal{X}$ which packs up the parameters as necessary fields within the module. Unfortunately, there is a whole spectrum of modules $\mathcal{X}_i$ that is missing: These are the module $\mathcal{X}$ where only `i` of the original parameters are exposed with the remaining being packed-away into the module body. It is tedious and error-prone to form all the $\mathcal{X}_i$ by hand; such 'unbundling' should be mechanically achievable from the completely bundled form $\mathcal{X}$. A similar issue happens when one wants to *describe a computation* using module $\mathcal{X}$, then its function symbols need to have associated syntactic counterparts; the tedium then increases if one considers the family $\mathcal{X}_i$.

This thesis aims to enhance the understanding of modules systems within dependently-typed languages by developing an in-language framework for unifying disparate presentations of what are essentially the same module. Moreover, the framework will be constructed with *practicality* in mind so that the end-result is not an unusable theoretical claim.

2.10.2 Objectives and Methodology

To reach a framework for the modelling of module systems for DTLs, this thesis sets a number of objectives which are described below.

◇ **Objective 1: Modelling Module Systems**

The first objective is to actually develop a framework that models module systems —grouping mechanisms— within DTLs. The resulting framework should capture at least the expected features:

1. Namespacing, or definitional extensions
2. Opaque fields, or parameters
3. Constructors, or uninterpreted identifiers

Moreover, the resulting framework should be *practical* so as to be a usable experimentation-site for further research or immediate application —at least, in DTLs. In this thesis, we present two *declarative* approaches using meta-programming and `do`-notation.

◇ **Objective 2: Support Unexpected Notions of Module**

The second objective is to make the resulting framework *extensible*. Users should be able to form new exotic notions of grouping mechanisms *within* a DTL rather than 'stepping outside' of it and altering its interpreter —which may be a code implementation or an abstract rewrite-system. Ideally, users would be able to formulate arbitrary constructions from Universal Algebra and Category Theory. For example, given a theory —a notion of grouping— one would like to 'glue' two 'instances' along an 'identified common interface'. More concretely, we may want to treat some parameters as 'the same' and others as 'different' to obtain a new module that has copies of some parameters but not others. Moreover, users should be able to mechanically produces the necessary morphisms to make this construction into a pushout. Likewise, we would expect products, unions, intersections, and substructures of theories —when possible, and then to be constructed by users. In this thesis, we only want to provide a fixed set of meta-primitives from which usual and (un)conventional notions of grouping may be defined.

◇ **Objective 3: Provide a Semantics**

The third objective is to provide a semantics for the resulting framework. We propose to implement the framework in the dependently-typed functional programming language Agda, thereby automatically furnishing our syntactic constructs with semantics as Agda functions and types. This has the pleasant side-effect of making the framework accessible to future researchers for experimentation.

2.11 Contributions

The fulfilment of the objectives of this thesis leads to the following contributions.

1. The ability to model module systems *for* DTLs *within* DTLs

2. The ability to arbitrarily *extend* such systems by users at a high-level

3. Demonstrate that there is an expressive yet minimal set of module meta-primitives which allow common module constructions to be defined

4. Demonstrate that relationships between modules can also be *mechanically* generated.

   ◇ In particular, if module $\mathcal{B}$ is obtained by applying a user-defined 'variational' to module $\mathcal{A}$, then the user could also enrich the child module $\mathcal{B}$ with morphisms that describe its relationships to the parent module $\mathcal{A}$.

   ◇ E.g., if $\mathcal{B}$ is an extension of $\mathcal{A}$, then we may have a "forgetful mapping" that drops the new components; or if $\mathcal{B}$ is a 'minimal' rendition of the theory $\mathcal{A}$, then we have a "smart constructor" that forms the rich $\mathcal{A}$ by only asking the few $\mathcal{B}$ components of the user.

5. Demonstrate that there is a *practical* implementation of such a framework

6. Solve the unbundling problem: The ability to 'unbundle' module fields as if they were parameters 'on the fly'

7. Bring algebraic data types under the umbrella of grouping mechanisms: An ADT is just a context whose symbols target the ADT 'carrier' and are not otherwise interpreted.

   ◇ In particular, both an ADT and a record can be obtained from a *single* context declaration.

8. Show that common data-structures are *mechanically* the (free) termtypes of common modules.

   ◇ In particular, lists arise from modules modelling collections whereas nullables — the `Maybe` monad— arises from modules modelling pointed structures.

   ◇ Moreover, such termtypes also have a *practical* interface.

9. Finally, the resulting framework is *mostly type-theory agnostic*: The target setting is DTLs but we only assume the barebones as discussed in **??**; if users drop parts of that theory, then *only* some parts of the framework will no longer apply.

   ◇ For instance, in DTLs without a fixed-point functor the framework still 'applies', but can no longer be used to provide arbitrary algebraic data types from contexts.

Bibliography

[Ast+02] Egidio Astesiano et al. "CASL: the Common Algebraic Specification Language". In: *Theor. Comput. Sci.* 286.2 (2002), pp. 153–196. DOI: 10.1016/S0304-3975(01)00368-1. URL: https://doi.org/10.1016/S0304-3975(01)00368-1 (cit. on p. 38).

[Bal03] Clemens Ballarin. "Locales and Locale Expressions in Isabelle/Isar". In: *Types for Proofs and Programs, International Workshop, TYPES 2003, Torino, Italy, April 30 - May 4, 2003, Revised Selected Papers*. 2003, pp. 34–50. DOI: 10.1007/978-3-540-24849-1_3. URL: https://doi.org/10.1007/978-3-540-24849-1%5C_3 (cit. on p. 43).

[BD08] Ana Bove and Peter Dybjer. "Dependent Types at Work". In: *Language Engineering and Rigorous Software Development, International LerNet ALFA Summer School 2008, Piriapolis, Uruguay, February 24 - March 1, 2008, Revised Tutorial Lectures*. 2008, pp. 57–99. DOI: 10.1007/978-3-642-03153-3_2. URL: https://doi.org/10.1007/978-3-642-03153-3%5C_2 (cit. on p. 29).

[BDN09] Ana Bove, Peter Dybjer, and Ulf Norell. "A Brief Overview of Agda — A Functional Language with Dependent Types". In: *Theorem Proving in Higher Order Logics, 22nd International Conference, TPHOLs 2009, Munich, Germany, August 17–20, 2009. Proceedings*. 2009, pp. 73–78. DOI: 10.1007/978-3-642-03359-9_6 (cit. on p. 42).

[Car86] John Cartmell. "Generalised algebraic theories and contextual categories". In: *Ann. Pure Appl. Log.* 32 (1986), pp. 209–243. DOI: 10.1016/0168-0072(86)90053-9. URL: https://doi.org/10.1016/0168-0072(86)90053-9 (cit. on p. 24).

[CCH73] R. I. Chaplin, R. E. Crosbie, and J. L. Hay. "A Graphical Representation of the Backus-Naur Form". In: *Comput. J.* 16.1 (1973), pp. 28–29. DOI: 10.1093/comjnl/16.1.28. URL: https://doi.org/10.1093/comjnl/16.1.28 (cit. on p. 10).

[Cho59a] Noam Chomsky. "A Note on Phrase Structure Grammars". In: *Inf. Control.* 2.4 (1959), pp. 393–395. DOI: 10.1016/S0019-9958(59)80017-6. URL: https://doi.org/10.1016/S0019-9958(59)80017-6 (cit. on p. 10).

[Cho59b] Noam Chomsky. “On Certain Formal Properties of Grammars”. In: *Inf. Control.* 2.2 (1959), pp. 137–167. DOI: 10.1016/S0019-9958(59)90362-6. URL: https://doi.org/10.1016/S0019-9958(59)90362-6 (cit. on p. 10).

[Cla+07] Manuel Clavel et al., eds. *All About Maude - A High-Performance Logical Framework, How to Specify, Program and Verify Systems in Rewriting Logic*. Vol. 4350. Lecture Notes in Computer Science. Springer, 2007. ISBN: 978-3-540-71940-3. DOI: 10.1007/978-3-540-71999-1. URL: https://doi.org/10.1007/978-3-540-71999-1 (cit. on p. 43).

[Coq18] The Coq Development Team. *The Coq Proof Assistant, version 8.8.0*. Apr. 2018. DOI: 10.5281/zenodo.1219885. URL: https://hal.inria.fr/hal-01954564 (cit. on p. 43).

[DM07] Francisco Durán and José Meseguer. “Maude’s module algebra”. In: *Sci. Comput. Program.* 66.2 (2007), pp. 125–153. DOI: 10.1016/j.scico.2006.07.002. URL: https://doi.org/10.1016/j.scico.2006.07.002 (cit. on p. 43).

[GCS14] Jason Gross, Adam Chlipala, and David I. Spivak. *Experience Implementing a Performant Category-Theory Library in Coq*. 2014. arXiv: 1401.7694v2 [math.CT] (cit. on p. 43).

[GDF02] Guoyong, Peimin Deng, and Jiali Feng. “Specification based on Backus-Naur Formalism and Programming Language”. In: *The Third Asian Workshop on Programming Languages and Systems, APLAS’02, Shanghai Jiao Tong University, Shanghai, China, November 29 - December 1, 2002, Proceedings*. 2002, pp. 95–101 (cit. on p. 10).

[Kah18] Wolfram Kahl. *Relation-Algebraic Theories in Agda*. 2018. URL: http://relmics.mcmaster.ca/RATH-Agda/ (visited on 10/12/2018) (cit. on p. 2).

[Knu64] Donald E. Knuth. “backus normal form vs. Backus Naur form”. In: *Commun. ACM* 7.12 (1964), pp. 735–736. DOI: 10.1145/355588.365140. URL: https://doi.org/10.1145/355588.365140 (cit. on p. 10).

[KS01] Wolfram Kahl and Jan Scheffczyk. “Named Instances for Haskell Type Classes”. In: 2001 (cit. on p. 37).

[KWP99] Florian Kammüller, Markus Wenzel, and Lawrence C. Paulson. “Locales - A Sectioning Concept for Isabelle”. In: *Theorem Proving in Higher Order Logics, 12th International Conference, TPHOLs’99, Nice, France, September, 1999, Proceedings*. 1999, pp. 149–166. DOI: 10.1007/3-540-48256-3_11. URL: https://doi.org/10.1007/3-540-48256-3%5C_11 (cit. on p. 43).

[Lar+11] Jeroen F. J. Laros et al. “A formalized description of the standard human variant nomenclature in Extended Backus-Naur Form”. In: *BMC Bioinform.* 12.S-4 (2011), S5. DOI: 10.1186/1471-2105-12-S4-S5. URL: https://doi.org/10.1186/1471-2105-12-S4-S5 (cit. on p. 10).

[McB00] Conor McBride. “Dependently typed functional programs and their proofs”. PhD thesis. University of Edinburgh, UK, 2000. URL: http://hdl.handle.net/1842/374 (cit. on p. 29).

[McK06] James McKinna. "Why dependent types matter". In: *Proceedings of the 33rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2006, Charleston, South Carolina, USA, January 11-13, 2006*. 2006, p. 1. DOI: 10.1145/1111037.1111038. URL: http://doi.acm.org/10.1145/1111037.1111038 (cit. on p. 29).

[Nor07] Ulf Norell. "Towards a Practical Programming Language Based on Dependent Type Theory". See also http://wiki.portal.chalmers.se/agda/pmwiki.php. PhD thesis. Dept. Comp. Sci. and Eng., Chalmers Univ. of Technology, Sept. 2007 (cit. on p. 42).

[Pau] Christine Paulin-Mohring. "The Calculus of Inductive Definitions and its Implementation: the Coq Proof Assistant". In: invited tutorial (cit. on p. 43).

[Pie10] Brigitte Pientka. "Beluga: Programming with Dependent Types, Contextual Data, and Contexts". In: *Functional and Logic Programming, 10th International Symposium, FLOPS 2010, Sendai, Japan, April 19-21, 2010. Proceedings*. 2010, pp. 1–12. DOI: 10.1007/978-3-642-12251-4_1. URL: https://doi.org/10.1007/978-3-642-12251-4%5C_1 (cit. on p. 42).

[PT15] Frank Pfenning and The Twelf Team. *The Twelf Project*. 2015. URL: http://twelf.org/wiki/Main_Page (visited on 10/19/2018) (cit. on p. 43).

[Rab10] Florian Rabe. "Representing Isabelle in LF". In: *Electronic Proceedings in Theoretical Computer Science* 34 (Sept. 2010), pp. 85–99. ISSN: 2075-2180. DOI: 10.4204/eptcs.34.8. URL: http://dx.doi.org/10.4204/EPTCS.34.8 (cit. on p. 43).

[RS09] Florian Rabe and Carsten Schürmann. "A practical module system for LF". In: *Proceedings of the Fourth International Workshop on Logical Frameworks and Meta-Languages: Theory and Practice, LFMTP '09, McGill University, Montreal, Canada, August 2, 2009*. 2009, pp. 40–48. DOI: 10.1145/1577824.1577831. URL: https://doi.org/10.1145/1577824.1577831 (cit. on p. 43).

[SD02] Aaron Stump and David L. Dill. "Faster Proof Checking in the Edinburgh Logical Framework". In: *Automated Deduction - CADE-18, 18th International Conference on Automated Deduction, Copenhagen, Denmark, July 27-30, 2002, Proceedings*. 2002, pp. 392–407. DOI: 10.1007/3-540-45620-1_32. URL: https://doi.org/10.1007/3-540-45620-1%5C_32 (cit. on p. 43).

[UCB08] Christian Urban, James Cheney, and Stefan Berghofer. *Mechanizing the Metatheory of LF*. 2008. arXiv: 0804.1667v3 [cs.LO] (cit. on p. 43).

[WK18] Philip Wadler and Wen Kokke. *Programming Language Foundations in Agda*. 2018. URL: https://plfa.github.io/ (visited on 10/12/2018) (cit. on p. 29).