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

April 8, 2020

PhD Thesis

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

Abstract

Structuring-mechanisms, such as Java's `package` and Haskell's `module`, are often afterthought secondary citizens whose primary purpose is to act as namespace delimiters, while relatively more effort is given to their abstraction encapsulation counterparts, e.g., Java's classes and Haskell's typeclasses. A *dependently-typed language* (DTL) is a typed language where we can write *types* that depend on *terms*; thereby blurring conventional distinctions between a variety of concepts. In contrast, languages with non-dependent type systems tend to distinguish *external vs. internal* structuring-mechanisms —as in Java's `package` for namespacing vs. `class` for abstraction encapsulation— with more dedicated attention and power for the internal case —as it is expressible within the type theory.

To our knowledge, relatively few languages —such as Ocaml, Maude, and the B Method— allow for the manipulation of external structuring-mechanisms as they do for internal ones. Sufficiently expressive type systems, such as those of dependently typed languages, allow for the internalisation of many concepts thereby conflating a number of traditional programming notions. Since DTLs permit types that depend on terms, the types may require non-trivial term calculation in order to be determined. Languages without such expressive type systems necessitate certain constraints on its constructs according to their intended usage. It is not clear whether such constraints have been brought to more expressive languages out of necessity or out of convention. Hence we propose a systematic exploration of the structuring-mechanism design space for dependently typed languages to understand *what are the module systems for DTLs?*

First-class structuring-mechanisms have values and types of their own which need to be subject to manipulation by the user, so it is reasonable to consider manipulation combinators for them from the beginning. Such combinators would correspond to the many generic operations that one naturally wants to perform on structuring-mechanisms —e.g., combining them, hiding components, renaming components— some of which, in the external case, are impossible to perform in any DTL without resorting to third-party tools for pre-processing. Our aim is to provide a sound footing for systems of structuring-mechanisms so that structuring-mechanisms become another common feature in dependently typed languages. An important contribution of this work is an Agda implementation of our module combinators —which we hope to be accepted into a future release of the Agda standard library.

If anything, our aim is practical —to save developers from ad hoc copy-paste preprocessing hacks.

—Source: `https://github.com/alhassy/next-700-module-systems`—

Contents

1 Introduction —The Thesis' "Story" 3

1.1 A Language Has Many Tongues 4

1.2 Needless Distinctions for Containers 5

1.3 Novel Contributions 6

1.4 Overview of the Remaining Chapters 9

2 The First Choice —Why DTLs, Why Agda? 11

2.1 Why DTLs? 12

2.1.1 Example 1: Sanitising raw data 12

2.1.2 Example 2: Correct-by-Construction Programming 14

2.1.3 The Curry-Howard Correspondence —"Propositions as Types" 15

2.1.4 The trials and tribulations of working with dependent types 16

2.2 DTLs Today, a précis 17

2.2.1 Agda –"Haskell on steroids" 18

2.2.2 Coq —"The standard proof assistant" 18

2.2.3 Idris —"Agda with tactics" 19

2.2.4 Lean —"Proofs for metaprogramming" 20

2.2.5 ATS —"Dependent types for systems programming" 20

2.2.6 F* —"The immature adult" 20

2.2.7 Beluga —“Context notation” 21

2.2.8 Notable Mentions 21

2.3 A Whirlwind Tour of Agda 22

2.3.1 Dependent Functions 22

2.3.2 Dependent Datatypes 23

2.3.3 Propositional Equality 25

2.3.4 Calculational Proofs —Making Use of Unicode Mixfix Lexemes 25

2.3.5 Modules —Namespace Management 26

2.3.6 Records 27

2.3.7 Interacting with the real world —Compilation, Haskell, and IO 28

2.4 Facets of Structuring Mechanisms: An Agda Rendition 30

2.4.1 Three Ways to Define Monoids 31

2.4.2 Instances and Their Use 33

2.4.3 A Fourth Definition —Contexts 34

2.5 Comparing Modules in Coq then in Agda 37

2.5.1 A Brief Overview of Coq Modules, Part 1 37

2.5.2 A Brief Overview of Coq Modules, Part 2 44

3 TODO Sections not yet written 46

Glossary 46

References 47

Chapter 1

Introduction —The Thesis' "Story"

In this chapter we aim to present the narrative that demonstrates the distinction between what can currently be accomplished and what is desired when working with composition of software units. We arrive at the observation that packaging concepts differ only in their use —for example, a typeclass and a record are both sequences of declarations that only differ in that the former is used for polymorphism with instance search whereas the latter is used as a structure, grouping related items together. In turn, we are led to propose that the various packaging concepts ought to have a uniform syntax. Moreover, since records are a particular notion of packaging, the commitment to syntactic similarity gives rise to a homoiconic nature to the host language.

Within this work we refer to a *simple type theory* as a language that contains typed lambda terms for terms and formuale; if in addition it contains lambda terms whose types are indexed by values then we say it is a *dependently-typed language*, or 'DTL' for short — depending on intent, value-indexed types could be interpreted as *propositions* and their terms as *proofs*. With the exception of declarations and ephemeral notions, nearly everything in a DTL is a typed lambda term. Just as Lisp's homoiconic nature blurs data and code leaving it not as a language with primitives but rather a language with meta-primitives, so too the lack of distinction between term and type lends itself to generic and uniform concepts in DTLs thereby leaving no syntactic distinction between a constructive proof and an algorithm.

An introduction to Agda and dependent types can be found in §2.3

The sections below explore our primary observation. Section 1 demonstrates the variety of 'tongues' present in a single language which are conflated in a DTL, section 2 discusses that such conflation should by necessity apply to notions of packaging, section 3 contains contributed work to ensure that happens. Finally, section 4 concludes by outlining the remainder of the thesis.

1.1 A Language Has Many Tongues

A programming language is actually many languages working together.

The most basic of imperative languages comes with a notion of ‘statement’ that is executed by the computer to alter ‘state’ and a notion of ‘value’ that can be assigned to memory locations. Statements may be sequenced or looped, whereas values may be added or multiplied, for example. In general, the operations on one linguistic category cannot be applied to the other. Unfortunately, a rigid separation between the two sub-languages means that binary choice, for example, conventionally invites two notations with identical semantics —e.g.; in `C` one writes `if (cond) clause`$_1$ `else clause`$_2$ for statements but must use the notation `cond ? term`$_1$ `: term`$_2$ for values. Hence, there are value and statement languages.

Let us continue using the `C` language for our examples since it is so ubiquitous and has influenced many languages. Such a choice has the benefit of referring to a concrete language, rather than speaking in vague generalities. Besides Agda —our language of choice— we shall also refer to Haskell as a representative of the functional side of programming. For example, in Haskell there is no distinction between values and statements —the latter being a particular instance of the former— and so it uses the same notation `if` $\boxed{\ldots}$ `then` $\boxed{\ldots}$ `else` $\boxed{\ldots}$ for both. However, in practice, statements in Haskell are more pragmatically used as a body of a `do` block for which the rules of conditionals and local variables change —hence, Haskell is not as uniform as it initially appears.

In `C`, one declares an integer value by `int x;` but a value of a user-defined type `T` is declared `struct T x;` since, for simplicity, one may think of `C` having an array named `struct` that contains the definitions of user-defined types `T` and the notation `struct T` acts as an array access. Since this is a clunky notation, we can provide an alias using the declaration `typedef existing-name new-name;`. Unfortunately, the existing name must necessarily be a type, such as `struct T` or `int`, and cannot be an arbitrary term. One must use `#define` to produce term aliases, which are handled by the `C` preprocessor, which also provides `#include` to ‘copy-paste import’ existing libraries. Hence, the type language is distinct from the libraries language, which is part of the preprocessor language.

In contrast, Haskell has a pragma language for enabling certain features of the compiler. Unlike `C`, it has an interface language using type-`class`-es which differs from its `module` language [DJH; SHH01; She] since the former’s names may be qualified by the names of the latter but not the other way around. In turn, type-`class` names may be used as constraints on types, but not so with `module` names. It may be argued that this interface language is part of the type language, but it is sufficiently different that it could be thought of as its own language [Ler00] —for example, it comes with keywords `class, instance, =>` that can only appear in special phrases. In addition, by default, variable declarations are the same for built-in and user-defined types —whereas `C` requires using `typedef` to mimic such behaviour. However, Haskell distinguishes between term and type aliases. In contrast, Agda treats aliasing as nothing more than a normal definition.

Certain application domains require high degrees of confidence in the correctness of software. Such program verification settings may thus have an additional specification language. For `C`, perhaps the most popular is the ANSI C Specification Language, ACSL [BP10]. Besides the `C` types, ACSL provides a type `integer` for specifications referring to unbounded integers as well as numerous other notions and notations not part of the `C` language. Hence, the specification language generally differs from the implementation language. In contrast, Haskell's specifications are generally [Hal+] in comments but its relative Agda allows specifications to occur at the type level.

Whether programs actually meet their specifications ultimately requires a proof language. For example, using the Frama-C tool [VME18], ACSL specifications can be supported by Isabelle or Coq proofs. In contrast, being dependently-typed, Agda allows us to use the implementation language also as a proof language —*the only distinction is a shift in our perspective; the syntax is the same.* Tools such as Idris and Coq come with 'tactics' —algorithms which one may invoke to produce proofs— and may combine them using specific operations that only act on tactics, whence yet another tongue.

Hence, even the simplest of programming languages contain the first three of the following sub-languages —types may be treated at runtime.

1. Expression language;
2. Statement, or control flow, language;
3. Type language;
4. Specification language;
5. Proof language;
6. Module language;
7. Meta-programming languages —including Coq tactics, C preprocessor, Haskell pragmas, Template Haskell's various quotation brackets `[x| ... ]`, Idris directives, etc.

As briefly discussed, the first five languages telescope down into one uniform language within the dependently-typed language Agda. So why not the module language?

1.2 Needless Distinctions for Containers

Computing is compositionality. Large mind-bending software developments are formed by composing smaller, much more manageable, pieces together. How? In the previous section we outlined a number of languages equipped with term constructors, yet we did not indicate which were more primitive and which could be derived.

The methods currently utilised are ad hoc, e.g., "dump the contents of packages into a new über package". What about when the packages contain conflicting names? "Make an über package with field names for each package's contents". What about viewing the new über package as a hierarchy of its packages? "Make conversion methods between the two representations." These tedious and error-prone operations *should be* mechanically derivable.

In general, there are special-purpose constructs specifically for working with packages of "usual", or "day-to-day" expression- or statement-level code. That is, a language for working with containers whose contents live in another language. This forces the users to think of these constructs as rare notions that are seldom needed —since they belong to an ephemeral language. They are only useful when connecting packages together and otherwise need not be learned.

When working with mutually dependent modules, a simple workaround to cyclic type-checking and loading is to create an interface file containing the declarations that dependents require. To mitigate such error-prone duplication of declarations, one may utilise literate programming [Knu84] to tangle the declarations to multiple files —the actual parent module and the interface module. This was the situation with Haskell before its recent module signature mechanism [Kil+14]. Being a purely functional language, it is unsurprising that Haskell treats nested record field updates awkwardly: Where a C-like language may have `a.b.c := d`, Haskell requires `a { b = b a {c = d}}` which necessarily has field names `b, c` polluting the global function namespace as field projections. Since a record is a possibly deeply nested list of declarations, it is trivial to flatten such a list to mechanically generate the names `‘‘a-b-c’’` —since the dot is reserved— unfortunately this is not possible in the core language thereby forcing users to employ 'lenses' [Rom20] to generate such accessors by compile-time meta-programming. In the setting of DTLs, records in the form of nested Σ-types tend to have tremendously poor performance —in existing implementations of Coq [GCS14] and Agda [Per17], the culprit generally being projections. More generally, what if we wanted to do something with packages that the host language does not support? "Use a pre-processor, approximate packaging at a different language level, or simply settle with what you have."

Main Observation Packages, modules, theories, contexts, traits, typeclasses, interfaces, what have you all boil down to dependent records at the end of the day and *really differ* in *how* they are used or implemented. At the end of section 3 we demonstrate various distinct presentations of such notions of packaging arising from a single package declaration.

1.3 Novel Contributions

The thesis investigates the current state of the art of grouping mechanisms —sometimes referred to as modules or packages—, their shortcomings, and implementing candidate solutions based upon a dependently-typed language.

The introduction of first-class structuring mechanisms drastically changes the situation by allowing the composition and manipulation of structuring mechanisms within the language itself. Granted, languages providing combinators for structuring mechanisms are not new; e.g., such notions already exist for Full Maude [DM07] and B [BGL06]. The former is closer in spirit to our work, but it differs from ours in that it is based on a *reflective logic*: A logic where certain aspects of its metatheory can be faithfully represented within the logic itself. Not only does the meta-theory of our effort not involve reflection, but our distinctive attribute is that our aim is to form powerful module system features for Dependently-Typed Languages (DTLs).

To the uninitiated, the shift to DTLs may not appear useful, or at least would not differ much from existing approaches. We believe otherwise; indeed, in programming and, more generally, in mathematics, there are three —below: 1, 2a, 2b— essentially equivalent perspectives to understanding a concept. Even though they are equivalent, each perspective has prompted numerous programming languages; as such, the equivalence does not make the selection of a perspective irrelevant. The perspectives are below, and examples in the subsequent table.

1. "Point-wise" or "Constituent-Based": A concept is understood by studying the concepts it is "made out of".

   Common examples include:

   - *Extensionality*: A mathematical set is determined by the elements it contains.
   - A method is determined by the sequence of statements or expressions it is composed from.
   - A package —such as a record or data declaration— is determined by its components, which may be *thought of* as fields or constructors.

   Object-oriented programming is based on the notion of inheritance which is founded on the "has a" and "is a" relationships.

2. "Point-free" or Relationship Based: A concept is understood by its relationship to other concepts in the domain of discourse.

   This approach comes into two sub-classifications:

   (a) "First Class Citizen" or "Concept as Data": The concept is treated as a static entity and is identified by applying operations *onto it* in order to observe its nature.

   Common examples include:

   - A singleton set is a set whose cardinality is 1.
   - A method, in any coding language, is a value with the ability to act on other values of a particular type.
   - A renaming scheme to provide different names for a given package; more generally, applicative modules.

(b) "Second Class Citizen" or "Concept as Method": The concept is treated as a dynamic entity that is fed input stimuli and is understood by its emitted observational output.

Common examples include:

- ⋄ A singleton set is a set for which there is a unique mapping to it from any other set. Input any set, obtain a map from it to the singleton set.
- ⋄ A method, in any coding language, is unique up to observational equality: Feed it arguments, check its behaviour. Realistically, one may want to also consider efficiency matters.
- ⋄ Generative modules as in the `new` keyword from object-oriented programming: Basic construction arguments are provided and a container object is produced.

Observing such a sub-classification as distinct led to traditional structural programming languages, whereas blurring the distinction somewhat led to functional programming.

Table 1.1: Four ways to percieve 'the' empty collection $\emptyset$, and associated theory

(1)	Extensional	$\mathtt{X} = \emptyset \equiv (\forall\ \mathtt{e} \bullet \mathtt{e} \in \mathtt{X} \equiv \mathtt{false})$	Predicate Logic
(2)	Intensional	$\mathtt{X} = \emptyset \equiv (\forall\ \mathtt{Y} \bullet \mathtt{X} \subseteq \mathtt{Y})$	Set Theory
(2a)	Data	$\mathtt{X} = \emptyset \equiv \mathtt{\#X} = \mathtt{0}$	Numbers-as-Sets
(2b)	Method	$\mathtt{X} = \emptyset \equiv (\forall\ \mathtt{Y} \bullet \exists_1\ \mathtt{f} \bullet \mathtt{f} \in (\mathtt{X} \to \mathtt{Y}))$	Function Theory

A simple selection of equivalent perspectives leads to wholly distinct paradigms of thought. It is with this idea that we seek to implement first-class grouping mechanisms in a dependently typed language —theories have been proposed, on paper, but as just discussed *actual design decisions may have challenging impacts on the overall system.* Most importantly, this is a *requirements driven* approach to coherent modularisation constructs in dependently typed languages.

Later on, we shall demonstrate that with a sufficiently expressive type system, a number of traditional programming notions regarding 'packaging up data' become conflated —in particular: Records and modules; which for the most part can all be thought of as "dependent products with named components". Languages without such expressive type systems necessitate certain constraints on these concepts according to their intended usage —e.g., no multiple inheritance for Java's classes and only one instance for Haskell's typeclasses. It is not clear whether such constraints have been brought to more expressive languages out of necessity, convention, or convenience. Hence, in chapter 3, we perform a systematic exploration of the structuring-mechanism design space for DTLs as a starting point for the design of an appropriate dependently-typed module system (§ 3). Along the way, we intend to provide a set of atomic combinators that suffice as building blocks for generally desirable features of grouping mechanisms, and moreover we intend to provide an analyses of their interactions.

That is, we want to look at the edge cases of the design space for structuring-mechanism *systems*, not only what is considered convenient or conventional. Along the way, we will undoubtedly encounter useless or non-feasible approaches. The systems we intend to consider would account for, say, module structures with intrinsic types —hence treating them as first class concepts— so that our examination is based on sound principles.

Understandably, some of the traditional constraints have to do with implementations. For example, a Haskell typeclass is generally implemented as a dictionary that can, for the most part, be inlined whereas a record is, in some languages, a contiguous memory block: They can be identified in a DTL, but their uses force different implementation methodologies and consequently they are segregated under different names.

In summary, our research builds upon the existing state of module systems [DCH03] in a dependently-typed setting [Mac86] which is substantiated by developing practical and pragmatic tools. Our outcomes include:

1. A clean module system for DTLs that treats modules uniformly as any other value type.
2. A variety of use-cases contrasting the resulting system with previous approaches.
   - ◇ We solve the so-called unbundling problem and demonstrate —using our implemented tools— how pushout and homomorphisms constructions, among many others, can be *mechanically* obtained.
3. A module system that enables rather than inhibits efficiency.
4. Demonstrate that module features traditionally handled using meta-programming can be brought to the data-value level; thereby not actually requiring the immense power and complexity of meta-programming.

Most importantly, we have implemented our theory thereby obtaining validation that it ‘works’. We provide an extensible Emacs interface as well as an Agda library for forming module constructions.

1.4 Overview of the Remaining Chapters

When a programming languages does not provide sufficiently expressive primitives for a concept —such as typeclass derivation [BLS18]— users use some form of pre-processing to accomplish their tasks. In our case, the insufficient primitives are regarding the creation and manipulation of theories —i.e., records, classes, packages, modules. In section 3 , we will demonstrate an prototype that clarified the requirements of our envisioned system. Even though the prototype appears to be metaprogramming, the aim is not to force users interested in manipulating packages to worry about the intricacies of representations; that is, the end goal is to avoid metaprogramming —which is an over-glorified form of preprocessing. The goal is to *use a dependently-typed language to implement the ‘missing’ module system features directly inside the language.*

An important design decision is whether the resulting development is intended to be reasoned about or not. If reasoning is important, then a language that better supports it is ideal. That is why we are using Agda —using a simpler language and maintaining data invariants eventually becomes much harder [LM13].

The remainder of the thesis is organised as follows.

- ◇ **§3 Examples from the wild**

  There are a host of repeated module patterns since modules are not a first-class construct. We look at three Agda libraries and extract "module design patterns for dependently-typed programming". To the best of our knowledge, we are the first to formalise such design patterns for dependently-typed languages. Three other, non-module, design patterns are discussed in [OS08].

- ◇ **§3 Metaprogramming Module Meta-primitives**

  To show that first-class modules are *reasonable*, we begin by providing `PackageFormer` [ACK19]: A specfication and manipulation language for modules, for Agda. To show that the approach is promising, we demonstrate how some problems from §3 can be tackled.

  - ○ The tool is a **practical** sandbox for exploring do-it-yourself grouping mechanisms: From pushouts and pullbacks, to forming homomorphism types over a given theory.

- ◇ **§3 Module Meta-primitives as Library Methods**

  The ideas learned from making the powerful `PackageFormer` prototype lead us to form the less-powerful `Context` framework, which has the orthogonal benefit of being an Agda library rather than an external pre-processing tool.

  - ○ Along the way, we solve the **unbundling problem**: Features of a structure may be exposed at the type level as-needed.

- ◇ **§3 Conclusion: The lingua franca dream as reality**

  We compare the external `PackageFormer` tool with the `Context` library, and discuss how the latter has brought us closer to our original goal of having a single language for expressing values, types, and modules.

It has been an exciting journey, I hope you enjoy the ride!

Chapter 2

The First Choice —Why DTLs, Why Agda?

Programming language communities whose language has a powerful type system, such as Haskell's, have proverbs such as "if it typechecks, ship it!" Such phrases are mostly in praise of the language's impressive type system. However, the motto is not flawless; e.g., consider [McB04] the Haskell term `if null xs then tail xs else xs` —it typechecks, but crashes at run time since empty lists have no (strictly smaller) tail. Dependently typed languages (DTLs) provide a static means of expressing the significance of particular values in legitimising some computations rather than others.

Dependent-types provide an immense level of expressivity thereby allowing varying degrees of precision to be embedded, or omitted, from the type of a declaration. This overwhelming degree of freedom comes at the cost of common albeit non-orthogonal styles of coding and compilation, which remain as open problems that are only mitigated by awkward workarounds such as Coq's distinction of types and propositions for compilation efficiency. The difficulties presented by DTLs are outweighed by the opportunities they provide [AMM05] —of central importance is that they blur distinctions between usual programming constructs [Mac86], which is in alignment with our thesis.

> The *purpose* of this section is to establish the necessary foundational aspects of dependently-typed languages (DTLs) by reviewing the existing DTLs and narrowing on Agda in particular.

Rather than dictatorially declare that Agda is the ideal setting for our research, we shall consider the possible candidates —only after arguing that dependently-typed languages provide power, and complexity, for our tasks. Having decided to use Agda, we provide a quick tutorial on the language and on dependent types. Finally, we conclude with demonstrating our observation of "all packaging mechanisms are essentially the same" formally through Agda examples by simulating different grouping constructs in the language.

2.1 Why DTLs?

In this section, we argue that dependently-typed languages constitute a poorly understood domain in comparison to their more popular counterparts, such as the functional language Haskell and the imperative language JavaScript. To keep the discussion self-contained, we first provide a quick, informal, overview of the power allotted by dependent types —a more formal introduction, backed by typechecked code, is presented later in §2.3.

Dependent-types allow us to encode properties of data *within the structure* of the data itself, and so all the data we consider is necessarily 'well-formed'. In contrast, without dependent types, one would (1) declare a data structure, *then* (2) define the subclass of such data that is 'well-formed' in some sense; *then*, (3) to work with this data, one provides an interface that only produces well-formed data, a so-called 'smart constructor', *finally*, one needs to test that their smart constructor actually only forms well-defined data elements. For instance, raw untyped λ-terms are not all sensible, and so one introduces types to organise them into sensible classes, then introduces inference rules that ensure only sensible terms are constructed.

> DTLs flatten the conventional four-stage process of declaring raw data, selecting a coherent subclass, providing a smart constructor, and proving the constructor is valid.

We shall explain this idea more concretely via two examples, in the following two sections. The Agda fragments presented will be explained in the accompanying text —an introduction to Agda is given in §2.3. Afterword, we conclude by briefly mentioning theoretical concerns when working with DTLs and, more importantly for topic on modularisation, issues of a more practical nature involving library development.

2.1.1 Example 1: Sanitising raw data

When interacting with users, a system receives raw data then 'sanitises' it, or ensures it is 'sanitised'. For instance, to subscribe to a mailing list, a user provides a string of symbols which the program then ensures it is a well-formatted email address. Below is a possible implementation of the email address portion within Haskell —the comments are a designers thought process as *allowed* by the coding language.

Traditional Four Stages to Structuring Data

```
{- (1) An email address is just a raw string -}
data Email = MkEmail String  deriving Show

{- (2) Actually, it has some structure -}
isValid :: Email -> Bool
isValid (MkEmail s) = let pre_rest = splitOn "@" s
                      in length pre_rest == 2
                      && length (splitOn ".com" (pre_rest !! 1)) == 1

{- (3) Given two strings, we can form an email address -}
mkEmail :: String -> String -> Email
mkEmail pre post = MkEmail (pre ++ "@" ++ post ".com")

{- (4) Also, mkEmail is a smart constructor for Email -}
{- ∀ pre post • isValid (mkEmail pre post)        -}
```

With dependent types, we can *encode* structural[1] properties: We can declare a type of strings necessarily of the form ⟨`string`⟩`@`⟨`string`⟩`.com`, thereby dispensing with any sanitation phase. In particular, in this style, a parser is essentially a type-checker. Moreover such checks happen at compile time since these are just like any other type.

Parsing ≈ Typechecking

```
data Email : String → Set where
  MkEmail : (pre post : String) → Email (pre ++ "@" ++ post ++ ".com")
```

The above declaration defines a new type `Email s` with values `MkEmail pre post` *precisely when* `s ≈ pre ++ "@" ++ post ++ ".com"`. Hence, any value of `Email s` is, by its very construction, a pair of strings, say, `pre` and `post` that compose to give the original address `s`. The above four steps in Haskell have been reduced to a single declaration in Agda.

What happened exactly? Where are the dependent-types? Let `X` denote the type of strings, `Y` the type of pairs of strings, `P` the property "x is composed of the pair y", and the lower-case `p` is the proviso in the Haskell code above. Let $\mathcal{Y}$ absorp the proviso property `p` —in the Agda code, this amounts to "building `p` into the type"— so that `y` $\in \mathcal{Y}$`(x)` $\equiv$ `p(x, y)`. Then the transition from specification, to Haskell implementation, to Agda code can be summarised in the following chain of equalities.

$$
\begin{array}{ll}
 & \textit{Every email address decomposes into a pair of strings} \\
\approx & \forall\ \mathtt{x} : \mathtt{X} \bullet \exists\ \mathtt{y} : \mathtt{Y} \bullet \mathtt{p(x,\ y)} \wedge \mathtt{P(x,\ y)} \\
\approx & \forall\ \mathtt{x} : \mathtt{X} \bullet \exists\ \mathtt{y} : \mathcal{Y}\mathtt{(x)} \bullet \mathtt{P(x,\ y)}
\end{array}
$$

[1] Arbitrary, semantic, properties can be attached to data constructors. However, properties encoded via syntactic structure can be mechanically checked via typechecking. Whereas needing *a proof of a property* may require human intervention.

The type $\mathcal{Y}$ is a dependent type: It is a type that *depends* on a term; namely, `x`.

When claims only hold under certain expected premises, it would be easier to reason and state the claims if such preconditions were incorporated into the types. This is common practice in mathematics —e.g., "the maximum operation over real numbers has a least element when *only considering* non-negative whole numbers" versus "the maximum operation *on naturals* has a least element"; i.e., mathematicians *declare a new set* $\mathbb{N} = \{r : \mathbb{R} \mid r \geq 0 \wedge \lceil r \rceil = r\}$. However, in conventional programming, there is no way to *form such a new type* denoting "the values of type A that satisfy property B"; unless you have access to dependent types, which call this type Σ `a : A • B(a)`.

2.1.2 Example 2: Correct-by-Construction Programming

Program verification is an 'after the fact' activity, like documentation; yet when a project behaves as desired, programmers seldom willingly go back to clean up and instead prefer a new project. This dissociation of concerns is remedied by enabling program verification to proceed side-by-side with development [Gri81; Coh90; Dij76]: Each proof of a program property acts as exhaustive test cases for that property.

With a careful specification of the type, there is only one program!

For example, suppose we want an implementation of a function f specified by the property `f 0 = 1 ∧ f (n + 1) = n × f n`, for any `n`. The first conjunct completely determines `f` on input `0`, however an inattentive implementer may decide to define `f n := f (n + 1) / n`. The resulting 'definition' clearly satisfies the specification, but it does not terminate on any positive input since it recursively calls itself on ever increasing arguments!

In comparison, since Agda requires all its functions to be terminating, after insisting the specification obligations hold by definition, `refl`, we turn to defining `f` by pattern matching and its implementation from there is fully forced: There are no more choices in implementation! Then, Agda's Emacs 'proof finder' Agsy automates the definition of `f`: There is only one road to defining `f` so that the constraints hold by 'refl'exivity —i.e., by definition.

Correct-by-Construction Programming

```
factorial :  Σ f : (ℕ → ℕ) •  f 0 ≡ 1 × (∀ {n} →  f (1 + n)  ≡  n * f n)
factorial = f , refl , refl
  where f : ℕ → ℕ
        f zero    = 1
        f (suc n) = n * f n
```

By utilising dependent types, run time errors —failures occurring during program execution, such as non-emptiness or well-formedness conditions— are transported to compile time, which are errors caught during typechecking. This is in itself a tremendously amazing feature.

Dependent types enable all errors, including logical errors, to become type checking errors!

Regarding the middle clause, *including logical errors*, suppose we are interested in a utility function whose inputs must be even numbers, or rather any commutable precondition `p`. In simpler type systems, such as JavaScript's, we could throw an exception if the input does not satisfy it or simply return a `null`, which need then needs to be handled at the call site by using conditionals or try-catch blocks. Instead of all of this explicit plumbing, DTLs allow us to define types and let the compiler handle the grunt work. That is, in a DTL we could encode the precondition directly into the function's type.

2.1.3 The Curry-Howard Correspondence —"Propositions as Types"

The Curry-Howard Correspondence makes a dependently-typed programming language a also a proof assistant: A proposition is proved by writing a program of the corresponding type.

Logic	**Programming**		Example Use in Programming
proof / proposition	element / type		"p is a proof of P" ≈ "p is of type P"
true	singleton type		return type of side-effect only methods
false	empty type		return type for non-terminating methods
$\Rightarrow$	function type	$\to$	methods with an input and output type
$\land$	product type	$\times$	simple records of data and methods
$\lor$	sum type	$+$	enumerations or tagged unions
$\forall$	dependent function type	Π	return type varies according to input *value*
$\exists$	dependent product type	Σ	record fields depend on each other's *values*
natural deduction	type system		ensuring only "meaningful" programs
hypothesis	free variable		global variables, closures
modus ponens	function application		executing methods on arguments
$\Rightarrow$ -introduction	λ-abstraction		parameters acting as local variables to method definitions
induction; elimination rules	Structural recursion		`for`-loops are precisely $\mathbb{N}$-induction

Let's augment the table a bit to relate concepts that we shall refer to in later sections.

Logic	**Programming**
Signature, term	Syntax; interface, record type, `class`
Algebra, Interpretation	Semantics; implementation, instance, object
Free Theory	Data structure
Inference rule	Algebraic datatype constructor
Monoid	Untyped programming / composition
Category	Typed programming / composition

2.1.4 The trials and tribulations of working with dependent types

Since a *dependently-typed language* is a typed language —i.e., a formal syntactic grammar and associated type system— where we can write *types* that depend on *terms*; consequently types may require non-trivial term calculation in order to be determined [McK06]. A glaring drawback is that types now depend on term calculations thereby rendering type checking, and type inference, to be difficult if not impossible [Dow93]. E.g., later we shall define the type `Vec A n` of lists of elements of `A` having length `n`, then, for instance, `Vec String (factorial 100)` is the type of really long lists of strings —the length will take some time to calculate.

Unsurprisingly, "doing" dependent typing "right" is still an open issue [Bra05; Bla10; LMS10; Bra; Wei]. In particular, after more than 30 years after Martin-Löf's work on the type theory [Mar85; MS84], it is still unclear how such typing should be implemented so that the result is usable and well-founded. Of interest is Agda which claims to have achieved this desired ground but, in reality, it is seldom used as a programming language due to efficiency issues; in contrast, Idris aims at efficiency but its use as a proof assistant is somewhat lacking in comparison to Agda. Below are a few other issues that demonstrate the non-triviality of problems in dependently-typed languages.

1. Should programs be total for the sake of consistency or can they be partially defined?
2. Do we allow the "Type in Type" axiom [Rus; Alt; Car; Luo90]?
3. What about "Axiom K" expressing *almost* the recursion scheme of identity types [Str93; McB00a; CDP14; GMM06; McB00b; HS94; Wer08]}?
4. Should dependent pattern matching give us more information about a type? How does this interact with side effects?
5. Should unification be proof-relevant; i.e., to consider the *ways* in which terms can be made equal [CD18]?
6. How do subtypes, which classically require proof irrelevance, tie into the paradigm?
7. How does proof-term erasure work [TB; BMM03; MS08; Has15]}?
8. When are two values, or programs, or types equal: When they have the same type?

9. Should a language permit non-termination or require explicit co-data?

Besides technical concerns, there are also pressing practical concerns. Since dependent types blur the distinction between value and type —thereby conflating many traditional programming concepts— library design becomes pretty delicate.

- ◇ For example, the method that extracts the first element of a list can in traditional languages be assigned usually two types —one with an explicit exception decoration such as Haskell's `Maybe` or C#'s `Nullable`, or without this and instead throwing an (implicit) exception. In addition, in a DTL, we can instead decorate the list with a positive length to avoid exceptions altogether, or request a non-emptiness proof, or output a dependent pair consisting of a proof that the input list is non-empty and, if so, an element of that list, or do we request as input a dependent pair consisting of a list and a non-emptiness proof —note that this is a Σ-type, in contrast to the curried form from earlier—, or $\cdots$.
- ◇ Moreover, when a function is written *which* properties should be attached to the resulting type and which should be stated separately?

  For example, if we write an append function for lists, do we separately prove that the length of an append is the sum of the lengths of its arguments, or do we encode that information into the return type by means of a dependent pair?

Hence programming style becomes vastly more important in DTLs since simple functions can have a diverse set of typings. In particular, this can lead to 'duplication' of code: Dependently-typed and simply typed variants of the 'same' concept, as well as the methods & proofs that operate on them; e.g., ℕ-indexed vectors vs. lists, [KG13; BG13; McB]. So much for the DRY[2] Principle. Since in a DTL records and modules are conflated, perhaps the structuring-mechanism combinators resulting from this research could reduce some of the 'duplication'.

We, as a community, are decidedly still learning about the role of dependent types in programming!

2.2 DTLs Today, a précis

We want to implement solutions in a dependently typed language. Let us discuss which are active and their capabilities.

To the best of our knowledge, as confirmed by Wikipedia [18b; 18a], there are currently less than 15 *actively developed* dependently-typed languages in-use *that are also used* as proof-assistants —which are interesting to us since we aim to mechanise all of our results:

[2] Don't Repeat Yourself

Algorithms as well as theorems. Below is a quick summary of our stance on the primary candidates.

Language	Primary reason it is not used in-place of Agda
Coq	Tactics reinforce a fictitious divide between propositions and types
Idris	Records can be parameterised but not indexed
Lean	Rapid development of Lean has left is backward incompatible and unstable
ATS	Weak module system
F*, Beluga	The language is immature; it has little support

2.2.1 Agda –"Haskell on steroids"

Agda [BDN09; Nor07] is one of the more popular proof assistants around; possibly due to its syntactic inheritance from Haskell —as is the case with Idris. Its Unicode mixfix lexemes permit somewhat faithful renditions of informal mathematics; e.g., calculational proofs can be encoded in seemingly informal style that they can be easily read by those unfamiliar with the system. It also allows traditional functional programming with the ability to 'escape under the hood' and write Haskell code. The language has not been designed solely with theorem proving in mind, as is the case for Coq, but rather has been designed with dependently-typed programming in mind [Jef13; WK18].

The current implementation of the Agda language 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 change in perspective allows Agda records to act as Haskell typeclasses. However, the relationship with Haskell is only superficial: Agda's current implementation does not support sharing. In particular, a parameterised module is only syntactic sugar such that each member of the module actually obtains a new functional parameter; as such, a computationally expensive parameter provided to a module invocation may be intended to be computed only once, but is actually computed at each call site.

2.2.2 Coq —"The standard proof assistant"

Coq [Pau; GCS14] is unquestionably one of, if not, the most popular proof assistant around. It has been used to produce mechanised proofs of the infamous Four Colour Theorem [Gon], the Feit-Thompson Theorem [Gon+13], and an optimising compiler for the C language: CompCert [Com18; KLW14].

Unlike Agda, Coq supports tactics [Asp+] —a brute force approach that renders (hundredfold) case analysis as child's play: Just refine your tactics till all the subgoals are achieved. Ultimately the cost of utilising tactics is that a tactical proof can only be understood with the aid of the system, and may otherwise be un-insightful and so failing to meet most of the purposes of proof [Far18] —which may well be a large barrier for mathematicians who value insightful proofs.

The current implementation of Coq provides the base features expected of any module system. A notable difference from Agda is that it allows to "copy and paste" contents of modules using the `include` keyword. Consequently it provides a number of module combinators, such as `<+` which is the infix form of module inclusion [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 [Cla+07; DM07] framework contains a similar yet more comprehensive algebra of modules and how they work with Maude theories.

As the oldest proof assistant, in a later section we shall compare and contrast its module system with Agda's to some depth.

2.2.3 Idris —"Agda with tactics"

Idris [Bra11] is a general purpose, functional, programming language with dependent types. Alongside ATS, below, it is perhaps the only language in our list that can truthfully boast to being general purpose and to have dependent types. It supports both equational and tactic based proof styles, like Agda and Coq respectively; unlike these two however, Idris erases unused proof-terms automatically rather than forcing the user to declare this far in advance as is the case with Agda and Coq. The only (negligible) downside, for us, is that the use of tactics creates a sort of distinction between the activities of proving and programming, which is mostly fictitious.

Intended to be a more accessible and practical version of Agda, Idris implements the base module system features and includes interesting new ones. Until recently, in Agda, one would write `module _ (x : ℕ) where ···` to parameterise every declaration in the block ı···ȷ by the name `x`; whereas in Idris, one writes `parameters (x : ℕ) ···` to obtain the same behaviour —which Agda has since improved upon it via 'generalisation': A declaration's type gets only the variables it actually uses, not every declared parameter.

Other than such pleasantries, Idris does not add anything of note. However, it does provide new constraints. As noted earlier, the current implementation of Idris attempts to erase implicits aggressively therefore providing speedup over Agda. In particular, Idris modules and records can be parameterised but not indexed —a limitation not in Agda.

Unlike Coq, Idris has been designed to "emphasise general purpose programming rather than theorem proving" [Idr18; Bra16]. However, like Coq, Idris provides a Haskell-looking typeclasses mechanism; but unlike Coq, it allows named instances. In contrast to Agda's record-instances, typeclasses result in backtracking to resolve operator overloading thereby having a slower type checker.

2.2.4 Lean —"Proofs for metaprogramming"

Lean [Mou+15; Mou16] is both a theorem prover and programming language; moreover it permits quotient types and so the usually-desired notion of extensional equality. It is primarily tactics-based, also permitting a `calc`-ulational proof format not too dissimilar with the standard equational proof format utilised in Agda.

Lean is based on a version of the Calculus of Inductive Constructions, like Coq. It is heavily aimed at metaprogramming for formal verification, thereby bridging the gap between interactive and automated theorem proving. Unfortunately, inspecting the language shows that its rapid development is not backwards-compatible —Lean 2 standard libraries have yet to be ported to Lean 3—, and unlike, for example, Coq and Isabelle which are backed by other complete languages, Lean is backed by Lean, which is unfortunately too young to program various tactics, for example.

2.2.5 ATS —"Dependent types for systems programming"

ATS, the Applied Type System [ATS18; CX05], is a language that combines programming and proving, but is aimed at unifying programming with formal specification. With the focus being more on programming than on proving.

ATS is intended as an approach to practical programming with theorem proving. Its module system is largely influenced by that of Modula-3, providing what would today be considered the bare bones of a module system. Advocating a programmer-centric approach to program verification that syntactically intertwines programming and theorem proving, ATS is a more mature relative of Idris —whereas Idris is Haskell-based, ATS is OCaml-based.

ATS is remarkable in that its performance is comparable to that of the C language, and it supports secure memory management by permitting type safe pointer arithmetic. In some regard, ATS is the fusions of Ocaml, C, and dependent types. Its module system has less to offer than Coq's.

2.2.6 F* —"The immature adult"

The F* [F T18] language supports dependent types, refinement types, and a weakest precondition calculus. However it is primarily aimed at program verification rather than general proof. Even though this language is roughly nine years in the making, it is not mature —one encounters great difficult in doing anything past the initial language tutorial.

The module system of F* is rather uninteresting, predominately acting as namespace management. It has very little to offer in comparison to Agda; e.g., within the last three years, it obtained a typeclass mechanism —regardless, typeclasses can be simulated as dependent records.

2.2.7 Beluga —“Context notation”

The distinctive feature and sole reason that we mention this language is its direct support for first-class contexts [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 we have mentioned, and will reiterate a few times, contexts are behaviourally indistinguishable from dependent sums.

A displeasure of Beluga is that, while embracing the Curry-Howard Correspondence, it insists on two syntactic categories: Data and computation. This is similar to Coq’s distinction of `Prop` and `Type`. Another issue is that to a large degree the terms one uses in their type declarations are closed and so have an empty context therefore one sees expressions of the form `[ |- t ]` since `t` is a closed term needing only the empty context. At a first glance, this is only a minor aesthetic concern; yet after inspection of the language’s webpage, tutorials, and publication matter, it is concerning that nearly all code makes use of empty contexts —which are easily spotted visually. The tremendous amount of empty contexts suggests that the language is not actually making substantial use of the concept, or it is yet unclear what pragmatic utility is provided by contexts, and, in either way, they might as well be relegated to a less intrusive notation. Finally, the language lacks any substantial standard libraries thereby rendering it more as a proof of concept rather than a serious system for considerable work.

2.2.8 Notable Mentions

The following are not actively being developed, as far we can tell from their websites or source repositories, but are interesting or have made useful contributions.

- ◇ 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’ [Bal03; KWP99]; unfortunately it is not a dependently-typed language —though DTLs can be implemented in it.
- ◇ Mizar, unlike the above, is based on (untyped) Tarski–Grothendieck set theory which in some-sense has a hierarchy of sets. Like Coq, it has a large library of formalised mathematics [Miz18; NK09; Ban+18].
- ◇ Developed in the early 1980s, Nuprl [PRL14] is constructive with a refinement-style logic; besides being a mature language, it has been used to provide proofs of problems related to Girard’s Paradox [Coq86].

- ◇ PVS, Prototype Verification System [Sha+01], differs from other DTLs in its support for subset types; however, the language seems to be unmaintained as of 2014.
- ◇ Twelf [PT15] is a logic programming language implementing Edinburgh's Logical Framework [UCB08; Rab10; SD02] and has been used to prove safety properties of 'real languages' such as SML. A notable practical module system [RS09] for Twelf has been implemented using signatures and signature morphisms.
- ◇ Matita [Asp+06; Mat16] is a Coq-like system that is much lighter [Asp+09]; it is been used for the verification of a complexity-preserving C compiler.

Dependent types are mostly visible within the functional community, however this is a matter of taste and culture as they can also be found in imperative settings, [Nan+08], albeit less prominently.

2.3 A Whirlwind Tour of Agda

Agda [McK06; McB00a; BD08; WK18] is based on Martin-Löf's intuitionistic type theory. By identifying types with terms, the type of small types is a larger type; e.g., ℕ : $\texttt{Set}_0$ and $\texttt{Set}_i$: $\texttt{Set}_{i+1}$ —the indices `i` are called *levels* and the small type $\texttt{Set}_0$ is abbreviated as `Set`. In some regard, Agda adds *harmonious* support for dependent types to Haskell.

Unlike most languages, Agda not only allows arbitrary mixfix Unicode lexemes, identifiers, but their use is encouraged by the community as a whole. Almost anything can be a valid name; e.g., `[]` and `_::_` to denote list constructors —underscores are used to indicate argument positions. Hence it is important to be liberal with whitespace; e.g., `e:τ` is a valid identifier, whereas `e : τ` declares term `e` to be of type τ. Agda's Emacs interface allows entering Unicode symbols in traditional LaTeX-style; e.g., `\McN`, `\_7`, `\::`, `\to` are replaced by 𝒩, ₇, ::, →. Moreover, the Emacs interface allows programming by gradual refinement of incomplete type-correct terms. One uses the "hole" marker `?` as a placeholder that is used to stepwise write a program.

2.3.1 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} → ⋯` 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) → ⋯
```

2.3.2 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:* Set$_n$ has type Set$_{n+1}$ *for any n*, however the *type* (n : Level) → Set n is *not* itself typeable —i.e., is not in Set$_l$ for any l— and Agda errors saying it is a value of Setω.

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 ++⟶+ 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.

2.3.3 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!

2.3.4 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
QED
```

Calculational Proof Syntax Embedded As Proof Forming Functions

```
infixr 5 _≡⟨_⟩_
infix  6 _QED

_QED : {A : Set} (a : A) → a ≡ a
_ QED = 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 *QED*)). We can code this up, as show above on the right.

2.3.5 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

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.

2.3.6 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.

`record` ≈ `module` + `data` 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.

2.3.7 Interacting with the real world —Compilation, Haskell, and IO

In order to be useful, a program must interact with the real world. Agda relegates the work to Haskell. The only concept here that is used in later sections will be Agda's do-notation, and so the purpose of this section is to demonstrate how to use it in a real scenario.

An Agda program module containing a `main` function is compiled into a standalone executable with `agda --compile myfile.agda`. If the module has no main file, use the flag `--no-main`. If you only want the resulting Haskell, not necessarily an executable program, then use the flag `--ghc-dont-call-ghc`.

The type of `main` should be `Agda.Builtin.IO.IO A`, for some `A`; this is just a proxy to Haskell's `IO`. We may `open import IO.Primitive` to get *this* `IO`, but this one works with costrings, which are a bit awkward. Instead, we use the standard library's wrapper type, also named `IO`. Then we use `run` to move from `IO` to `Primitive.IO`; conversely one uses `lift`.

Necessary Imports

```
open import Data.Nat                         using (ℕ; suc)
open import Data.Nat.Show                    using (show)
open import Data.Char                        using (Char)
open import Data.List as L                   using (map; sum; upTo)
open import Function                         using (_$_; const; _∘_)
open import Data.String as S                 using (String; _++_; fromList)
open import Agda.Builtin.Unit                using (⊤)
open import Codata.Musical.Colist            using (take)
open import Codata.Musical.Costring          using (Costring)
open import Data.BoundedVec.Inefficient as B using (toList)
open import Agda.Builtin.Coinduction using (SHARP_)
open import IO as IO                         using (run ; putStrLn ; IO)
import IO.Primitive as Primitive
```

*Agda has **no** primitives for side-effects, instead it allows arbitrary Haskell functions to be imported as axioms, whose definitions are only used at run-time.*

Agda lets us use do-notation as in Haskell. To do so, methods named `_≫_` and `_≫=_` need to be in scope —that is all. The type of `IO._≫_` takes two "lazy" IO actions and yield a non-lazy IO action. The one below is a homogeneously typed version.

Non-lazy Do-combinators

```
infixr 1 _>>=_ _>>_

_>>=_ : ∀ {ℓ} {α β : Set ℓ} → IO α → (α → IO β) → IO β
this >>= f = SHARP this IO.>>= λ x → SHARP f x

_>>_ : ∀{ℓ} {α β : Set ℓ} → IO α → IO β → IO β
x >> y = x >>= const y
```

Oddly, Agda's standard library comes with `readFile` and `writeFile`, but the symmetry ends there since it provides `putStrLn` but not `getLine`. Mimicking the `IO.Primitive` module, we define *two* versions ourselves as proxies for Haskell's `getLine` —the second one below is bounded by 100 characters, whereas the first is not.

Postulating Foreign Haskell Functions

```
postulate
  getLine∞ : Primitive.IO Costring

{-# FOREIGN GHC
  toColist :: [a] -> MAlonzo.Code.Codata.Musical.Colist.AgdaColist a
  toColist []       = MAlonzo.Code.Codata.Musical.Colist.Nil
  toColist (x : xs) =
    MAlonzo.Code.Codata.Musical.Colist.Cons x (MAlonzo.RTE.Sharp (toColist xs))
#-}

{- Haskell's prelude is implicitly available; this is for demonstration. -}
{-# FOREIGN GHC import Prelude as Haskell #-}
{-# COMPILE GHC getLine∞  = fmap toColist Haskell.getLine #-}

-- (1)
-- getLine : IO Costring
-- getLine = IO.lift getLine∞

getLine : IO String
getLine = IO.lift
  $ getLine∞ Primitive.>>= (Primitive.return ∘ S.fromList ∘ B.toList ∘ take 100)
```

We obtain `MAlonzo` strings, then convert those to colists, then eventually lift those to the wrapper `IO` type.

Let's also give ourselves Haskell's `read` method.

Postulating Haskell's 'read'

```
postulate readInt  : L.List Char → ℕ
{-# COMPILE GHC readInt = \x -> read x :: Integer  #-}
```

Now we write our `main` method.

An Agda Program: Triangle Numbers with IO

```
main : Primitive.IO ⊤
main = run do putStrLn "Hello, world! I'm a compiled Agda program!"

              putStrLn "What is your name?"
              name ← getLine

              putStrLn "Please enter a number."
              num ← getLine
              let tri = show $ sum $ upTo $ suc $ readInt $ S.toList num
              putStrLn $ "The triangle number of " ++ num ++ " is " ++ tri

              putStrLn "Bye, "
              -- IO.putStrLn∞ name  {- If we use approach (1) above. -}
              putStrLn $ "\t" ++ name
```

For example, the 12^{th} triangle number is $\sum_{i=0}^{12} i = 78$. Interestingly, when an integer parse fails, the program just crashes.

Calling this file `CompilingAgda.agda`, we may compile then run it with:

Compiling The Program

```
NAME=CompilingAgda; time agda --compile $NAME.agda; ./$NAME
```

The very first time you compile may take ∼80 seconds since some prerequisites need to be compiled, but future compilations are within ∼10 seconds. The generated Haskell source lives under the newly created MAlonzo directory; namely `./MAlonzo/Code/CompilingAgda.hs`.

2.4 Facets of Structuring Mechanisms: An Agda Rendition

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.

2.4.1 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 [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 [Ast+02] and so programs may be written according to one view, but easily repurposed for other view with little human intervention.

2.4.2 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. #+LaTeX:

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 proj$_1$ 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.

2.4.3 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[3] bundled. Additionally, if we insert a Σ before each name we essentially regain the `Monoid-Σ` 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.

[3] 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.

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 _+_ (+-identity^l _) (+-identity^r _) +-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 3 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.

2.5 Comparing Modules in Coq then in Agda

Module systems parameterise programs, proofs, and tactics over structures. In the first section below, we shall form a library simple graphs and show how to work with it in both Coq and Agda. In order to demonstrate that *all packaging concepts essentially coincide in a DTL*, we shall only use the `record` construct in Agda —completely ignoring the `data` and `module` forms which would otherwise be more natural in certain scenarios below. In the second section below, we look at a few technical aspects of Coq modules.

Along the way, we shall flesh out our concerns regarding using Coq:

1. Modules and their types are explicitly given their own language.
    - They have their own syntax.
2. Tactics hide any insight in proofs, and decrease readability.

Agda packaging mechanisms will be given less attention, since they were covered in previous sections.

2.5.1 A Brief Overview of Coq Modules, Part 1

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, 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.
```

Let go through the proof of `decidable`.

1. λ-introduce the quantified variables `x, y` with `intros`.
2. We rewrite the definition of `Edges` into the Boolean valued order on Booleans, then rewrite that definition as well.
3. We perform case analysis on `x` and on `y` with `destruct`.
4. There are now a number of subgoals —to find out which, one must interact with the system— and so we use the `all:` tactic to provide a recipe to handle them.
    (a) Try to prove the `right` part of the sum `{x <= y} + {not (x <= y)}`;
    (b) Otherwise, if we explicitly `fail`, try to prove the `left` part.

In contrast, in Agda, we explicitly λ-introduce the variables and immediately perform case analysis; then use `C-c C-a` to have the cases automatically filled it.

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 define 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

```
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

```
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

```
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

```
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

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.

2.5.2 A Brief Overview of Coq Modules, Part 2

Coq modules are essentially Agda records —which is unsurprising since our thesis states packaging containers are all essentially the same. In more detail, both notions coincide with that of a signature —a sequence of pairs of name-type declarations. Where Agda users would speak of a *record instance*, Coq users would speak of a *module implementation*. To make matters worse, Coq has a notion of records which are far weaker than Agda's; e.g., by default all record field names are globally exposed and records are non-recursive.

Coq's module system extends that of Ocaml; a notable divergence is that Coq permits parameterised module types —i.e., parameterised record types, in Agda parlance. Such module types are also known as 'functors' by Coq and Ocaml users; which are "generative": Invocations generate new datatypes. Perhaps an example will make this rather strange concept more apparent.

Example of Generative Functors

```
Module Type Unit. End Unit.
Module TT <: Unit. End TT.

Module F (X : Unit).
  Inductive t : Type := MakeT.
End F.

Module A := F TT.
Module B := F TT.
Fail Check eq_refl : A.t = B.t.
```

Corresponding Agda Code

```
record Unit : Set where
tt : Unit; tt = record {}

module F (X : Unit) where
  data t : Set where MakeT : t

module A = F tt
module B = F tt

eq : A.t ≡ B.t
eq = refl
```

As seen, in Coq the inductive types are different yet in Agda they are the same. This is because Agda treats such parameterised records, or functors, as 'applicative': They can only be applied, like functions. Coq's modules η-expand and so aliasing does nothing, but functors do not η-reduce, and as such one cannot expect them to be applicative, and so are generative. For simplicity, we may think of generative functor applications `F X` as actually `F X t` where `t` is an implicit tag such as textual position or clock time. From an object-oriented programming perspective, `F X` for a generative functor `F` is like the `new` keyword in Java/C#: A new instance is created which is distinct from all other instances even though the same class is utilised. So much for the esotericity of generative functors.

Unlike Agda, which uses records to provide traditional record types, Haskell-like typeclasses, and even a module perspective of both, Coq utilises distinct mechanisms for typeclasses and canonical structures. In contrast, Agda allows named instances since all instances are named and can be provided where an implicit failed to be found. Moreover, Coq's approach demands greater familiarity with the unifer than Agda's approach.

Chapter 3

TODO Sections not yet written

Glossary

context A sequence of “variable : type” declarations; a dictionarry associating variables to types; c.f., record-type and object-oriented class. 33

Curry-Howard Correspondence Programming and proving are essentially the same idea. 14

Dependent Function A function whose result type depends on the value of the argument. 21

do-notation Syntactic abbrevation that renders purely functional code as if it were sequential and imperative.. 27

homoiconic The lack of distinction between ‘data’ and ‘method’. E.g., `'(+ 1 2)` is considered a list of symbols, whereas the *unquoted* term `(+ 1 2)` is considered a function call that reduces to 3. 2

Module systems Module systems parameterise programs, proofs, and tactics over structures. 36

record Rather than holding a bunch of items in our hands and running around with them, we can put them in a bag and run around with it. That is, a record type bundles up related concepts so that may be treated as one coherent entity. If record types can ‘inherit’ from one another, then we have the notion of an ‘object’. 2

signature A sequence of pairs of name-type declarations; an alias for ‘context’ and ‘telescope’. 43

typeclass Essentially a dictionary that associates types with a particular list of methods which define the typeclass. Whenever such a method is invoked, the dictionary is accessed for the inferred type and the appropriate definition is used, if possible. This provides a form of ad-hoc polymorphism: We have a list of methods that appear polymorphic, but in-fact their definitions depend on a particular parent type. 2

Bibliography

[18a] *Dependent type — Wikipedia, The Free Encyclopedia*. 2018. URL: https://en.wikipedia.org/wiki/Dependent_type (visited on 10/19/2018) (cit. on p. 17).

[18b] *Proof assistant — Wikipedia, The Free Encyclopedia*. 2018. URL: https://en.wikipedia.org/wiki/Proof_assistant (visited on 10/19/2018) (cit. on p. 17).

[ACK19] Musa Al-hassy, Jacques Carette, and Wolfram Kahl. "A language feature to unbundle data at will (short paper)". In: *Proceedings of the 18th ACM SIGPLAN International Conference on Generative Programming: Concepts and Experiences, GPCE 2019, Athens, Greece, October 21-22, 2019*. Ed. by Ina Schaefer, Christoph Reichenbach, and Tijs van der Storm. ACM, 2019, pp. 14–19. ISBN: 978-1-4503-6980-0. DOI: 10.1145/3357765.3359523. URL: https://doi.org/10.1145/3357765.3359523 (cit. on p. 10).

[Alt] Thorsten Altenkirch. *Inconsistency of Set:Set*. URL: http://www.cs.nott.ac.uk/~psztxa/g53cfr/l20.html/l20.html (visited on 10/19/2018) (cit. on p. 16).

[AMM05] Thorsten Alkenkirch, Conor McBride, and James McKinna. *Why Dependent Types Matter*. 2005. URL: http://www.cs.nott.ac.uk/~psztxa/publ/ydtm.pdf (visited on 10/19/2018) (cit. on p. 11).

[Asp+] Andrea Asperti et al. *A new type for tactics*. URL: http://matita.cs.unibo.it/PAPERS/plmms09.pdf (visited on 10/19/2018) (cit. on p. 18).

[Asp+06] Andrea Asperti et al. "Crafting a Proof Assistant". In: *Types for Proofs and Programs, International Workshop, TYPES 2006, Nottingham, UK, April 18-21, 2006, Revised Selected Papers*. 2006, pp. 18–32. DOI: 10.1007/978-3-540-74464-1_2. URL: https://doi.org/10.1007/978-3-540-74464-1%5C_2 (cit. on p. 22).

[Asp+09] A. Asperti et al. "A compact kernel for the calculus of inductive constructions". In: *Sadhana* 34.1 (Feb. 2009), pp. 71–144. ISSN: 0973-7677. DOI: 10.1007/s12046-009-0003-3. URL: http://dx.doi.org/10.1007/s12046-009-0003-3 (cit. on p. 22).

[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. 33).

[ATS18] The ATS Team. *The ATS Programming Language: Unleashing the Potentials of Types and Templates!* 2018. URL: http://www.ats-lang.org/#What_is_ATS_good_for (visited on 10/19/2018) (cit. on p. 20).

[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. 21).

[Ban+18] Grzegorz Bancerek et al. "The Role of the Mizar Mathematical Library for Interactive Proof Development in Mizar". In: *J. Autom. Reasoning* 61.1-4 (2018), pp. 9–32. DOI: 10.1007/s10817-017-9440-6. URL: https://doi.org/10.1007/s10817-017-9440-6 (cit. on p. 21).

[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. 22).

[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. 18).

[BG13] Jean-Philippe Bernardy and Moulin Guilhem. "Type-theory in Color". In: *SIGPLAN Not.* 48.9 (Sept. 2013), pp. 61–72. ISSN: 0362-1340. DOI: 10.1145/2544174.2500577. URL: http://doi.acm.org/10.1145/2544174.2500577 (cit. on p. 17).

[BGL06] Sandrine Blazy, Frédéric Gervais, and Régine Laleau. "Reuse of Specification Patterns with the B Method". In: *CoRR* abs/cs/0610097 (2006). arXiv: cs/0610097. URL: http://arxiv.org/abs/cs/0610097 (cit. on p. 7).

[Bla10] Michael Blaguszewski. "Implementing and Optimizing a Simple, Dependently-Typed Language". MA thesis. Chalmers University of Technology, 2010. URL: http://publications.lib.chalmers.se/records/fulltext/124826.pdf (cit. on p. 16).

[BLS18] Baldur Blöndal, Andres Löh, and Ryan Scott. "Deriving via: or, how to turn hand-written instances into an anti-pattern". In: *Proceedings of the 11th ACM SIGPLAN International Symposium on Haskell, Haskell@ICFP 2018, St. Louis, MO, USA, September 27-17, 2018*. 2018, pp. 55–67. DOI: 10.1145/3242744.3242746. URL: https://doi.org/10.1145/3242744.3242746 (cit. on p. 9).

[BMM03] Edwin Brady, Conor McBride, and James McKinna. "Inductive Families Need Not Store Their Indices". In: *Types for Proofs and Programs, International Workshop, TYPES 2003, Torino, Italy, April 30 - May 4, 2003, Revised Selected Papers*. 2003, pp. 115–129. DOI: 10.1007/978-3-540-24849-1_8. URL: https://doi.org/10.1007/978-3-540-24849-1%5C_8 (cit. on p. 16).

[BP10] Eduardo Brito and Jorge Sousa Pinto. "Program Verification in SPARK and ACSL: A Comparative Case Study". In: *Reliable Software Technologiey - Ada-Europe 2010, 15th Ada-Europe International Conference on Reliable Software Technologies, Valencia, Spain, June 14-18, 2010. Proceedings*. 2010, pp. 97–110. DOI: 10.1007/978-3-642-13550-7_7. URL: https://doi.org/10.1007/978-3-642-13550-7%5C_7 (cit. on p. 5).

[Bra] Edwin Brady. *Lectures on Implementing Idris*. URL: https://www.idris-lang.org/dependently-typed-functional-programming-with-idris-course-videos-and-slides/ (visited on 10/19/2018) (cit. on p. 16).

[Bra05] Edwin Brady. "Practical implementation of a dependently typed functional programming language". PhD thesis. Durham University, UK, 2005. URL: http://etheses.dur.ac.uk/2800/ (cit. on p. 16).

[Bra11] Edwin C. Brady. "IDRIS — Systems Programming Meets Full Dependent Types". In: *Proceedings of the 5th ACM workshop on Programming languages meets program verification*. PLPV '11. Austin, Texas, USA: ACM, 2011, pp. 43–54. ISBN: 978-1-4503-0487-0. DOI: http://doi.acm.org/10.1145/1929529.1929536. URL: http://doi.acm.org/10.1145/1929529.1929536 (cit. on p. 19).

[Bra16] Edwin Brady. *Type-driven Development With Idris*. Manning, 2016. ISBN: 9781617293023. URL: http://www.worldcat.org/isbn/9781617293023 (cit. on p. 19).

[Car] Luca Cardelli. *A polymorphic λ-calculus with Type:Type*. URL: http://lucacardelli.name/Papers/TypeType.A4.pdf (visited on 10/19/2018) (cit. on p. 16).

[CD18] Jesper Cockx and Dominique Devriese. "Proof-relevant unification: Dependent pattern matching with only the axioms of your type theory". In: *J. Funct. Program.* 28 (2018), e12. DOI: 10.1017/S095679681800014X. URL: https://doi.org/10.1017/S095679681800014X (cit. on p. 16).

[CDP14] Jesper Cockx, Dominique Devriese, and Frank Piessens. "Pattern matching without K". In: *Proceedings of the 19th ACM SIGPLAN international conference on Functional programming, Gothenburg, Sweden, September 1-3, 2014*. 2014, pp. 257–268. DOI: 10.1145/2628136.2628139. URL: http://doi.acm.org/10.1145/2628136.2628139 (cit. on p. 16).

[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. 19).

[Coh90] Edward Cohen. *Programming in the 1990s - An Introduction to the Calculation of Programs*. Texts and Monographs in Computer Science. Springer, 1990. ISBN: 978-0-387-97382-1. DOI: 10.1007/978-1-4613-9706-9. URL: https://doi.org/10.1007/978-1-4613-9706-9 (cit. on p. 14).

[Com18] The Compcert Team. *The Compcert C Compiler*. 2018. URL: http://compcert.inria.fr/compcert-C.html (visited on 10/19/2018) (cit. on p. 18).

[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. 19).

[Coq86] Thierry Coquand. "An Analysis of Girard's Paradox". In: *Proceedings of the Symposium on Logic in Computer Science (LICS '86), Cambridge, Massachusetts, USA, June 16-18, 1986*. 1986, pp. 227–236 (cit. on p. 21).

[CX05] Chiyan Chen and Hongwei Xi. "Combining programming with theorem proving". In: *Proceedings of the 10th ACM SIGPLAN International Conference on Functional Programming, ICFP 2005, Tallinn, Estonia, September 26-28, 2005*. 2005, pp. 66–77. DOI: 10.1145/1086365.1086375. URL: http://doi.acm.org/10.1145/1086365.1086375 (cit. on p. 20).

[DCH03] Derek Dreyer, Karl Crary, and Robert Harper. "A type system for higher-order modules". In: *Conference Record of POPL 2003: The 30th SIGPLAN-SIGACT Symposium on Principles of Programming Languages, New Orleans, Louisisana, USA, January 15-17, 2003*. 2003, pp. 236–249. DOI: 10.1145/640128.604151. URL: https://doi.org/10.1145/640128.604151 (cit. on p. 9).

[Dij76] Edsger W. Dijkstra. *A Discipline of Programming*. Prentice-Hall, 1976. ISBN: 013215871X. URL: http://www.worldcat.org/oclc/01958445 (cit. on p. 14).

[DJH] Iavor S. Diatchki, Mark P. Jones, and Thomas Hallgren. "A formal specification of the Haskell 98 module system". In: pp. 17–28. URL: http://doi.acm.org/10.1145/581690.581692 (cit. on p. 4).

[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 pp. 7, 19).

[Dow93] Gilles Dowek. "The Undecidability of Typability in the Lambda-Pi-Calculus". In: *Typed Lambda Calculi and Applications, International Conference on Typed Lambda Calculi and Applications, TLCA '93, Utrecht, The Netherlands, March 16-18, 1993, Proceedings*. 1993, pp. 139–145. DOI: 10.1007/BFb0037103. URL: https://doi.org/10.1007/BFb0037103 (cit. on p. 16).

[F T18] The F* Team. *F* Official Website*. 2018. URL: https://www.fstar-lang.org/ (visited on 10/19/2018) (cit. on p. 20).

[Far18] William M. Farmer. *A New Style of Proof for Mathematics Organized as a Network of Axiomatic Theories*. 2018. arXiv: 1806.00810v2 [cs.LO] (cit. on p. 19).

[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 pp. 6, 18).

[GMM06] Healfdene Goguen, Conor McBride, and James McKinna. "Eliminating Dependent Pattern Matching". In: *Algebra, Meaning, and Computation, Essays Dedicated to Joseph A. Goguen on the Occasion of His 65th Birthday*. 2006, pp. 521–540. DOI: 10.1007/11780274_27. URL: https://doi.org/10.1007/11780274%5C_27 (cit. on p. 16).

[Gon] Georges Gonthier. *Formal Proof–The Four-Color Theorem.* URL: http://www.ams.org/notices/200811/ (visited on 10/19/2018) (cit. on p. 18).

[Gon+13] Georges Gonthier et al. "A Machine-Checked Proof of the Odd Order Theorem". In: *Interactive Theorem Proving - 4th International Conference, ITP 2013, Rennes, France, July 22-26, 2013. Proceedings*. 2013, pp. 163–179. DOI: 10.1007/978-3-642-39634-2_14. URL: https://doi.org/10.1007/978-3-642-39634-2%5C_14 (cit. on p. 18).

[Gri81] David Gries. *The Science of Programming*. Texts and Monographs in Computer Science. Springer, 1981. ISBN: 978-0-387-96480-5. DOI: 10.1007/978-1-4612-5983-1. URL: https://doi.org/10.1007/978-1-4612-5983-1 (cit. on p. 14).

[Hal+] Thomas Hallgren et al. "An Overview of the Programatica Toolset". In: *HCSS '04*. URL: http://www.cse.ogi.edu/PacSoft/projects/programatica/ (cit. on p. 5).

[Has15] Philipp Haselwarter. "Towards a Proof-Irrelevant Calculus of Inductive Constructions". MA thesis. 2015. URL: http://www.haselwarter.org/~philipp/piCoq.pdf (cit. on p. 16).

[HS94] Martin Hofmann and Thomas Streicher. "The Groupoid Model Refutes Uniqueness of Identity Proofs". In: *Proceedings of the Ninth Annual Symposium on Logic in Computer Science (LICS '94), Paris, France, July 4-7, 1994*. 1994, pp. 208–212. DOI: 10.1109/LICS.1994.316071. URL: https://doi.org/10.1109/LICS.1994.316071 (cit. on p. 16).

[Idr18] The Idris Team. *Idris: Frequently Asked Questions*. 2018. URL: http://docs.idris-lang.org/en/latest/faq/faq.html (visited on 10/19/2018) (cit. on p. 19).

[Jef13] Alan Jeffrey. "Dependently Typed Web Client Applications - FRP in Agda in HTML5". In: *Practical Aspects of Declarative Languages - 15th International Symposium, PADL 2013, Rome, Italy, January 21-22, 2013. Proceedings*. 2013, pp. 228–243. DOI: 10.1007/978-3-642-45284-0_16. URL: https://doi.org/10.1007/978-3-642-45284-0%5C_16 (cit. on p. 18).

[KG13] Hsiang-Shang Ko and Jeremy Gibbons. "Relational Algebraic Ornaments". In: *Proceedings of the 2013 ACM SIGPLAN Workshop on Dependently-typed Programming*. DTP '13. Boston, Massachusetts, USA: ACM, 2013, pp. 37–48. ISBN: 978-1-4503-2384-0. DOI: 10.1145/2502409.2502413. URL: http://doi.acm.org/10.1145/2502409.2502413 (cit. on p. 17).

[Kil+14] Scott Kilpatrick et al. "Backpack: retrofitting Haskell with interfaces". In: *The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014*. 2014, pp. 19–32. DOI: 10.1145/2535838.2535884. URL: https://doi.org/10.1145/2535838.2535884 (cit. on p. 6).

[KLW14] Robbert Krebbers, Xavier Leroy, and Freek Wiedijk. "Formal C Semantics: CompCert and the C Standard". In: *Interactive Theorem Proving - 5th International Conference, ITP 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings.* 2014, pp. 543–548. DOI: 10.1007/978-3-319-08970-6_36. URL: https://doi.org/10.1007/978-3-319-08970-6%5C_36 (cit. on p. 18).

[Knu84] Donald E. Knuth. "Literate Programming". In: *Comput. J.* 27.2 (1984), pp. 97–111. DOI: 10.1093/comjnl/27.2.97. URL: https://doi.org/10.1093/comjnl/27.2.97 (cit. on p. 6).

[KS01] Wolfram Kahl and Jan Scheffczyk. "Named Instances for Haskell Type Classes". In: 2001 (cit. on p. 32).

[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. 21).

[Ler00] Xavier Leroy. "A modular module system". In: *J. Funct. Program.* 10.3 (2000), pp. 269–303. DOI: 10.1017/S0956796800003683 (cit. on p. 4).

[LM13] Sam Lindley and Conor McBride. "Hasochism: the pleasure and pain of dependently typed haskell programming". In: *Proceedings of the 2013 ACM SIGPLAN Symposium on Haskell, Boston, MA, USA, September 23-24, 2013.* 2013, pp. 81–92. DOI: 10.1145/2503778.2503786. URL: https://doi.org/10.1145/2503778.2503786 (cit. on p. 10).

[LMS10] Andres Löh, Conor McBride, and Wouter Swierstra. "A Tutorial Implementation of a Dependently Typed Lambda Calculus". In: *Fundam. Inform.* 102.2 (2010), pp. 177–207. DOI: 10.3233/FI-2010-304. URL: https://doi.org/10.3233/FI-2010-304 (cit. on p. 16).

[Luo90] Zhaohui Luo. "An extended calculus of constructions". PhD thesis. University of Edinburgh, UK, 1990. URL: http://hdl.handle.net/1842/12487 (cit. on p. 16).

[Mac86] David B. MacQueen. "Using Dependent Types to Express Modular Structure". In: *Conference Record of the Thirteenth Annual ACM Symposium on Principles of Programming Languages, St. Petersburg Beach, Florida, USA, January 1986.* 1986, pp. 277–286. DOI: 10.1145/512644.512670. URL: https://doi.org/10.1145/512644.512670 (cit. on pp. 9, 11).

[Mar85] P. Martin-Löf. "Constructive Mathematics and Computer Programming". In: *Proc. Of a Discussion Meeting of the Royal Society of London on Mathematical Logic and Programming Languages.* London, United Kingdom: Prentice-Hall, Inc., 1985, pp. 167–184. ISBN: 0-13-561465-1. URL: http://dl.acm.org/citation.cfm?id=3721.3731 (cit. on p. 16).

[Mat16] The Matita Team. *The Matita Interactive Theorem Prover.* 2016. URL: http://matita.cs.unibo.it (visited on 10/19/2018) (cit. on p. 22).

[McB] Conor McBride. “Ornamental Algebras, Algebraic Ornaments”. In: *Unpublished Draft* (). URL: https://personal.cis.strath.ac.uk/conor.mcbride/pub/OAAO/Ornament.pdf (visited on 10/19/2018) (cit. on p. 17).

[McB00a] 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 pp. 16, 22).

[McB00b] Conor McBride. “Elimination with a Motive”. In: *Types for Proofs and Programs, International Workshop, TYPES 2000, Durham, UK, December 8-12, 2000, Selected Papers*. 2000, pp. 197–216. DOI: 10.1007/3-540-45842-5_13. URL: https://doi.org/10.1007/3-540-45842-5%5C_13 (cit. on p. 16).

[McB04] Conor McBride. “Epigram: Practical Programming with Dependent Types”. In: *Advanced Functional Programming, 5th International School, AFP 2004, Tartu, Estonia, August 14-21, 2004, Revised Lectures*. Ed. by Varmo Vene and Tarmo Uustalu. Vol. 3622. Lecture Notes in Computer Science. Springer, 2004, pp. 130–170. ISBN: 3-540-28540-7. DOI: 10.1007/11546382_3. URL: https://doi.org/10.1007/11546382%5C_3 (cit. on p. 11).

[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 pp. 16, 22).

[Miz18] The Mizar Team. *Mizar Home Page*. 2018. URL: http://www.mizar.org/ (visited on 10/19/2018) (cit. on p. 21).

[Mou+15] Leonardo Mendonça de Moura et al. “The Lean Theorem Prover (System Description)”. In: *Automated Deduction - CADE-25 - 25th International Conference on Automated Deduction, Berlin, Germany, August 1-7, 2015, Proceedings*. 2015, pp. 378–388. DOI: 10.1007/978-3-319-21401-6_26. URL: https://doi.org/10.1007/978-3-319-21401-6%5C_26 (cit. on p. 20).

[Mou16] Leonardo de Moura. “Formalizing Mathematics using the Lean Theorem Prover”. In: *International Symposium on Artificial Intelligence and Mathematics, ISAIM 2016, Fort Lauderdale, Florida, USA, January 4-6, 2016*. 2016. URL: http://isaim2016.cs.virginia.edu/papers/ISAIM2016%5C_Proofs%5C_DeMoura.pdf (cit. on p. 20).

[MS08] Nathan Mishra-Linger and Tim Sheard. “Erasure and Polymorphism in Pure Type Systems”. In: *Foundations of Software Science and Computational Structures, 11th International Conference, FOSSACS 2008, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2008, Budapest, Hungary, March 29 - April 6, 2008. Proceedings*. 2008, pp. 350–364. DOI: 10.1007/978-3-540-78499-9_25. URL: https://doi.org/10.1007/978-3-540-78499-9%5C_25 (cit. on p. 16).

[MS84] P. Martin-Löf and G. Sambin. *Intuitionistic type theory*. Studies in proof theory. Bibliopolis, 1984. URL: https://books.google.ca/books?id=%5C_DOZAQAAIAAJ (cit. on p. 16).

[Nan+08] Aleksandar Nanevski et al. "Ynot: dependent types for imperative programs". In: *Proceeding of the 13th ACM SIGPLAN international conference on Functional programming, ICFP 2008, Victoria, BC, Canada, September 20-28, 2008*. 2008, pp. 229–240. DOI: 10.1145/1411204.1411237. URL: http://doi.acm.org/10.1145/1411204.1411237 (cit. on p. 22).

[NK09] Adam Naumowicz and Artur Kornilowicz. "A Brief Overview of Mizar". In: *Theorem Proving in Higher Order Logics, 22nd International Conference, TPHOLs 2009, Munich, Germany, August 17-20, 2009. Proceedings*. 2009, pp. 67–72. DOI: 10.1007/978-3-642-03359-9_5. URL: https://doi.org/10.1007/978-3-642-03359-9%5C_5 (cit. on p. 21).

[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. 18).

[OS08] Nicolas Oury and Wouter Swierstra. "The Power of Pi". In: *Proceedings of the 13th ACM SIGPLAN International Conference on Functional Programming*. ICFP '08. Victoria, BC, Canada: Association for Computing Machinery, 2008, pp. 39–50. ISBN: 9781595939197. DOI: 10.1145/1411204.1411213. URL: https://doi.org/10.1145/1411204.1411213 (cit. on p. 10).

[Pau] Christine Paulin-Mohring. "The Calculus of Inductive Definitions and its Implementation: the Coq Proof Assistant". In: invited tutorial (cit. on p. 18).

[Per17] Natalie Perna. *(Re-)Creating sharing in Agda's GHC backend*. Jan. 2017. URL: https://macsphere.mcmaster.ca/handle/11375/22177 (cit. on p. 6).

[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. 21).

[PRL14] The PRL Team. *PRL Project: Proof/Program Refinment Logic*. 2014. URL: http://www.nuprl.org (visited on 10/19/2018) (cit. on p. 21).

[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. 22).

[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. 22).

[Rom20] Mario Román. *Profunctor optics and traversals*. 2020. arXiv: 2001.08045v1 [cs.PL] (cit. on p. 6).

[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. 22).

[Rus] Bertrand Russell. *Mathematical Logic as Based on the Theory of Types*. URL: https://fi.ort.edu.uy/innovaportal/file/20124/1/37-russell1905.pdf (visited on 10/19/2018) (cit. on p. 16).

[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. 22).

[Sha+01] Natarajan Shankar et al. *PVS Prover Guide*. 2001. URL: http://pvs.csl.sri.com/doc/pvs-prover-guide.pdf (visited on 04/19/2019) (cit. on p. 22).

[She] Tim Sheard. "Generic Unification via Two-Level Types and Parameterized Modules". In: *ICFP 2001*. to appear. acm press (cit. on p. 4).

[SHH01] Tim Sheard, William Harrison, and James Hook. "Modeling the Fine Control of Demand in Haskell." (submitted to Haskell workshop 2001). 2001 (cit. on p. 4).

[Str93] Thomas Streicher. "Investigations Into Intensional Type Theory". PhD thesis. 1993. URL: https://www2.mathematik.tu-darmstadt.de/~streicher/HabilStreicher.pdf (cit. on p. 16).

[TB] Matus Tejiscak and Edwin Brady. "Practical Erasure in Dependently Typed Languages". In: *Unpublished Draft* (). URL: https://eb.host.cs.st-andrews.ac.uk/drafts/dtp-erasure-draft.pdf (visited on 10/19/2018) (cit. on p. 16).

[UCB08] Christian Urban, James Cheney, and Stefan Berghofer. *Mechanizing the Metatheory of LF*. 2008. arXiv: 0804.1667v3 [cs.LO] (cit. on p. 22).

[VME18] Grigoriy Volkov, Mikhail U. Mandrykin, and Denis Efremov. "Lemma Functions for Frama-C: C Programs as Proofs". In: *CoRR* abs/1811.05879 (2018). arXiv: 1811.05879. URL: http://arxiv.org/abs/1811.05879 (cit. on p. 5).

[Wei] Stephanie Weirich. *2014 OPLSS Lectures* Designing Dependently-Typed Programming Languages. URL: https://www.cs.uoregon.edu/research/summerschool/summer14/curriculum.html (visited on 10/19/2018) (cit. on p. 16).

[Wer08] Benjamin Werner. "On the Strength of Proof-irrelevant Type Theories". In: *Logical Methods in Computer Science* 4.3 (2008). DOI: 10.2168/LMCS-4(3:13)2008. URL: https://doi.org/10.2168/LMCS-4(3:13)2008 (cit. on p. 16).

[WK18] Philip Wadler and Wen Kokke. *Programming Language Foundations in Agda*. 2018. URL: https://plfa.github.io/ (visited on 10/12/2018) (cit. on pp. 18, 22).