

UNIVERSITÀ DEGLI STUDI DI UDINE

---

Dipartimento di Scienze Matematiche, Informatiche e Fisiche

Corso di Laurea Magistrale in Matematica

Tesi di Laurea

# A PROTOTYPE IMPLEMENTATION OF CUBICAL TYPE THEORY WITH PARTIAL AND RESTRICTION TYPES

Relatori:

Prof. FABIO ALESSI

Prof. FURIO HONSELL

Correlatore:

Prof. THIERRY COQUAND

Laureando:

MATTIA FURLAN

---

ANNO ACCADEMICO 2021-2022



# Abstract

Cubical type theory gives a constructive interpretation of the univalence axiom, which has been one of the central problems in homotopy type theory. In this thesis we present a version of cubical type theory with explicit partial and restriction types, also giving a partial semantic justification of the theory using the presheaf model of cubical sets. Finally we describe the main outcome of our work, which is a software implementation of the aforementioned type theory, written in Haskell, which reads and type-checks a source file containing a list of definitions, allowing then the user to experiment with it.

**Keywords:** *cubical type theory, univalence, restriction types, presheaf categories, functional programming, Haskell, type-checking.*



# Introduction

## 1 Intuitionistic type theory

The topic of this thesis is type theory, a branch of mathematics and computer science that traces its origins back to Russell’s theory of types in the early 1900’s, developed to be a solid foundation for mathematics which avoided the paradoxes. More precisely, we focus on some recent developments of intuitionistic type theory [ML75], introduced by Per Martin-Löf as a formal system meant to be a foundation for constructive mathematics. It is based on the Brouwer-Heyting-Kolmogorov interpretation of intuitionistic logic, which explains the meaning of the logical connectives in terms of computations, and on the so called Curry-Howard correspondence (or *propositions-as-types* [How80]), whose motto is «a proposition is the type of its proofs». The main feature of intuitionistic type theory is the fact that it can also be seen as a functional programming language, based on the typed lambda calculus, with a type system so rich that indeed it can interpret (higher order) logic. It should be noted that the type system of intuitionistic type theory is much more evolved than the ones found in ordinary programming languages, as they usually lack *dependent types*.<sup>1</sup> The problem with dependent types is that to keep type checking decidable, the language must be strongly normalizing, that is every computation must halt, and this implies the non-Turing completeness of the language.<sup>2</sup> Having a very expressive type system allows to state formally (i.e. inside the type system itself) a specification of a program, so that developing a program to fulfil its task and proving its correctness can be done at the same time. Although the non-Turing completeness can be a problem, it can be argued that dependent types remedy a bit, at least for practical purposes, since often it is

---

<sup>1</sup>Dependent types are types that depend on a value: a standard example is `vector(n)`, which is the type of vectors of length  $n$ . The dependent type is `vector` itself, not `vector(n)`.

<sup>2</sup>The normalizing property is strongly connected to the consistency of the underlying (intuitionistic) logic: a non terminating computation would be interpreted logically as a proof of falsum.

possible to avoid blocking the computation: an example is the function `head` which returns the first element of a list, as it must handle the empty list case somehow, usually in some artificial way, e.g. by reporting an I/O error and halting; with dependent types it can be solved easily, by passing not only the list but also a proof (that is, a term witnessing...) that the length of the list is not zero;<sup>3</sup> by doing this, the empty list case is automatically excluded.

The propositions-as-types paradigm, which may be more appropriately called proofs-as-programs, is actually practically implemented in some proof assistants such as Coq and Agda, as one can extract automatically a concrete program, written for example in Haskell,<sup>4</sup> that computes the function corresponding to a given proof. To make a possibly trivial example, from a Coq formalization of Euclid's proof of the infinity of prime numbers,<sup>5</sup> one can extract an Haskell program that, given a natural number, outputs a prime greater than that.

Turning back to the foundations, one of the most important features of intuitionistic type theory is the treatment of equality, of which there exists two main notions. The first is the *judgmental* or *definitional* equality, which is a relation between the terms of the theory but is external to it, and expresses the fact that two terms are convertible to each other, by simplifying the terms and unfolding the definitions.<sup>6</sup> In this thesis we will always write  $a \equiv b$  to mean that  $a$  and  $b$  are judgmentally equal. The second notion of equality, often called *definitional* equality, is more subtle and is internal to the theory itself: for each pair of terms  $a$  and  $b$  of the same type  $A$ , one can form the type  $\text{Id}_A(a, b)$ , often written more simply as  $a =_A b$ ; an element  $p$  of type  $a =_A b$  is then a witness that  $a$  and  $b$  are (propositionally) equal, but this does not imply that  $a \equiv b$ .<sup>7</sup> Propositional equality can be seen as an inductive relation, but is more simply modelled by an introduction rule asserting reflexivity of equality,

<sup>3</sup>With the notation that we will introduce in chapter 1, the signature of the function, for lists of naturals, would be  $\text{head} : [n : \mathbb{N}] (n > 0) \rightarrow \text{vector}_{\mathbb{N}}(n) \rightarrow \mathbb{N}$ .

<sup>4</sup>Haskell, named after the logician Haskell B. Curry (1900 - 1982), is one of the most commonly used purely functional programming languages, with static typing, type inference and lazy evaluation as its main features.

<sup>5</sup>I think it is worth to spend a few words to say that albeit the proof seems not to be really constructive, since the law of the excluded middle (LEM) is used to test whether the number  $N = p_1 \cdots p_n + 1$  is prime or not, that instance of LEM is intuitionistically valid, as the primeness property is obviously decidable.

<sup>6</sup>The strong normalization property implies the decidability of the judgmental equality.

<sup>7</sup>We say that the equality is *intensional*; it is possible to add the equality reflection rule (i.e. propositional equality implies judgmental equality), but it would destroy the decidability of the type-checking. Note that this implies not being able to even (computationally) recognize a valid proof.

and by an elimination rule (also called J-rule) which allows to prove a predicate about two equal elements  $a$  and  $b$  of type  $A$ , eventually depending also on the proof that they are equal, by proving only the simpler case where the two elements are judgementally the same and the equality is given by reflexivity. This seemingly simple treatment is the bridge to the homotopical interpretation of type theory, as it gives rise to the so called (weak)  $\infty$ -groupoid structure,<sup>8</sup> due to the possibility of iterating the equality type: given  $a, b : A$  and two proofs  $p, q : a =_A b$ , due to intensionality it shall not always hold that  $p \equiv q$ , and indeed it makes sense to form the type  $p =_{(a=_A b)} q$  of identifications between proofs of equality of  $a$  and  $b$ ; then we can continue: given two different identifications  $\alpha, \beta : p =_{(a=_A b)} q$ , we can form the type  $\alpha =_{(p=_{(a=_A b)} q)} \beta$ , and so on. The aforementioned structure of  $\infty$ -groupoid is given by the groupoid operations (identity, inverse, composition) induced by the elimination rule for propositional equality. The crucial fact is that this structure does not collapse, as one may intuitively expect that there is only one way to prove an equality, a principle known as *uniqueness of identity proofs* (UIP); [HS96] first proved that UIP does not hold in general, by exploiting the so called *groupoid model*, where types are interpreted by groupoids, the elements of the type are the elements of the corresponding groupoid and equality is modelled by arrows in that groupoid; a counterexample to UIP is then a groupoid with more than an arrow between two elements.

## 2 The homotopical interpretation

The groupoid model suggests that types should not be treated just as sets of points, and indeed an interpretation should exploit the  $\infty$ -groupoid structure. In the homotopical interpretation types are seen as topological spaces and identities between points as topological paths, i.e. continuous functions from the unit interval to the type/space. As I said in the previous section, using the J-rule it is possible to define the operations of *path inversion*,  $(a =_A b) \rightarrow (b =_A a)$ ,  $p \mapsto p^{-1}$ , and *path composition*,  $(a =_A b) \rightarrow (b =_A c) \rightarrow (a =_A c)$ ,  $p, q \mapsto p \cdot q$ , which satisfy the groupoid laws, but only up to (higher order) propositional equality,<sup>9</sup> e.g. for  $p : a =_A b$ ,  $p \cdot p^{-1}$  need not be judgmentally

<sup>8</sup>A groupoid is a category where every arrow is invertible, or equivalently is a group where the binary operation is a partial function (but the inverse has to be total). For an explanation of what a (weak)  $\infty$ -groupoid is, see the next footnote.

<sup>9</sup>The idea of a weak  $\infty$ -groupoid is the following: the identities between paths (i.e. arrows, or 1-morphisms) need not be exact, but instead they can be witnessed by ‘order two arrows’ (or 2-morphisms) between them, which are functors. Functors can be composed horizontally and vertically, and both operations have their own rules (unit and associativity), along with an interchange rule of the two operations; these rules need not hold strictly, but again only

equal to  $\mathbf{refl}_A(a)$ , but it can be proved that  $p \cdot p^{-1} =_{(a=Aa)} \mathbf{refl}_A(a)$ . This is easily explained topologically: the concatenation of a path with its inverse is almost never pointwise equal to the trivial path at its beginning point, but is always homotopic to it (note that an homotopy is nothing else than path between two paths). The connection between homotopy theory, higher-dimensional category theory and type theory arose around 2006 by the works of Awodey and Warren [AW09] and of Voevodsky [Voe06], resulting most notably in Voevodsky’s model of type theory in Kan simplicial sets [KL21].

### 3 Univalence and cubical type theory

The simplicial model of Voevodsky satisfies the so called *univalence property* (now called univalence axiom), which is about equality of types (i.e. paths inside the universe of types), as it says informally that equivalent types are actually (propositionally) equal. This is important because it adds more structure to the type-theoretic universe and because it makes possible to identify equivalent structures not in the informal way that it is usually done in mathematics, but explicitly using the language of type theory.<sup>10</sup> To make an example,<sup>11</sup> suppose we define two types  $\mathbf{Nat}$  and  $\mathbf{Nat}'$  inductively with the constructors  $\mathbf{Z} : \mathbf{Nat}$ ,  $\mathbf{S} : \mathbf{Nat} \rightarrow \mathbf{Nat}$  and  $\mathbf{zero} : \mathbf{Nat}'$ ,  $\mathbf{suc} : \mathbf{Nat}' \rightarrow \mathbf{Nat}'$ ; these two types are obviously equivalent in some intuitive sense, and suppose for now that this equivalence is formally witnessed by a suitable term  $\mathbf{e} : \mathbf{Equiv}(\mathbf{Nat}, \mathbf{Nat}')$ ; the axiom of univalence allows us to obtain a term  $\mathbf{ua}(\mathbf{e}) : \mathbf{Nat} =_{\mathcal{U}} \mathbf{Nat}'$ , which means we can *transport* theorems (i.e. terms) from  $\mathbf{Nat}$  to  $\mathbf{Nat}'$  and vice versa.<sup>12</sup> E.g. let us suppose that we have derived  $[n, m : \mathbf{Nat}] (n + m =_{\mathbf{Nat}} m + n)$ ; then we get ‘for free’ also  $[n, m : \mathbf{Nat}'] (n +' m =_{\mathbf{Nat}'} m +' n)$ . The univalence axiom is so called because it is not derivable from the other rules of intuitionistic type theory (and indeed it does not hold in the groupoid model). In general it is possible to add axioms to intuitionistic type theory, or to be more precise, to postulate the existence of terms with a given type (i.e.

---

up to a 3-morphism (natural transformation), and so on. This is a topic of higher category theory, and indeed a weak  $\infty$ -groupoid is defined as a weak  $\infty$ -category where every  $k$ -morphism is invertible (note that the fact that a  $k$ -morphism is invertible is witnessed by a  $k + 1$ -morphism), for each  $k \geq 0$ .

<sup>10</sup>Moreover, univalence implies that every construction in the type theory is homotopy invariant; this, along with *higher inductive types* (see [Uni13] chapter 6), allows to develop a synthetic approach to homotopy theory (see [Uni13] chapter 8).

<sup>11</sup>For a less trivial one, see [Uni13] 2.14.

<sup>12</sup>The transport is a basic principle of homotopy type theory, derivable from the J-rule, which is nothing else than Leibniz’s principle of indiscernibles, i.e. for a type family  $P : A \rightarrow \mathbf{U}$  and a path  $p : a =_A b$ , we have  $\mathbf{transport}^P(p, -) : P(a) \rightarrow P(b)$ .



**ex-middle** :  $[A : \mathbb{U}](A + \neg A)$  for the excluded middle). Note that although the excluded middle is consistent with intuitionistic type theory,<sup>13</sup> adding it makes no more possible to extract a program from a classical proof. Similarly, the problem with univalence is that it has to be postulated as an axiom, so proofs using it lose their computational content; the same happens with function extensionality, which is consistent with the theory (although it is implied by univalence). We have to be precise by what we mean with the possibility of extracting a program from a proof, which known as the *canonicity property*: we mean that every closed term that has the type of natural numbers reduces to a numeral in a computable way.<sup>14</sup> It is now clear that finding a constructive justification of univalence is (or, has been) a central topic in type theory. Cubical type theory, recently introduced in [CCHM15], allows to prove univalence while still keeping the computational content of the theory.

The key difference between CTT (cubical type theory) and HOTT (homotopy type theory) is the treatment of equality: whereas in the latter equality is inductively defined, in the former it is modelled in a more primitive, topological manner, i.e. as functions (paths) from a formal unit interval  $\mathbb{I}$  into a specified type. To make things more concrete, suppose that  $a$  and  $b$  have type  $A$ , then a witness of equality between  $a$  and  $b$  is a function  $p$ , called path, of type  $\mathbb{I} \rightarrow A$ , such that  $p\,0 \equiv a_1$  and  $p\,1 \equiv a_2$ , where  $0$  and  $1$  are the formal representation of zero and one in the unit interval. We use the notation  $\mathbf{Path}_A(a, b)$  for paths between elements  $a, b$  of type  $A$ . The key point is that  $\mathbb{I}$  is not a type, although it is possible to abstract over an element of  $\mathbb{I}$  and to apply a path to elements of  $\mathbb{I}$ . It should be kept clear from the beginning that path types do not correspond exactly to identity types in HOTT, as for example the elimination rule for path types holds only up to homotopy and not judgmentally.<sup>15</sup>

An enlightening example with path types is function extensionality, which can be proved in a surprisingly simple way: suppose that we have a (dependent) path  $p : [x : A] \mathbf{Path}_B(f\,x, g\,x)$  between two functions  $f, g : A \rightarrow B$ . Then the term

$$\beta \equiv [i : \mathbb{I}][x : A] \, p\,x\,i$$

<sup>13</sup>But not with the univalence axiom, see [Uni13] 3.2.7. Indeed, the ‘right’ formulation of LEM is not the naive one we presented, but  $[A : \mathbb{U}] \mathbf{isProp}\,A \rightarrow A + \neg A$ , which is consistent, as it holds in the simplicial model. The predicate  $\mathbf{isProp}$  classifies the so called *mere propositions*, or  $(-1)$ -types, which allow to develop classical logic in univalent foundations (see chapter 3 of [Uni13]).

<sup>14</sup>This is how the idea of a theory with computational content is formalized: with a suitable coding every other term of the theory can be thought as a function  $\mathbb{N} \rightarrow \mathbb{N}$ .

<sup>15</sup>Anyway, it is possible to define a data type  $\mathbf{Id}$  in CTT from path types so that they correspond exactly to HOTT’s identity types, making it possible to interpret HOTT inside CTT (see [CCHM15] 9.1, due to A. Swan).

is a path in  $A \rightarrow B$  between  $f$  and  $g$ , because

$$\beta \ 0 \equiv [x : A] \ p \ x \ 0 \equiv [x : A] \ f \ x \equiv f$$

and similarly  $\beta \ 1 \equiv g$ . Note that what we did is basically just swapping  $[i : \mathbb{I}]$  with  $[a : A]$  to get from  $p$  to  $\beta$ .

Equalities can be visualized as paths between the two endpoints, whose line structure can be thought as a degenerate ‘1-dimensional’ hypercube, described by the formula  $i = 0 \vee i = 1$ .

$$p \ 0 \xrightarrow{p} p \ 1$$

Homotopies, that is paths of paths, can be viewed as squares, or in other words 2-dimensional hypercubes. In the figure below,  $\alpha$  is an homotopy between the paths  $\alpha \ 0$  (or  $[j : \mathbb{I}] \ \alpha \ 0 \ j$ , with endpoints  $\alpha \ 0 \ 0$  and  $\alpha \ 0 \ 1$ ) and  $\alpha \ 1$  (or  $[j : \mathbb{I}] \ \alpha \ 1 \ j$ , with endpoints  $\alpha \ 1 \ 0$  and  $\alpha \ 1 \ 1$ ). We explicitly represent the axes for clarity; note that the structure can be described by the formula  $i = 0 \vee i = 1 \vee j = 0 \vee j = 1$ .

Disposing only of the interval does not bring us very far: the real power of CTT is the compositional structure (or *Kan structure*) that each type is equipped with. Indeed, the syntax of CTT is modelled in a way that reflects a model of type theory in cubical sets [Hub16], where each type has to satisfy the so-called *uniform Kan condition*, which is a generalization of the homotopy-theoretic Kan condition which informally says that for each  $n$ -dimensional hypercube missing one ‘face’ there is a complete hypercube that extends it. For example, suppose we have a term of type  $A$  defined on all the sides of a square except the top (we say that the type of that term is a *partial type*), that is on the *extent*  $i = 0 \vee i = 1 \vee j = 0$ ; then we can obtain a term defined on whole square (the *filler*) which extends the partial one. One easy application of composition is the concatenation of two paths, which we show in section 1.2.2. Another application is the derivation of the *transport* function, which allows to transfer

properties along paths, i.e. paths  $\text{Path}_A(x, y)$  induce functions  $P \ x \rightarrow P \ y$  for each  $P$ . Composition is defined inductively on the type family, which requires great care especially for the universe of types.

We use the notation  $[\varphi]A$  for the type of partial elements of  $A$  defined on the extent  $\varphi$  and  $[\psi \mapsto t]A$  for the type of (total) elements of  $A$  which agree with  $t$  on  $\psi$ . We talk respectively of partial and restriction types; the latter is used for example to assert that the composition agrees with the given partial term under the incomplete hypercube, or in other words that the composition extends the partial term. We remark that although the concept of partial type is very important for the presentation, it remains implicit in [CCHM15] and in the `cubicaltt` implementation.<sup>16</sup>

## 4 Contributions of the thesis

In this thesis we investigate and implement a modification of cubical type theory with explicit partial and restriction types, that is a type theory with:

- Basic type formers of intuitionistic type theory: empty and unit types, naturals, (dependent) products, (dependent) sums, coproducts.<sup>17</sup>
- A universe of types  $\mathbb{U}$ ;
- A formal unit interval  $\mathbb{I}$  with endpoints  $0$  and  $1$ . Although not being considered a type, it is possible to define and apply functions with domain  $\mathbb{I}$ , i.e. paths.
- Formulas built from atomic ones of the kind  $(i = 0)$ ,  $(i = 1)$  and  $(i = j)$ , where  $i, j : \mathbb{I}$  are called dimension names, using the operations  $\wedge$  and  $\vee$ .<sup>18</sup> Formulas are used only in partial and restriction types and in compositions; note that a conjunctive formula describes a face of a hypercube and a formula in disjunctive normal form describes a union of faces, that is a sub-polyhedra of an hypercube.
- Partial types of the form  $[\varphi]A$ , where  $A$  is a type and  $\varphi$  is a formula in disjunctive normal form. The meaning of  $[\varphi]A$  is that of a type defined

<sup>16</sup><https://github.com/mortberg/cubicaltt>

<sup>17</sup>Unit, sums and products is all that is needed to define non-inductive ADTs (algebraic data types). The empty and unit types will actually be derived types, the latter defined using a partial version of the naturals.

<sup>18</sup>Formulas of the form  $(i = j)$  are needed for higher inductive types, which we do not treat in this thesis. We decided to handle this kind of formulas anyway, in case of future upgrades of the implementation.

only of the extent  $\varphi$ . To define partial elements, we use *systems*, written as  $[\psi_1 \mapsto t_1, \dots, \psi_n \mapsto t_n]$ , where  $\varphi$  is the disjunction of the  $\psi$ 's, and  $t_i$  is the term associated to the face described by the conjunctive formula  $\psi_i$  (note that we have to ensure that the terms agree whenever the faces overlap, that is on the edges, described by the conjunction of the formulas of the two faces).

- Restriction types of the form  $[\psi_1 \mapsto t_1, \dots, \psi_n \mapsto t_n]A$ , where  $A$  is a type, and for each  $i$ ,  $\psi_i$  is a conjunctive formula and  $t_i$  is a term of type  $[\psi_i]A$ . The meaning of  $[\psi_1 \mapsto t_1, \dots, \psi_n \mapsto t_n]A$  is that of the type of elements of  $A$  that on each  $\psi_i$  are convertible to the given  $t_i$ . Analogously to systems, terms on overlapping formulas must be checked.

The handling of formulas requires special attention during type-checking and evaluation, managing individually the special cases of partial and restriction types. In particular, during type-checking we must pay attention to ‘propagate’ partial and restriction types (e.g. from  $f : [\psi \mapsto g](A \rightarrow B)$  and  $a : A$ , the application  $f\ a$  shall have type  $[\psi \mapsto g\ a]B$ ; inferring just type  $B$  results in a loss of information); during evaluation, some terms which we call *neutral* (i.e. terms for which we don’t have a definition at that moment of evaluation) have to be annotated with their type, and this has to reflect the typing rules. The need for annotation is that a neutral term with restriction type may have a true formula, which means that the whole term shall be reduced to the term associated with the true formula. Several choices about the exact rules to be admitted have been made and are presented in chapter 1.

After introducing the theory in the first chapter, in the second one we describe a category-theoretic semantics for this type theory using presheaf models; in particular we explain how to model partial and restriction types, also describing the connections with the subobject classifier available in any presheaf category, as is the category of *cubical sets*. Finally we describe an interpretation of the syntax into cubical sets, stating a soundness theorem for that semantics. We do not deal with the full semantics needed to handle univalence (i.e. Kan cubical sets [Hub16]).

Finally in chapter 3 we describe the details of the Haskell implementation of this type theory, using most notably a bidirectional type-checker and the normalization by evaluation technique. The result is a program which, given in input a file or a list of declarations (i.e. of the form **name** : **type**) and definitions (i.e. of the form **name** : **type** = **def**), type-checks it and then starts a REPL loop where it is possible to input new declarations and definitions and to infer the type of the given terms. The full code can be found at

<https://github.com/mattia-furlan/MasterThesisCTT>.

We remark that the focus of this thesis is the treatment of explicit partial and restriction types, and the purpose is not a full implementation of cubical type theory; indeed, in the implementation we have not developed composition for the universe of types, so that univalence is not yet provable; moreover, an efficient and smart implementation of composition is still to be engineered. This may be a direction for future work; other features that could be added to make the implementation more complete and user-friendly are:

- An infinite hierarchy of universes  $\mathcal{U}_0 : \mathcal{U}_1 : \dots$ , with a mechanism of universe polymorphism,<sup>19</sup> which can be implicit (that is, handled by the program) as in Coq, or explicit (that is, handled by the user with a specific syntax) as in Agda.
- The possibility of defining custom inductive types, or even higher inductive types.
- Implicit arguments when defining functions, which allow to shorten significantly the code written by the user.<sup>20</sup>

---

<sup>19</sup>By universe polymorphism we mean the ability to define functions uniformly with respect to all the universe levels. For example, with the implicit approach, one wants to write simply  $\mathbf{f} : [A, B : \mathcal{U}] \mathcal{U} = \dots$  to mean that  $\mathbf{f}$  is a function which given two types  $A$  and  $B$  of any universes  $\mathcal{U}_n$  and  $\mathcal{U}_m$ , produces a type in the universe  $\mathcal{U}_k$  where the definition lives (which has to be inferred by the program).  $\mathbf{f}$  itself is element of an universe, of level  $\max\{n+1, m+1, k\}$ .

<sup>20</sup>Example: `apply : [A, B :  $\mathcal{U}$ ][ $f : A \rightarrow B$ ][ $a : A$ ] B`; the first two arguments  $A$  and  $B$  need not be specified when calling `apply`, since they can be deduced from the argument binding to  $f$ .



# Contents

<b>Abstract</b>	<b>iii</b>
<b>Introduction</b>	<b>v</b>
1 Intuitionistic type theory . . . . .	v
2 The homotopical interpretation . . . . .	vii
3 Univalence and cubical type theory . . . . .	viii
4 Contributions of the thesis . . . . .	xi
<b>1 Theory</b>	<b>1</b>
1.1 The basic type theory . . . . .	1
1.1.1 Syntactical constraints . . . . .	4
1.1.2 Contexts . . . . .	6
1.1.3 Typing rules . . . . .	7
1.1.4 Operational semantics and evaluation . . . . .	10
1.1.5 Metatheoretical results . . . . .	13
1.1.6 Examples . . . . .	14
1.2 Extension with partial and restriction types . . . . .	16
1.2.1 Path types . . . . .	17
1.2.2 Syntax for composition . . . . .	18
1.2.3 Contexts and directions environments . . . . .	20
1.3 Typing rules . . . . .	21
1.4 Evaluation . . . . .	27
1.5 $\alpha\eta$ -conversion . . . . .	33
1.6 Metatheoretical results . . . . .	37
1.7 Examples . . . . .	38
1.7.1 Equivalence of two product types . . . . .	38
1.7.2 Path operations . . . . .	42
<b>2 Semantics</b>	<b>47</b>
2.1 Categories with families . . . . .	47

2.2	Presheaf models . . . . .	52
2.2.1	$\Pi$ -types . . . . .	54
2.2.2	$\Sigma$ -types . . . . .	56
2.2.3	Universes . . . . .	57
2.3	Cubical sets . . . . .	58
2.4	Semantics of the full theory . . . . .	59
2.4.1	Modelling formulas . . . . .	60
2.4.2	Modelling partial and restriction types . . . . .	62
2.5	Interpretation of the syntax . . . . .	64
<b>3</b>	<b>Implementation</b>	<b>67</b>
3.1	Lexical analysis and parsing . . . . .	68
3.2	Interval and formulas . . . . .	72
3.3	Core language . . . . .	76
3.4	Evaluation . . . . .	83
3.5	Conversion . . . . .	97
3.6	Type-checking . . . . .	101
3.7	Main program . . . . .	108
<b>A</b>	<b>Yoneda lemma</b>	<b>117</b>
<b>B</b>	<b>The subobject classifier</b>	<b>119</b>
<b>C</b>	<b>Disjointness of coproduct injections</b>	<b>125</b>
	<b>Bibliography</b>	<b>129</b>



# Chapter 1

## Theory

### 1.1 The basic type theory

We first present the basic intuitionistic type theory underlying our implementation, which we will then extend with the constructs of cubical type theory (interval, systems, partial and restriction types).

First of all we define the syntax of the terms of the basic theory. It is worth pointing out that what we call terms is different (more general) than terms usually intended in non-dependently typed  $\lambda$ -calculi, as there one can distinguish between types and terms (that is, the syntactic objects that can be assigned a type) regardless of the type-checking. Instead in dependently typed  $\lambda$ -calculi one cannot do this distinction, but can only define what is a type in a context ( $A$  is a type in context  $\Gamma$  if  $\Gamma \vdash A : \mathbb{U}$ ) and what is a term of a given type in a context ( $a$  is a term of type  $A$  in context  $\Gamma$  if  $A$  is a type in context  $\Gamma$  and  $\Gamma \vdash a : A$ ). Therefore, here by term we mean a syntactic object of the language, which can also be ill-typed.<sup>21</sup>

**Definition 1.1** (Terms). *Terms are inductively defined by:*

1. *Variables  $x, y, z, \dots$*
2. *A universe of types,  $\mathbb{U}$ .*
3. *A ‘let-definition’ mechanism of the form  $[x : A = M]M'$ , where  $x$  is a variable and  $A, M$  and  $M'$  are terms; it means ‘let  $x$  be of type  $A$  and judgmentally equal to  $M$  inside  $M'$ ’.*

---

<sup>21</sup>In the literature they are usually called *pre-terms* or *raw terms*.

4. For  $\Pi$ -types, i.e. (dependent) function types:

- (a) Abstraction  $[x : A]M$ , where  $x$  is a variable and  $A, M$  are terms. It is used both for the  $\lambda$ -abstraction for terms (i.e.  $\lambda x : A.M$ ) and for dependent product types (i.e.  $\Pi x : A.M$ ). The context in which a term of that form is used clears the ambiguity. When  $x$  does not appear in  $M$ , we shall simply write  $A \rightarrow M$ .
- (b) Application  $(M_1 M_2)$ , where  $M_1$  and  $M_2$  are terms.

5. For  $\Sigma$ -types, i.e. (dependent) pair types:

- (a) Dependent sum types  $\langle x : A \rangle M$ , where  $x$  is a variable and  $A, M$  are terms. When  $x$  does not appear in  $M$ , we shall simply write  $A * M$ .
- (b) Pair constructor  $(M_1, M_2)$ , where  $M_1$  and  $M_2$  are terms.
- (c) Projections  $M.1$  and  $M.2$ , where  $M$  is a term.<sup>22</sup>

6. For coproduct types:

- (a) Coproduct types  $A + B$ , where  $A$  and  $B$  are terms.
- (b) Left and right injections  $\text{inl } M$  and  $\text{inr } M$ , where  $M$  is a term.
- (c) Elimination rule for coproduct types: given terms  $A$  (type family),  $M_l$  (left case),  $M_r$  (right case) and  $M$ ,  $\text{split } A M_l M_r M$  is a term.

7. The type of natural numbers,  $\mathbf{N}$ , along with the constant  $\mathbf{Z}$  and the unary constructor  $\mathbf{S}$ . Moreover, for terms  $A$  (type family),  $M_0$  (base case),  $M_s$  (successor case) and  $N$ ,  $\text{ind } A M_0 M_s N$  is a term, which represents the induction principle (i.e. the elimination rule) for  $\mathbf{N}$ .

For brevity we do not include neither the empty type, as it can be defined using the impredicativity of the universe,<sup>23</sup> nor the unit type since it will be possible to derive it later too using cubical concepts (section 1.2).

<sup>22</sup>The two projections allows to define the elimination rule (or induction principle) for  $\Sigma$ -types; otherwise one can take the elimination rule as a primitive, and then define the two projections using it.

<sup>23</sup>The empty type, logically corresponding to *falsum*, is defined as  $\text{empty} : \mathbf{U} = [X : \mathbf{U}]X$ . The eliminator principle for the empty type is nothing else than the ‘*ex falso quodlibet*’ law (false implies anything), which is straightforward to derive:  $\text{ind-empty} : [A : \mathbf{U}] \text{empty} \rightarrow A = [A : \mathbf{U}][b : \text{empty}] b A$ . Impredicativity means that one can form types of the form  $[X : \mathbf{U}]Y$ , so that  $X$  quantifies over all types of the universe, including the one being defined.

The syntax can be presented more succinctly with a formal grammar, as follows, where  $x$  is a generic variable and  $A, B, M$  (eventually subscripted) are meta-variables for terms.

$$\begin{aligned}
A, B, M ::= & \mathbf{U} \mid x \\
& \mid [x : A = N]M && \text{(Let-definition)} \\
& \mid M_1 \ M_2 \mid [x : A]M && \text{(\Pi-types)} \\
& \mid \langle x : A \rangle M \mid (M_1, M_2) \mid M.1 \mid M.2 && \text{(\Sigma-types)} \\
& \mid A + B \mid \mathbf{inl} \ M \mid \mathbf{inr} \ M \mid \mathbf{split} \ A \ M_l \ M_r \ M && \text{(Coproducts)} \\
& \mid \mathbf{N} \mid \mathbf{0} \mid \mathbf{S} \mid \mathbf{ind} \ A \ M_0 \ M_s \ M && \text{(Naturals)}
\end{aligned}$$

It is important, especially for the implementation, to isolate a subset of the terms, known as *neutral terms* and denoted with  $K$ , which is composed by terms in  $\beta$ -normal form, i.e. terms that do not contain any redex, that is eliminators (function application, projections  $.1$  and  $.2$ ,  $\mathbf{split}$  and  $\mathbf{ind}$ ) applied to constructors of the same type. Neutral terms are: variables, all the terms whose main ‘term-constructor’ is not an eliminator,<sup>24</sup> and eliminators applied to a neutral terms only. Therefore, the grammar for neutral terms is the following:

$$\begin{aligned}
A, B, M ::= & \mathbf{U} \mid K \\
& \mid [x : A]M && \text{(\Pi-types)} \\
& \mid \langle x : A \rangle M \mid (M_1, M_2) && \text{(\Sigma-types)} \\
& \mid A + B \mid \mathbf{inl} \ M \mid \mathbf{inr} \ M && \text{(Coproducts)} \\
& \mid \mathbf{N} \mid \mathbf{0} \mid \mathbf{S} && \text{(Naturals)} \\
\\
K ::= & x \mid K \ M \mid \mathbf{ind} \ A \ M_0 \ M_s \ K \\
& \mid K.1 \mid K.2 \mid \mathbf{split} \ A \ M_l \ M_r \ K && \text{(Neutrals)}
\end{aligned}$$

We also consider values, i.e. the results of the evaluation of terms (evaluation will be discussed in section 1.1.4), as neutral terms, excluding the abstractions  $[x : A]B$  and  $\langle x : A \rangle B$ , extended with a closure operator of the form

<sup>24</sup>By the main term-constructor I mean the root of the tree associated to a term. For example, the term  $([x : \mathbf{N}] \ \mathbf{plus} \ x \ (\mathbf{S} \ Z)) \ Z$  has function application as its main term-constructor.

$\text{closure}(M, \Gamma)$ ,<sup>25</sup> where  $M$  is an (unevaluated) term of the form  $[x : A]B$  or  $\langle x : A \rangle B$  and the closure environment is specified by the context  $\Gamma$  (discussed in section 1.1.2). We write meta-variables representing values in bold, i.e.  $\mathbf{v}$ , to distinguish them from terms.

The only change we make in the abstract syntax is that we annotate neutral values with their (evaluated) type, written as  $\mathbf{v}^t$ . As will become clear later, type annotations are required in order to simplify cubical expressions: for example if the variable  $x$  has type  $[i : \mathbb{I}][i = 0) \mapsto a, (i = 1) \mapsto b]A$ ,<sup>26</sup> which means that  $x$  must be equal to  $a$  when  $i = 0$  and to  $b$  when  $i = 1$ , then the evaluation function shall reduce  $x$  0 to  $a$ , but it must know the type of  $x$  to do so. Note that type annotations are not needed for the basic theory, but it makes the presentation simpler to understand if we introduce them first in this simpler case.

Having defined terms and values, we give the rules to form a whole ‘program’, that is a list of declarations, definitions and examples,<sup>27</sup> which we formalize in the following grammar, where  $A, B, M$  are meta-variables for terms. Note that this part, albeit being practically important, is formally superfluous, since a sequence of definitions and declarations may be replaced by a single term using the abstractions  $[x : A]$  and  $[x : A = M]$ ;

$$\begin{aligned} \text{Program} &::= [\text{TopLevel}] \\ \text{TopLevel} &::= \text{Definition} \mid \text{Declaration} \mid \text{Example} \\ \text{Definition} &::= x : A = M \\ \text{Declaration} &::= x : A \\ \text{Example} &::= M \end{aligned}$$

### 1.1.1 Syntactical constraints

It is well known that one has to be careful with variables when performing reduction of terms, because there might occur a ‘capture of variable’, even in seemingly ‘safe’ cases, as the example shows (from [vBJ77]).

Supposing that

$$a : (A \rightarrow A) \rightarrow A \rightarrow A, \quad b : A \rightarrow A \rightarrow A,$$

<sup>25</sup>The point of evaluation is avoiding unnecessary syntactical substitutions, by reducing redexes only when the body of a term is free of abstractions. This is accomplished by using closures.

<sup>26</sup>Later we will call a type of this form a *path type*, and say that  $x$  is a path between  $a$  and  $b$  in type  $A$ .

<sup>27</sup>An ‘example’ is a term whose type will be inferred, if well-typed.

the term

$$([u : (A \rightarrow A \rightarrow A) \rightarrow A \rightarrow A \rightarrow A] u (u b))([z : A \rightarrow A \rightarrow A][y, x : A] a (z x) y)$$

is well typed and the reduction chain starts as follows:

$$\begin{aligned} &([u : (A \rightarrow A \rightarrow A) \rightarrow A \rightarrow A \rightarrow A] u (u b))([z : A \rightarrow A \rightarrow A][y, x : A] a (z x) y) \\ &\rightarrow_{\beta} ([z : A \rightarrow A \rightarrow A][y, x : A] a (z x) y)(([z : A \rightarrow A \rightarrow A][y, x : A] a (z x) y) b) \\ &\rightarrow_{\beta} ([z : A \rightarrow A \rightarrow A][y, x : A] a (z x) y)([y, x : A] a (b x) y) \\ &\rightarrow_{\beta} [y, x : A] a (([y, x : A] a (b x) y) x) y \end{aligned}$$

At this point it is necessary to rename one of the bound variables  $x$ , otherwise the term would reduce to

$$[y, x : A] a ([x : A] a (b x) x) y$$

which is not correct. The point of this example is that the capture of variable problem might happen even if in the starting term each binding variable is declared only once and the variables used in the sub-terms forming function applications are all different.

This problem must be handled with great care if one implements  $\beta$ -reduction syntactically, which is moreover inefficient; instead, we use the normalization-by-evaluation technique (see section 1.1.4), which defers actual substitutions until the body of a function is free of abstractions, by using closures, so that when the substitution is made, only the variables that were originally bound in the body of the function will be substituted by the corresponding terms.

There is a second subtlety that we must address, that is the eventual shadowing of names. Consider the following context:

$$x : \mathbb{N}, \quad y : \mathbb{N} = x, \quad x : \mathbb{N} \rightarrow \mathbb{N}.$$

If this has to be accepted, the program must handle somehow the fact that  $y$  of type  $\mathbb{N}$  seems to get assigned an object of type  $\mathbb{N} \rightarrow \mathbb{N}$ ; for example, Agda allows this by using indexes to discriminate between variables with the same name,<sup>28</sup> but this approach can still be confusing to the user. Instead, we decided to forbid name shadowing, so that the implementation is simpler. Note that the name shadowing check is done every time a context is expanded, i.e. with each new ‘top-level’ declaration or definition and when type-checking

<sup>28</sup>A technique called *namespaced De Bruijn indices*, see <https://www.haskellforall.com/2021/08/namespaced-de-bruijn-indices.html>.

an abstraction. It has to be made clear that the following context is valid, as the two variables  $x$  are not in the same scope:

$$\begin{aligned}\text{fun1} : \mathbb{N} \rightarrow \mathbb{N} &= [x : \mathbb{N}] \ x \\ \text{fun2} : \mathbb{N} \rightarrow \mathbb{N} &= [x : \mathbb{N}] \ \mathbf{S} \ x\end{aligned}$$

### 1.1.2 Contexts

To state the typing rules of the theory, we need a formal notion of context, which is thought as a list of declarations and definitions; moreover, we augment it with value bindings of the form  $x \mapsto \mathbf{v}$ , which are used only during evaluation.<sup>29</sup> Note that the evaluation function needs the list of declarations and definitions to annotate neutral terms with their type.

**Definition 1.2** (Context).

1.  $()$  is the empty context;
2.  $\Gamma, x : A$  extends the context  $\Gamma$  with a declaration, where the type  $A$  is a term;
3.  $\Gamma, x : A = M$  extends the context  $\Gamma$  with a definition, where both the type  $A$  and the body  $M$  are terms;
4.  $\Gamma, x \mapsto \mathbf{v}$  extends the context  $\Gamma$  binding the variable  $x$  to the value  $\mathbf{v}$ .

Although being used for the formal recursive definition, we will obviously omit the  $()$  symbol for the empty context.

The utility function `LOOKUPTYPE` retrieves the (evaluated) type of an identifier from the given context; we denote evaluation of  $A$  in context  $\Gamma$  with  $(A)_\Gamma$  (see section 1.1.4). Keep in mind that evaluation is done only after type-checking, so that any variable with no declaration is reported as an error before evaluation takes place. The function `LOOKUPTYPE` can be specified formally by recursion on the structure of the context (where the last ‘ $-$ ’ means ‘every other possibility’):

$$\begin{aligned}\text{LOOKUPTYPE}(\Gamma, x : A), x) &= (A)_\Gamma \\ \text{LOOKUPTYPE}(\Gamma, x : A = B), x) &= (A)_\Gamma \\ \text{LOOKUPTYPE}(\Gamma, -, x) &= \text{LOOKUPTYPE}(\Gamma, x)\end{aligned}$$

---

<sup>29</sup>Therefore our notion of context is not the usual one; it may be more appropriately called ‘extended context’ or ‘context plus environment’.

### 1.1.3 Typing rules

We use a technique called *bidirectional type checking*, that is we define and implement two relations, one for type inference (written  $\Gamma \vdash t \Rightarrow \mathbf{ty}$ ) and one for type checking (written  $\Gamma \vdash t \Leftarrow \mathbf{ty}$ ), which allow to type-check programs in a fairly straightforward manner while maintaining a close correspondence with the syntax and also producing good error messages.<sup>30</sup> Moreover, this approach requires type annotations only at the ‘top-level’ of the declarations and not in every sub-term, allowing e.g. to write only `inl a` instead of `inlA,B a`, or `(a, b)` instead of `(a, b)A,B` or even  $\lambda$ -abstractions without mentioning the type, as it has to be already present in the top-level signature (e.g. in  $f : \mathbb{N} \rightarrow \mathbb{N} = [n] \mathbb{S} n$ ,  $n$  must have type  $\mathbb{N}$  due to the signature).<sup>31</sup> Note that terms are checked against evaluated types, as they are in  $\beta$ -normal form.

We now present the rules for a bidirectional type-checker for the basic theory; later, to handle partial and restriction types, we will use not only the context  $\Gamma$  for type-checking but also a *directions environment*  $\Theta$  (see section 1.2.3).

The rule about the universe (i.e. the one asserting  $U : U$ ) requires some explanation, first of all because it makes the theory inconsistent (Girard’s paradox). In the usual presentations of Martin-Löf’s type theory (e.g. [ML75], [Hof97]), one has a separate kind of judgment for types, usually written as  $\Gamma \vdash A \text{ Type}$ , so that it is then possible to formulate the type forming rules, e.g. from  $\Gamma, x : A \vdash B \text{ Type}$  infer  $\Gamma \vdash [x : A] B \text{ Type}$ , without mentioning any universe of types. One can then introduce a universe, containing codes for types (such a universe is said to be *à la Tarski*), in which type formers can be ‘reflected’ (see 2.8). With just one universe  $U_0$  one does not get farther than before, as it is not possible to write impredicative definitions, i.e. quantifying over types. To do so, one must introduce a new universe  $U_1$  which contains a code for  $U_0$  and also for every type in  $U_0$ ,<sup>32</sup> where it is possible to form types which quantify over  $U_0$ ; of course one may then want to quantify over types in  $U_1$ , which means that a new universe  $U_2$  has to be introduced, and so on obtaining a cumulative chain of universes  $U_0, U_1, U_2, \dots$ .<sup>33</sup> The implementation of an infinite chain of universes, especially if the universe indexing has to be invisible to the user,

<sup>30</sup>Compare with the Hindley-Milner type-checking algorithm [Mil78], which uses the unification algorithm. Error reporting there can be difficult to interpret.

<sup>31</sup>However, to make the syntax more uniform and simple, we require to always include the type in abstractions.

<sup>32</sup>The universes are then cumulative.

<sup>33</sup>This is the approach used in Coq, where there is a cumulative chain of universes  $\text{Type}_0, \text{Type}_1, \text{Type}_2, \dots$ , which is however usually invisible to the user, showing just  $\text{Type}$ .  $\text{Type}_0$  is split into  $\text{Prop}$  (impredicative and proof irrelevant) and  $\text{Set}$  (predicative and proof relevant). See also <http://adam.chlipala.net/cpdt/html/Universes.html>.

requires quite a lot of work, therefore in the prototype implementation we present in this thesis there is just one universe; stating the inconsistent  $\mathbb{U} : \mathbb{U}$  is a way to allow impredicative definitions while maintaining the implementation simple. Of course, one must be careful not to use it improperly to prove false results. As an example of ‘proper’ use, we can form the empty type, putting  $x \equiv X$ ,  $ty \equiv \mathbb{U}$  and  $e \equiv X$ :

$$\frac{\Gamma \vdash \mathbb{U} \Leftarrow \mathbb{U} \quad \Gamma, X : \mathbb{U} \vdash X \Leftarrow \mathbb{U}}{\Gamma \vdash [X : \mathbb{U}]X \Leftarrow \mathbb{U}} \text{ (Pi)}$$

## Type inference

$$\overline{\Gamma \vdash x \Rightarrow \text{LOOKUPTYPE}(\Gamma, x)} \quad \text{(Var)}$$

$$\overline{\Gamma \vdash \mathbb{U} \Rightarrow \mathbb{U}} \quad \text{(Universe)}$$

$$\frac{\Gamma \vdash f \Rightarrow \text{closure}([x : ty]e, \Gamma') \quad \Gamma \vdash a \Leftarrow (ty)_{\Gamma'}}{\Gamma \vdash f \ a \Rightarrow \text{APP}(\text{closure}([x : ty]e, \Gamma'), (a)_{\Gamma})} \quad \text{(App)}$$

$$\frac{\Gamma \vdash p \Rightarrow \text{closure}(\langle x : ty \rangle e, \Gamma')}{\Gamma \vdash p.1 \Rightarrow (ty)_{\Gamma'}} \quad \text{(Sigma-1)}$$

$$\frac{\Gamma \vdash p \Rightarrow \text{closure}(\langle x : ty \rangle e, \Gamma')}{\Gamma \vdash p.2 \Rightarrow (e)_{\Gamma', x \mapsto (p.1)_{\Gamma}}} \quad \text{(Sigma-2)}$$

$$\frac{\begin{array}{l} \Gamma \vdash F \Leftarrow \mathbf{ty}_1 + \mathbf{ty}_2 \rightarrow \mathbb{U} \quad \Gamma \vdash f_1 \Leftarrow ([x : ty_1] \ F \ (\mathbf{inl} \ x))_{\Gamma} \\ \Gamma \vdash t \Rightarrow \mathbf{ty}_1 + \mathbf{ty}_2 \quad \Gamma \vdash f_2 \Leftarrow ([x : ty_2] \ F \ (\mathbf{inr} \ x))_{\Gamma} \end{array}}{\Gamma \vdash \text{split } F \ f_1 \ f_2 \ t \Rightarrow (F \ t)_{\Gamma}} \quad (x = \text{NEWVAR}(\Gamma)) \quad \text{(Split)}$$

$$\overline{\Gamma \vdash \mathbb{N} \Rightarrow \mathbb{U}} \quad \text{(Nat)}$$

$$\overline{\Gamma \vdash \mathbb{Z} \Rightarrow \mathbb{N}} \quad \text{(Zero)}$$



$$\frac{\Gamma \vdash n \Leftarrow \mathbf{N}}{\Gamma \vdash \mathbf{S} \, n \Rightarrow \mathbf{N}} \quad (\text{Succ})$$

$$\frac{\begin{array}{c} \Gamma \vdash F \Leftarrow \mathbf{N} \rightarrow \mathbf{U} \quad \Gamma \vdash c_0 \Leftarrow (F \, \mathbf{Z})_\Gamma \\ \Gamma \vdash n \Leftarrow \mathbf{N} \quad \Gamma \vdash c_s \Leftarrow ([m : \mathbf{N}] \, F \, m \rightarrow F \, (\mathbf{S} \, m))_\Gamma \end{array}}{\Gamma \vdash \text{ind} \, F \, c_0 \, c_s \, n \Rightarrow (F \, n)_\Gamma} \quad (m = \text{NEWVAR}(\Gamma)) \quad (\text{Ind})$$

## Type checking

$$\frac{\Gamma \vdash ty \Leftarrow \mathbf{U} \quad \Gamma \vdash e \Leftarrow (ty)_\Gamma \quad \Gamma, x : ty = e \vdash t \Leftarrow \mathbf{A}}{\Gamma \vdash [x : ty = e]t \Leftarrow \mathbf{A}} \quad (\text{Def})$$

$$\frac{\Gamma \vdash ty \Leftarrow \mathbf{U} \quad \Gamma, x : ty \vdash e \Leftarrow \mathbf{U}}{\Gamma \vdash [x : ty]e \Leftarrow \mathbf{U}} \quad (\text{Pi})$$

$$\frac{\Gamma \vdash ty \Leftarrow \mathbf{U} \quad \Gamma, x : ty \vdash e \Leftarrow \mathbf{U}}{\Gamma \vdash \langle x : ty \rangle e \Leftarrow \mathbf{U}} \quad (\text{Sigma})$$

$$\frac{\begin{array}{c} \Gamma \vdash ty \Leftarrow \mathbf{U} \quad (ty)_\Gamma \sim_{\tau(\Gamma)} (ty_1)_{\Gamma_1} \\ \Gamma, x : ty, x \mapsto v \vdash e \Leftarrow \text{APP}(\text{closure}([x_1 : ty_1]e_1, \Gamma_1), v^{(ty_1)_{\Gamma_1}}) \end{array}}{\Gamma \vdash [x : ty]e \Leftarrow \text{closure}([x_1 : ty_1]e_1, \Gamma_1)} \quad (v = \text{NEWVAR}(\Gamma_1)) \quad (\text{Abstraction})$$

$$\frac{\Gamma \vdash s \Leftarrow (ty)_{\Gamma'} \quad \Gamma \vdash t \Leftarrow (e)_{\Gamma', x \mapsto (s)_\Gamma}}{\Gamma \vdash (s, t) \Leftarrow \text{closure}(\langle x : ty \rangle e, \Gamma')} \quad (\text{Pair})$$

$$\frac{\Gamma \vdash A \Leftarrow \mathbf{U} \quad \Gamma \vdash B \Leftarrow \mathbf{U}}{\Gamma \vdash A + B \Leftarrow \mathbf{U}} \quad (\text{Coproduct})$$

$$\frac{\Gamma \vdash t_1 \Leftarrow \mathbf{A}}{\Gamma \vdash \text{inl} \, t_1 \Leftarrow \mathbf{A} + \mathbf{B}} \quad (\text{Inl})$$

$$\frac{\Gamma \vdash t_2 \Leftarrow \mathbf{B}}{\Gamma \vdash \mathbf{inr} \, t_2 \Leftarrow \mathbf{A} + \mathbf{B}} \quad (\text{Inr})$$

$$\frac{\Gamma \vdash e \Rightarrow \mathbf{A} \quad \mathbf{A} \sim_{\tau(\Gamma)} \mathbf{A}'}{\Gamma \vdash e \Leftarrow \mathbf{A}'} \quad (\text{Infer})$$

In the last rule,  $\mathbf{A} \sim_{\tau(\Gamma)} \mathbf{A}'$  means that values  $\mathbf{A}$  and  $\mathbf{A}'$  are  $\alpha\eta$ -equivalent;<sup>34</sup>  $\tau(\Gamma)$  is the list of names declared in the context  $\Gamma$ . We refer to section 1.5 for the definition of the  $\alpha\eta$ -equivalence (or  $\alpha\eta$ -conversion) predicate, written once for the full type theory.

### 1.1.4 Operational semantics and evaluation

Given a context  $\Gamma$ , the function  $\text{EVAL}_\Gamma$  gets a term as input and gives the corresponding value as output. The point of evaluation is getting the canonical form of a term.<sup>35</sup> Instead of writing  $\text{EVAL}_\Gamma(t)$ , we shall simply write  $(t)_\Gamma$ . The key point of evaluation is that of using closures to defer computation in the case of abstractions of the form  $[x : A]M$  or  $\langle x : A \rangle M$ ; as already explained in section 1.1, in this way the structure of the body is preserved until it becomes free of abstractions, and only at that point the substitutions are actually performed.<sup>36</sup>

Evaluation is then defined by recursion on the structure of the terms.

$$\begin{aligned} (x)_\Gamma &= x^{\text{LOOKUP\_TYPE}(\Gamma, x)} \\ (\mathbf{U})_\Gamma &= \mathbf{U} \\ ([x : ty = e]t)_\Gamma &= (t)_{\Gamma, x:ty=e} \\ ([x : ty]e)_\Gamma &= \text{closure}([x : ty]e, \Gamma) \\ (f \, a)_\Gamma &= \text{APP}((f)_\Gamma, (a)_\Gamma) \\ (\langle x : ty \rangle e)_\Gamma &= \text{closure}(\langle x : ty \rangle e, \Gamma) \\ (t_1, t_2)_\Gamma &= ((t_1)_\Gamma, (t_2)_\Gamma) \\ (t.1)_\Gamma &= \text{FST}((t)_\Gamma) \end{aligned}$$

<sup>34</sup> $\alpha$ -equivalence is about identifying values up to renaming of variables;  $\eta$ -equivalence means that for function (respectively pair) types,  $f$  and  $[x : A] f \, x$  (respectively  $p$  and  $(p.1, p.2)$ ) are identified.

<sup>35</sup>The canonical form is the  $\beta$ -normal form; keep in mind that values may contain closures, so to get the  $\beta$ -normal form as a term, one has to convert closures into terms (this process is called ‘reading-back’, see section 1.1.4).

<sup>36</sup>This approach was first introduced by P. J. Landin in his seminal paper [Lan64].

$$\begin{aligned}
(t.2)_\Gamma &= \text{SND}((t)_\Gamma) \\
(A + B)_\Gamma &= (A)_\Gamma + (B)_\Gamma \\
(\text{inl } t_1)_\Gamma &= \text{inl } (t_1)_\Gamma \\
(\text{inr } t_2)_\Gamma &= \text{inr } (t_2)_\Gamma \\
(\text{split } ty \ f_1 \ f_2 \ t)_\Gamma &= \text{SPLIT}((ty)_\Gamma, (f_1)_\Gamma, (f_2)_\Gamma, (t)_\Gamma) \\
(\mathbf{N})_\Gamma &= \mathbf{N} \\
(\mathbf{Z})_\Gamma &= \mathbf{Z} \\
(\mathbf{S } n)_\Gamma &= \mathbf{S } (n)_\Gamma \\
(\text{ind } F \ c_0 \ c_s \ n)_\Gamma &= \text{IND}((F)_\Gamma, (c_0)_\Gamma, (c_s)_\Gamma, (n)_\Gamma)
\end{aligned}$$

Note that the result of the evaluation of a variable is always a neutral term, which is the variable itself annotated with its type; moreover, each eliminator is handled individually using an helper function (written in small caps), as we need to handle carefully the case when the argument is neutral. We specify them below, but we will need to expand them to handle restriction types in section 1.4.

- APP applied to **f** and **a** first checks if **f** is a closure, and if so it evaluates it with the given value **a**, otherwise **f a** must be a neutral application which gets annotated with its type.<sup>37</sup>

$$\begin{aligned}
\text{APP}(\text{closure}([x : ty]e, \Gamma), \mathbf{a}) &= (e)_{\Gamma, x \mapsto \mathbf{a}} \\
\text{APP}(\mathbf{f}^{\text{closure}([x : ty]e, \Gamma)}, \mathbf{a}) &= (\mathbf{f } \mathbf{a})^{(e)_{\Gamma, x \mapsto \mathbf{a}}}
\end{aligned}$$

- FST and SND return respectively the first and the second component of a pair, if the value is not neutral; otherwise they annotate the whole value with the corresponding type.

$$\begin{aligned}
\text{FST}((\mathbf{v}_1, \mathbf{v}_2)) &= \mathbf{v}_1 \\
\text{FST}(\mathbf{v}^{\text{closure}([x : ty]e, \Gamma)}) &= (\mathbf{v}.1)^{(ty)_\Gamma} \\
\text{SND}((\mathbf{v}_1, \mathbf{v}_2)) &= \mathbf{v}_2 \\
\text{SND}(\mathbf{v}^{\text{closure}([x : ty]e, \Gamma)}) &= (\mathbf{v}.2)^{(e)_{\Gamma, x \mapsto \text{FST}(\mathbf{v})}}
\end{aligned}$$

- SPLIT does by-case analysis on the given argument, if it is not neutral, otherwise the whole term becomes neutral and gets annotated with its type.

$$\text{SPLIT}(\mathbf{F}, \mathbf{f}_1, \mathbf{f}_2, \text{inl } \mathbf{v}_1) = \text{APP}(\mathbf{f}_1, \mathbf{v}_1)$$

---

<sup>37</sup>Remember that terms are type-checked before they get evaluated, so the types are assumed to be correct, and in particular in this case the type of **f** has to be a function type.

$$\begin{aligned}\text{SPLIT}(\mathbf{F}, \mathbf{f}_1, \mathbf{f}_2, \text{inr } \mathbf{v}_2) &= \text{APP}(\mathbf{f}_2, \mathbf{v}_2) \\ \text{SPLIT}(\mathbf{F}, \mathbf{f}_1, \mathbf{f}_2, \mathbf{v}^{\text{ty}'}) &= (\text{split } \mathbf{F} \ \mathbf{f}_1 \ \mathbf{f}_2 \ \mathbf{v})^{\text{APP}(\mathbf{F}, \mathbf{v})}\end{aligned}$$

- IND evaluates an induction by pattern-matching on the argument  $n$ ; if  $n$  is neutral, then the whole induction is neutral and so it gets annotated with its type.

$$\begin{aligned}\text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \mathbf{Z}) &= \mathbf{c}_0 \\ \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \mathbf{S} \ \mathbf{m}) &= \text{APP}(\text{APP}(\mathbf{c}_s, \mathbf{m}), \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \mathbf{m})) \\ \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \mathbf{n}^{\mathbf{N}}) &= (\text{ind } \mathbf{F} \ \mathbf{c}_0 \ \mathbf{c}_s \ \mathbf{n})^{\text{APP}(\mathbf{F}, \mathbf{n})}\end{aligned}$$

### Reading back

Having discussed evaluation, we now describe the function  $\mathcal{R}$  which converts values back into terms, that is by recursively evaluating the closures. In that way, starting from a term, by first evaluating and then reading back, one gets the  $\beta$ -normal form of that term.

The read-back function  $\mathcal{R}$  keeps track of the list of already used names  $ns$ , to avoid name conflicts when reading back closures. For all the values except closures,  $\mathcal{R}$  is defined inductively in the obvious manner.<sup>38</sup>

$$\begin{aligned}\mathcal{R}_{ns}(\mathbf{x}) &= x \\ \mathcal{R}_{ns}(\mathbf{U}) &= \mathbf{U} \\ \mathcal{R}_{ns}(\mathbf{k} \ \mathbf{a}) &= \mathcal{R}_{ns}(\mathbf{k}) \ \mathcal{R}_{ns}(\mathbf{a}) \\ \mathcal{R}_{ns}((\mathbf{v}_1, \mathbf{v}_2)) &= (\mathcal{R}_{ns}(\mathbf{v}_1), \mathcal{R}_{ns}(\mathbf{v}_2)) \\ \mathcal{R}_{ns}(\mathbf{k}.1) &= \mathcal{R}_{ns}(\mathbf{k}).1 \\ \mathcal{R}_{ns}(\mathbf{k}.2) &= \mathcal{R}_{ns}(\mathbf{k}).2 \\ \mathcal{R}_{ns}(\mathbf{A} + \mathbf{B}) &= \mathcal{R}_{ns}(\mathbf{A}) + \mathcal{R}_{ns}(\mathbf{B}) \\ \mathcal{R}_{ns}(\text{inl } \mathbf{v}_1) &= \text{inl } \mathcal{R}_{ns}(\mathbf{v}_1) \\ \mathcal{R}_{ns}(\text{inr } \mathbf{v}_2) &= \text{inr } \mathcal{R}_{ns}(\mathbf{v}_2) \\ \mathcal{R}_{ns}(\text{split } \text{ty } \mathbf{f}_1 \ \mathbf{f}_2 \ \mathbf{k}) &= \text{split } \mathcal{R}_{ns}(\text{ty}) \ \mathcal{R}_{ns}(\mathbf{f}_1) \ \mathcal{R}_{ns}(\mathbf{f}_2) \ \mathcal{R}_{ns}(\mathbf{k}) \\ \mathcal{R}_{ns}(\mathbf{N}) &= \mathbf{N} \\ \mathcal{R}_{ns}(\mathbf{Z}) &= \mathbf{Z} \\ \mathcal{R}_{ns}(\mathbf{S} \ n) &= \mathbf{S} \ (\mathcal{R}_{ns}(n)) \\ \mathcal{R}_{ns}(\text{ind } F \ c_0 \ c_s \ k) &= \text{ind } \mathcal{R}_{ns}(F) \ \mathcal{R}_{ns}(c_0) \ \mathcal{R}_{ns}(c_s) \ \mathcal{R}_{ns}(k)\end{aligned}$$

<sup>38</sup>In the definition,  $\mathbf{k}$  represents a neutral term; note that e.g. if a value has the form  $\mathbf{k} \ \mathbf{a}$ , then  $\mathbf{k}$  must be neutral, and the same happens with all the other eliminators.

Finally for closures we read-back the argument type and the evaluated body (with a fresh variable  $x'$ ).

$$\begin{aligned}\mathcal{R}_{ns}(\text{closure}([x : ty]e, \Gamma)) &= [x' : ty']e' \\ \mathcal{R}_{ns}(\text{closure}(\langle x : ty \rangle e, \Gamma)) &= \langle x' : ty' \rangle e'\end{aligned}$$

where

$$\begin{cases} x' &= \text{NEWVAR}(ns) \\ ty' &= \mathcal{R}_{ns}((ty)_{\Gamma}) \\ e' &= \mathcal{R}_{ns, x'}((e)_{\Gamma, x \mapsto x'(ty)_{\Gamma}}) \end{cases}$$

### 1.1.5 Metatheoretical results

The basic theory discussed so far, with an infinite hierarchy of cumulative universes instead of a single (inconsistent) universe, is basically the one described in [ML75], for which a normalization theorem is proved, by extending the now classical Tait's reducibility method (see [GTL89]).

**Theorem 1** (Strong normalization).

*Every term reduces to an unique normal term.*

Normalization in our presentation has to be thought as evaluation followed by reading back (term  $\rightarrow$  value  $\rightarrow$  term), which implements  $\beta$ -reduction and whose termination is guaranteed by the above theorem. By unique we mean unique up to  $\alpha\eta$ -conversion (see section 1.5).

Strong normalization implies the following results, albeit they are clear from the given implementation.

**Theorem 2** (Decidability of  $\alpha\eta$ -conversion).

*For any two terms of the same type, it is decidable whether they are  $\alpha\eta$ -equivalent or not.*

**Theorem 3** (Decidability of type-checking).

*Given a context  $\Gamma$  and terms  $a$  and  $A$ , it is decidable whether  $\Gamma \vdash a \Leftarrow A$ .*

As a last note, in the introduction we have remarked that functions defined in Martin-Löf's type theory are computable and validate the canonicity property, and indeed if  $\vdash f \Leftarrow \mathbb{N} \rightarrow \mathbb{N}$ , then for  $\vdash n \Leftarrow \mathbb{N}, \vdash f\ m \Leftarrow \mathbb{N}$  reduces to a (closed) normal term of type  $\mathbb{N}$ , which must be a numeral; the computation is done by following the evaluation rules.

### 1.1.6 Examples

We report some brief examples which can be written in this basic type theory.

First of all we can define, using the well known recursive definitions, the basic arithmetic operations.

```

idN : N → U = [x : N] N
plus : N → N → N = [m : N][n : N] ind idN m ([n' : N][mPn' : N] S mPn') n
mult : N → N → N = [m : N][n : N] ind idN Z ([n' : N][mTn' : N] plus mTn' m) n
exp : N → N → N = [m : N][n : N] ind idN (S Z) ([n' : N][mEn' : N] mult mEn' m) n

```

These functions obviously satisfy (judgmentally) the identities between numerals, and it is possible to prove (using path types, see section 1.2.1) the usual properties by induction (commutativity, associativity, etc).

We assume to have a unit type (which we will introduce in section 1.7) with a single constructor and the induction/elimination principle:

```

tt : unit
unitInd : [C : unit → U] C tt → [x : unit] C x

```

Using `unit` and coproducts we can form the `bool` type and derive its induction/elimination principle:

```

bool : U = unit + unit
false : bool = inl tt
true : bool = inr tt
boolInd : [C : bool → U] C false → C true → [x : bool] C x
        = [C : bool → U][cf : C false][ct : C true][x : bool]
          split C ([u : unit] unitInd ([u' : unit] C (inl u')) cf u)
              ([u : unit] unitInd ([u' : unit] C (inr u')) ct u) x
boolRec : [C : U] C → C → bool → C
        = [C : U][f : C][t : C][x : bool] boolInd (bool → C) f t x

```

Then we can define the boolean operations and some relations (e.g. equality, less-or-equal) between naturals using the recursive characterization.<sup>39</sup>

```

If : [C : U] bool → C → C → C

```

---

<sup>39</sup>We define by induction on  $m : \mathbb{N}$  a function  $\mathbb{N} \rightarrow \text{bool}$ , thought as  $(m = -)$ . When  $m \equiv Z$ , the function returns `true` on  $Z$  and `false` on successors; when  $m \equiv S m'$ , the function returns `false` on  $Z$  and on successors  $n \equiv S n'$  it computes the previous value (i.e.  $m' = n'$ , the inductive hypothesis). Similarly for ‘less-or-equal’.

$$\begin{aligned}
&= [C : \mathbb{U}][x : \text{bool}][t : C][f : C] \text{ boolRec } C \ f \ t \ x \\
\text{not} : \text{bool} \rightarrow \text{bool} &= [b : \text{bool}] \text{ If bool } b \ \text{false} \ \text{true} \\
\text{and} : \text{bool} \rightarrow \text{bool} \rightarrow \text{bool} &= [b1, b2 : \text{bool}] \text{ If bool } b1 \ b2 \ \text{false} \\
&\quad \text{or} : \text{bool} \rightarrow \text{bool} \rightarrow \text{bool} = [b1, b2 : \text{bool}] \text{ If bool } b1 \ \text{true} \ b2 \\
\text{natEq} : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \text{bool} &= [m : \mathbb{N}] \text{ ind } (\mathbb{N} \rightarrow \mathbb{N} \rightarrow \text{bool}) \\
&\quad ([n : \mathbb{N}] \text{ ind } (\mathbb{N} \rightarrow \text{bool}) \ \text{true} \ (\mathbb{N} \rightarrow \text{bool} \rightarrow \text{false}) \ n) \\
&\quad ([m' : \mathbb{N}][m'Eq : \mathbb{N} \rightarrow \text{bool}][n : \mathbb{N}] \\
&\quad \quad \text{ind } (\mathbb{N} \rightarrow \text{bool}) \ \text{false} \ ([n' : \mathbb{N}] \text{ bool} \rightarrow m'Eq \ n') \ n) \ m \\
\text{natNeq} : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \text{bool} &= [m, n : \mathbb{N}] \text{ not } (\text{natEq } m \ n) \\
\text{natLeq} : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \text{bool} &= [m : \mathbb{N}] \text{ ind } (\mathbb{N} \rightarrow \mathbb{N} \rightarrow \text{bool}) \ (\mathbb{N} \rightarrow \text{true}) \\
&\quad ([m' : \mathbb{N}][m'Leq : \mathbb{N} \rightarrow \text{bool}][n : \mathbb{N}] \\
&\quad \quad \text{ind } (\mathbb{N} \rightarrow \text{bool}) \ \text{false} \ ([n' : \mathbb{N}] \text{ bool} \rightarrow m'Leq \ n') \ n) \ m \\
\text{natLe} : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \text{bool} &= [m, n : \mathbb{N}] \text{ and } (\text{natLeq } m \ n) \ (\text{natNeq } m \ n)
\end{aligned}$$

Using `bool` and function types we can define an alternative product type, which is the type of functions  $\text{bool} \rightarrow \mathbb{U}$  mapping `false` to the first type and `true` to the second one. In section 1.7, after introducing path types and transport, we will prove the propositional  $\eta$ -equality and the inductive/elimination principle for `prod`, which will finally allow us to prove that `prod A B` is equivalent to  $A * B$ .

$$\begin{aligned}
\text{prod} : \mathbb{U} \rightarrow \mathbb{U} \rightarrow \mathbb{U} &= [A, B : \mathbb{U}][x : \text{bool}] \text{ boolRec } \mathbb{U} \ A \ B \ x \\
\text{couple} : [A, B : \mathbb{U}] \ A \rightarrow B \rightarrow \text{prod } A \ B \\
&= [A, B : \mathbb{U}][a : A][b : B] \text{ boolInd } ([x : \text{bool}] \text{ boolRec } \mathbb{U} \ A \ B \ x) \ a \ b \\
\text{pi1} : [A, B : \mathbb{U}] \ \text{prod } A \ B \rightarrow A &= [A, B : \mathbb{U}][p : \text{prod } A \ B] \ p \ \text{false} \\
\text{pi2} : [A, B : \mathbb{U}] \ \text{prod } A \ B \rightarrow B &= [A, B : \mathbb{U}][p : \text{prod } A \ B] \ p \ \text{true}
\end{aligned}$$

As a last example, we can prove the so called ‘type-theoretic axiom of choice’ (see [Uni13] 1.6 and 2.15.7) and the induction/elimination principle for  $\Sigma$ -types,<sup>40</sup> but note that these need  $\eta$ -conversion to type-check. From the induction principle we can deduce the recursion (i.e. non-dependent) principle.

$$\begin{aligned}
\text{AC} : [A : \mathbb{U}][B : \mathbb{U}][C : A \rightarrow B \rightarrow \mathbb{U}] \\
&\quad ([x : A]\langle y : B \rangle C \ x \ y) \rightarrow \langle f : A \rightarrow B \rangle [x : A] \ C \ x \ (f \ x) \\
&= [A : \mathbb{U}][B : \mathbb{U}][C : A \rightarrow B \rightarrow \mathbb{U}][h : [x : A]\langle y : B \rangle C \ x \ y] \\
&\quad (([x : A](h \ x).1), ([x : A](h \ x).2))
\end{aligned}$$

<sup>40</sup>Recall that we chose to use projections as primitives in our language.

$$\begin{aligned}
\text{indSigma} &: [A : \mathbb{U}][B : A \rightarrow \mathbb{U}][C : (\langle x : A \rangle B x) \rightarrow \mathbb{U}] \\
&\quad ([a : A][b : B a] C (a, b)) \rightarrow [p : \langle x : A \rangle B x] C p \\
&= [A : \mathbb{U}][B : A \rightarrow \mathbb{U}][C : (\langle x : A \rangle B x) \rightarrow \mathbb{U}] \\
&\quad [h : [a : A][b : B a] C (a, b)][p : \langle x : A \rangle B x] h p.1 p.2
\end{aligned}$$

$$\begin{aligned}
\text{recSigma} &: [A : \mathbb{U}][B : \mathbb{U}][C : A * B \rightarrow \mathbb{U}] \\
&\quad ([a : A][b : B] C (a, b)) \rightarrow [p : A * B] C p \\
&= [A : \mathbb{U}][B : \mathbb{U}][C : A * B \rightarrow \mathbb{U}][h : [a : A][b : B] C (a, b)] \\
&\quad \text{indSigma } A (A \rightarrow B) C h
\end{aligned}$$

## 1.2 Extension with partial and restriction types

We now extend the basic type theory discussed so far with the constructs of cubical type theory, that is the interval, formulas, systems, partial and restriction types. We also add a composition (i.e. Kan) operation, which however has to be seen only as an experimental feature, as its implementation is still incomplete.<sup>41</sup>

The syntax is expanded as follows:

$$\begin{aligned}
A, B, M &::= \dots \\
&\quad | \mathbb{I} \mid 0 \mid 1 && \text{(Interval)} \\
&\quad | [\psi_1 \mapsto M_1, \dots, \psi_n \mapsto M_n] && \text{(System)} \\
&\quad | [\varphi]A && \text{(Partial type)} \\
&\quad | [\psi_1 \mapsto M_1, \dots, \psi_n \mapsto M_n]A && \text{(Restriction type)} \\
\\
K &::= \dots \\
&\quad | \text{comp } K \varphi M_0 M_u M_b M_i && \text{(Composition)}
\end{aligned}$$

However, care must be taken in the case of **comp**, as it may become neutral when the first argument (type family) is not neutral but  $M_b$  is.<sup>42</sup>

<sup>41</sup>As already remarked in the introduction, we have not implemented it for the universe of types.

<sup>42</sup>For example for coproducts and naturals.



We also introduce a syntax for formulas (we use  $i$  and  $j$  for generic *interval variables*).

$$\begin{aligned}\chi &::= (i = 0) \mid (i = 1) \mid (i = j) && \text{(Atomic)} \\ \psi &::= \chi \mid \chi \wedge \psi && \text{(Conjunction)} \\ \varphi &::= \psi \mid \psi \vee \varphi && \text{(Disjunctive n.f.)}\end{aligned}$$

We chose not to allow arbitrary formulas in the syntax, but only conjunctive formulas in systems and restriction types and formulas in disjunctive normal form in partial types, because it makes little sense to write programs breaking that rule and because this constraint simplifies the implementation.

We will often use a standard vector notation for systems and restriction types, i.e. writing just

$$[\vec{\psi} \mapsto \vec{M}]$$

instead of

$$[\psi_1 \mapsto M_1, \dots, \psi_n \mapsto M_n].$$

When also write for example

$$[\vec{\psi} \mapsto \vec{f} \ a], \quad [\vec{\psi} \mapsto \vec{p}.1]$$

respectively for

$$[\psi_1 \mapsto f_1 \ a, \dots, \psi_n \mapsto f_n \ a], \quad [\psi_1 \mapsto (p_1).1, \dots, \psi_n \mapsto (p_n).1].$$

### 1.2.1 Path types

There is no need for a primitive syntax for path types in the language, as is in [CCHM15], because we can exploit restriction types to define path types as a derived notion. Indeed, a path  $p : \text{Path}_A(a, b)$  is nothing else than a  $p : \mathbb{I} \rightarrow A$  such that  $p \ 0 \equiv a$  and  $p \ 1 \equiv b$ , that is

$$\text{Path}_A(a, b) \equiv [i : \mathbb{I}][i = 0 \mapsto a, i = 1 \mapsto b]A.$$

More generally:

$$\text{Path} \equiv [A : \mathbb{U}][a, b : A][i : \mathbb{I}][i = 0 \mapsto a, i = 1 \mapsto b]A.$$

The trivial path at  $a : A$ , which corresponds to a proof of reflexivity, is then defined as the constant path at  $a$ :

$$\text{refl} : [A : \mathbb{U}][a : A] \text{Path}_A(a, a) = [A : \mathbb{U}][a : A][i : \mathbb{I}] \ a.$$

It is trivial to see that every inference rule of [CCHM15] (section 3.1) holds if path types are defined this way.

### 1.2.2 Syntax for composition

We use the following notation for compositions:  $\text{comp } F \varphi i_0 u b i$ , where:

- $F : \mathbb{I} \rightarrow \mathbb{U}$  is a type family;
- $\varphi$  is the formula describing the sides of the composition figure;
- $i_0 : \mathbb{I}$  is the starting point of the composition;
- $u : [x : \mathbb{I}][\varphi]F x$  is the partial term, defined on  $\varphi$ , which will be extended by the composition;
- $b : [\varphi \mapsto u i_0]F i_0$  is the base case, defined on the starting point  $i_0$ ; the term  $b$  must agree with  $u i_0$  on  $\varphi$ , that is on the intersections of the base with the sides;
- $i : \mathbb{I}$  is the end point of the composition.

The composition has type  $[i = i_0 \mapsto b, \varphi \mapsto u i]F i$ , i.e. it extends  $b$  on  $i = i_0$  and  $u$  on  $\varphi$ . Note that it cannot be just  $[\varphi \mapsto u i]F i$ , as under  $i = i_0$  the type would be  $[\varphi \mapsto u i_0]F i_0$ , the same as  $b$ , but we still have to assert that the composition and  $b$  are convertible in that case.

The inference rule for composition shall be therefore the following:<sup>43</sup>

$$\frac{\begin{array}{c} \Gamma \vdash \varphi : \mathbb{F} \quad \Gamma \vdash u : [x : \mathbb{I}][\varphi]F x \quad \Gamma \vdash i_0 : \mathbb{I} \\ \Gamma \vdash F : \mathbb{I} \rightarrow \mathbb{U} \quad \Gamma \vdash b : [\varphi \mapsto u i_0]F i_0 \quad \Gamma \vdash i : \mathbb{I} \end{array}}{\Gamma \vdash \text{comp } F \varphi i_0 u b i : [i = i_0 \mapsto b \mid \varphi \mapsto u i]F i}$$

We make an example to make clear how composition works, demonstrating how to obtain the concatenation of two paths.

Suppose we are given a type  $A : \mathbb{U}$  and three points  $a, b, c : A$ , with paths  $p : \text{Path}_A(a, b)$  and  $q : \text{Path}_A(b, c)$ ; we want to obtain a path  $pq : \text{Path}_A(a, c)$ .

We draw a square having  $p$  as the base, so  $i_0 \equiv 0$  is the starting point and  $p i$  is the base case, with the constant path  $\text{refl}_A(a)$  as the left side and the path  $q$  as the right side. With composition (at the end point 1) we finally obtain a path from  $a$  to  $c$ . In more detail, keeping in mind that we quantify over  $i : \mathbb{I}$  before the composition,

- $F$  is the constant type family  $\mathbb{I} \rightarrow A$ ;
- $\varphi$  is  $i = 0 \vee i = 1$  (left and right sides of the square);

<sup>43</sup>In section 1.3 we will state it more precisely, conforming to the bidirectional type-checking mechanism and using the directions environment in addition to the context.

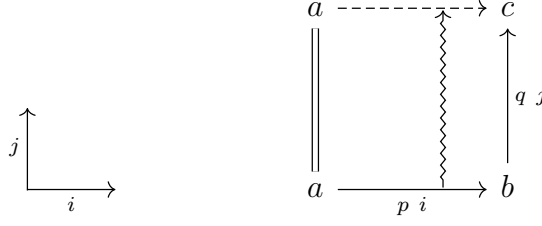


Figure 1.1: Concatenation of two paths. The result is the dotted line (lid of the square), which is a path connecting  $a$  to  $c$ . The twisted line only represents the act of composition (along the direction  $j$ ), obtaining a point on the lid from the base point  $p\ i$ , for each point  $i : \mathbb{I}$  which we quantify over.

- $i_0$  is the starting point 0;
- $u$  is the partial term defined only on the sides, given by

$$[j : \mathbb{I}][i = 0 \mapsto a, i = 1 \mapsto q\ j];^{44}$$

- $b$  is the base case, given by  $p\ i$ ;
- The end point is 1.<sup>45</sup>

The code for concatenation is therefore:

```
concat : [A : U][a, b, c : A] Path A a b → Path A b c → Path A a c
      = [A : U][a, b, c : A][p : Path A a b][q : Path A b c][i : I]
      comp (I → A) (i = 0 ∨ i = 1) 0 ([j : I][i = 0 ↦ a, i = 1 ↦ q j]) (p i) 1
```

Indeed we can verify, now informally using the evaluation rules which will be presented in section 1.4, that the concatenation is a path with the right endpoints:

$$\begin{aligned} & (\text{concat } A\ a\ b\ c\ p\ q)\ 0 \\ & \equiv \text{comp } (\mathbb{I} \rightarrow A)\ (0 = 0 \vee 0 = 1)\ 0\ ([j : \mathbb{I}][0 = 0 \mapsto a, 0 = 1 \mapsto q\ j])\ (p\ 0)\ 1 \\ & \equiv \text{comp } (\mathbb{I} \rightarrow A)\ \text{True}\ 0\ ([j : \mathbb{I}][\text{True} \mapsto a])\ a\ 1 \\ & \equiv ([j : \mathbb{I}][\text{True} \mapsto a])\ 0 \end{aligned}$$

<sup>44</sup>We use 1 because we are only interested in the lid, not on the whole square (filler), which we would get by using  $i$  as the end point.

<sup>45</sup>We could also have written  $\text{refl}_A(a)\ j$  instead of  $a$  in the system.

$$\equiv a$$

And similarly:

$$\begin{aligned} & (\text{concat } A \ a \ b \ c \ p \ q) \ 1 \\ & \equiv \text{comp } (\mathbb{I} \rightarrow A) \ (1 = 0 \vee 1 = 1) \ 0 \ ([j : \mathbb{I}][1 = 0 \mapsto a, 1 = 1 \mapsto q \ j]) \ (p \ 1) \ 1 \\ & \equiv \text{comp } (\mathbb{I} \rightarrow A) \ \text{True} \ 0 \ ([j : \mathbb{I}][\text{True} \mapsto q \ j]) \ b \ 1 \\ & \equiv ([j : \mathbb{I}][\text{True} \mapsto q \ j]) \ 1 \\ & \equiv q \ 1 \\ & \equiv c \end{aligned}$$

### 1.2.3 Contexts and directions environments

We give again the definition of the context, now allowing also interval variables declarations of the kind  $i : \mathbb{I}$ .<sup>46</sup>

**Definition 1.3** (Context).

1.  $()$  is the empty context;
2.  $\Gamma, x : A$  and  $\Gamma, i : \mathbb{I}$  extend the context  $\Gamma$  with a declaration;
3.  $\Gamma, x : A = M$  extends the context  $\Gamma$  with a definition;
4.  $\Gamma, x \mapsto \mathbf{v}$  extends the context  $\Gamma$  binding the variable  $x$  to the value  $\mathbf{v}$ .

The type-checking rules (section 1.3) require the use of formulas in contexts, e.g. when type-checking a declaration of the form  $\Gamma \vdash e : [\psi \mapsto t]A$ , one has to check that  $\Gamma, \psi \vdash t : A$ , that is,  $t$  has to be of type  $A$  when subject to the constraint  $\psi$ ; the context  $\Gamma, \psi$  has to be thought as a restricted context.

Instead of adding formulas to contexts, we use a different context-like structure to store information about formulas, called *directions environment*, because it makes the implementation and the presentation simpler, as the context and the directions environment serve different purposes which are handled distinctly.<sup>47</sup> The directions environment is used only during type-checking and  $\alpha\eta$ -conversion, and not during evaluation.

<sup>46</sup>However, we do not allow definitions of type  $\mathbb{I}$ , that is of the form  $i : \mathbb{I} = j$ . This would complicate the evaluation of formulas, especially when the directions environment contains an interval variable which also has a definition, and we don't think it would be useful at all.

<sup>47</sup>Note that if  $\Gamma$  and  $\Delta$  are contexts without formulas, then a judgment in  $\Gamma, \psi_1, \Delta, \psi_2$  is equivalent to a judgement in  $\Gamma, \Delta, \psi_1 \wedge \psi_2$ . This means that we can always split the 'full' context into two contexts  $\Gamma; \Theta$ , where  $\Gamma$  does not contain any formula and  $\Theta$  is the directions environment.

Moreover, note that the meaning of a judgement of the form  $\Gamma, \psi_1 \vee \dots \psi_n \vdash J$  is that  $\Gamma, \psi_1 \vdash J, \dots, \Gamma, \psi_n \vdash J$ , so that the directions environment only need to store information about a conjunction of atomic formulas.

To manage and simplify conjunctive formulas efficiently, we use a particular data structure which is formed by:

- A list (*zeros*) of names which shall be replaced by 0.
- A list (*ones*) of names which shall be replaced by 1.
- A list of partitions (*diagonals*), that is, a list of lists of names; each partition represents the names which shall be identified.

For example, the formula  $(i = 0) \wedge (j = k) \wedge (w = r) \wedge (w = 1)$  is stored as  $([i], [w, r], [[j, k]])$ , meaning that  $i$  is mapped to 0,  $w, r$  to 1 and  $j, k$  are identified.

Even if it is implemented using the aforementioned lists, we will use a simple context-like notation for the directions environment, as if it were a list of bindings.

**Definition 1.4** (Directions environment).

1.  $()$  is the empty directions environment;
2.  $\Theta, i \mapsto 0$  (or  $i \mapsto 1$ ) extends the directions environment  $\Theta$  binding the name  $i$  to 0 (or to 1);
3.  $\Theta, i \mapsto j$  extends the directions environment  $\Theta$  binding the name  $i$  to the name  $j$  (diagonal).

As a last note, it is important to keep in mind that interval values can appear both in the directions environment (which is used when checking under a formula) and in the context during evaluation (e.g.  $\Gamma$  could contain value bindings of the form  $i \mapsto 0$ ,  $i \mapsto 1$  or  $i \mapsto j^{\mathbb{I}}$ ), but the two are indeed used for distinct purposes.

## 1.3 Typing rules

We now present the type-checking rules for the full system, extending the ones of section 1.1.3. The main difference is that now judgments are of the form

$$\Gamma; \Theta \vdash J$$

i.e. we use not only the context  $\Gamma$ , but also the directions environment  $\Theta$ , which is used when type-checking under a formula (constraint).

We also need other kinds of judgments to state the rules, which are:

- $\Gamma \vdash \varphi : \mathbb{F}$  means that  $\varphi$  is a formula whose variables are declared in  $\Gamma$ .
- $\mathbf{v}_1 \sim_{\tau(\Gamma)}^{\Theta} \mathbf{v}_2$  means that values  $\mathbf{v}_1$  and  $\mathbf{v}_2$  are  $\alpha\eta$ -equivalent modulo the constraints in  $\Theta$ ;  $\tau(\Gamma)$  is the list of names declared in the context  $\Gamma$ .<sup>48</sup>
- $\psi_1 \leq^{\Theta} \psi_2$  means that  $\psi_1$  logically implies  $\psi_2$  modulo the constraints in  $\Theta$ .
- $\psi_1 \sim^{\Theta} \psi_2$  means that  $\psi_1$  and  $\psi_2$  are logically equivalent modulo the constraints in  $\Theta$ , i.e. that  $\psi_1 \leq^{\Theta} \psi_2$  and  $\psi_2 \leq^{\Theta} \psi_1$ .

The implementation of the three judgments regarding the formulas is relatively straightforward and is discussed in sections 3.2 and 3.6.

We allow only a restricted form of subtyping, as specified by the rules (Weak-Partial) and (Weak-Restr). This means that subtyping works only at the ‘top-level’, e.g.

$$\begin{aligned} x &: [i = 0 \vee i = 1]\mathbb{N} \\ y &: [i = 0]\mathbb{N} = x \end{aligned}$$

is admitted but

$$\begin{aligned} f &: [i : \mathbb{I}][i = 0 \vee i = 1]\mathbb{N} \\ g &: [i : \mathbb{I}][i = 0]\mathbb{N} = f \end{aligned}$$

is rejected.<sup>49</sup> Note that however we can still define  $g$  as follows:

$$g' : [i : \mathbb{I}][i = 0]\mathbb{N} = [i : \mathbb{I}] f i$$

## Type inference

$$\overline{\Gamma; \Theta \vdash x \Rightarrow \text{LOOKUPTYPE}(\Gamma, x)} \quad (\text{Var})$$

$$\overline{\Gamma; \Theta \vdash \mathbb{U} \Rightarrow \mathbb{U}} \quad (\text{Universe})$$

<sup>48</sup>See section 1.5.

<sup>49</sup>Even  $y' : [i = 0]\mathbb{N} = [i = 0 \mapsto \mathbb{Z}, i = 1 \mapsto \mathbb{S} \mathbb{Z}]$  is rejected, as it makes no sense to write it that way (compare with  $y$ ).

$$\frac{\Gamma; \Theta \vdash f \Rightarrow \text{closure}([x : ty]e, \Gamma') \quad \Gamma; \Theta \vdash a \Leftarrow (ty)_{\Gamma'}}{\Gamma; \Theta \vdash f \ a \Rightarrow \text{APP}(\text{closure}([x : ty]e, \Gamma'), (a)_{\Gamma})} \quad (\text{App})$$

$$\frac{\Gamma; \Theta \vdash f \Rightarrow [\vec{\psi} \mapsto \vec{g}] \text{closure}([x : ty]e, \Gamma') \quad \Gamma; \Theta \vdash a \Leftarrow (ty)_{\Gamma'}}{\Gamma; \Theta \vdash f \ a \Rightarrow [\vec{\psi} \mapsto \text{APP}(\vec{g}, (a)_{\Gamma})] \text{APP}(\text{closure}([x : ty]e, \Gamma'), (a)_{\Gamma})} \quad (\text{App-Restr})$$

$$\frac{\Gamma; \Theta \vdash f \Rightarrow [\varphi] \text{closure}([x : ty]e, \Gamma') \quad \Gamma; \Theta \vdash a \Leftarrow (ty)_{\Gamma'}}{\Gamma; \Theta \vdash f \ a \Rightarrow [\varphi] \text{APP}(\text{closure}([x : ty]e, \Gamma'), (a)_{\Gamma})} \quad (\text{App-Partial})$$

$$\frac{\Gamma; \Theta \vdash p \Rightarrow \text{closure}(\langle x : ty \rangle e, \Gamma')}{\Gamma; \Theta \vdash p.1 \Rightarrow (ty)_{\Gamma'}} \quad (\text{Sigma-1})$$

$$\frac{\Gamma; \Theta \vdash p \Rightarrow \text{closure}(\langle x : ty \rangle e, \Gamma')}{\Gamma; \Theta \vdash p.2 \Rightarrow (e)_{\Gamma', x \mapsto (p.1)_{\Gamma}}} \quad (\text{Sigma-2})$$

$$\frac{\Gamma; \Theta \vdash p \Rightarrow [\vec{\psi} \mapsto \vec{q}] \text{closure}(\langle x : ty \rangle e, \Gamma')}{\Gamma; \Theta \vdash p.1 \Rightarrow [\vec{\psi} \mapsto \text{FST}(\vec{q})](ty)_{\Gamma'}} \quad (\text{Sigma-1-Restr})$$

$$\frac{\Gamma; \Theta \vdash p \Rightarrow [\vec{\psi} \mapsto \vec{q}] \text{closure}(\langle x : ty \rangle e, \Gamma')}{\Gamma; \Theta \vdash p.2 \Rightarrow [\vec{\psi} \mapsto \text{SND}(\vec{q})](e)_{\Gamma', x \mapsto (p.1)_{\Gamma}}} \quad (\text{Sigma-2-Restr})$$

$$\frac{\Gamma; \Theta \vdash p \Rightarrow [\varphi] \text{closure}(\langle x : ty \rangle e, \Gamma')}{\Gamma; \Theta \vdash p.1 \Rightarrow [\varphi](ty)_{\Gamma'}} \quad (\text{Sigma-1-Partial})$$

$$\frac{\Gamma; \Theta \vdash p \Rightarrow [\varphi] \text{closure}(\langle x : ty \rangle e, \Gamma')}{\Gamma; \Theta \vdash p.2 \Rightarrow [\varphi](e)_{\Gamma', x \mapsto (p.1)_{\Gamma}}} \quad (\text{Sigma-2-Partial})$$

$$\frac{\Gamma; \Theta \vdash F \Leftarrow \mathbf{ty}_1 + \mathbf{ty}_2 \rightarrow \mathbf{U} \quad \Gamma; \Theta \vdash f_1 \Leftarrow ([x : ty_1] \ F \ (\mathbf{inl} \ x))_{\Gamma} \quad \Gamma; \Theta \vdash t \Rightarrow \mathbf{ty}_1 + \mathbf{ty}_2 \quad \Gamma; \Theta \vdash f_2 \Leftarrow ([x : ty_2] \ F \ (\mathbf{inr} \ x))_{\Gamma}}{\Gamma; \Theta \vdash \text{split} \ F \ f_1 \ f_2 \ t \Rightarrow (F \ t)_{\Gamma}} \quad (x = \text{NEWVAR}(\Gamma)) \quad (\text{Split})$$

$$\frac{\Gamma; \Theta \vdash F \Leftarrow \mathbf{ty}_1 + \mathbf{ty}_2 \rightarrow \mathbf{U} \quad \Gamma; \Theta \vdash f_1 \Leftarrow ([x : ty_1] F (\mathbf{inl} x))_{\Gamma} \quad \Gamma; \Theta \vdash t \Rightarrow [\vec{\psi} \mapsto \vec{\mathbf{t}}](\mathbf{ty}_1 + \mathbf{ty}_2) \quad \Gamma; \Theta \vdash f_2 \Leftarrow ([x : ty_2] F (\mathbf{inr} x))_{\Gamma}}{\Gamma; \Theta \vdash \mathbf{split} F f_1 f_2 t \Rightarrow [\vec{\psi} \mapsto \mathbf{SPLIT}((F)_{\Gamma}, (f_1)_{\Gamma}, (f_2)_{\Gamma}, \vec{\mathbf{t}})](F t)_{\Gamma}} \quad (x = \mathbf{NEWVAR}(\Gamma))$$

(Split-Restr)

$$\frac{\Gamma; \Theta \vdash F \Leftarrow \mathbf{ty}_1 + \mathbf{ty}_2 \rightarrow \mathbf{U} \quad \Gamma; \Theta \vdash f_1 \Leftarrow ([x : ty_1] F (\mathbf{inl} x))_{\Gamma} \quad \Gamma; \Theta \vdash t \Rightarrow [\varphi](\mathbf{ty}_1 + \mathbf{ty}_2) \quad \Gamma; \Theta \vdash f_2 \Leftarrow ([x : ty_2] F (\mathbf{inr} x))_{\Gamma}}{\Gamma; \Theta \vdash \mathbf{split} F f_1 f_2 t \Rightarrow [\varphi](F t)_{\Gamma}} \quad (x = \mathbf{NEWVAR}(\Gamma))$$

(Split-Partial)

$$\frac{\Gamma \vdash \varphi : \mathbb{F} \quad \Gamma; \Theta \vdash u \Leftarrow ([x : \mathbb{I}][\varphi] F x)_{\Gamma} \quad \Gamma; \Theta \vdash i_0 \Leftarrow \mathbb{I} \quad \Gamma; \Theta \vdash F \Leftarrow \mathbb{I} \rightarrow \mathbf{U} \quad \Gamma; \Theta \vdash b \Leftarrow ([\varphi \mapsto u i_0] F i_0)_{\Gamma} \quad \Gamma; \Theta \vdash i \Leftarrow \mathbb{I}}{\Gamma; \Theta \vdash \mathbf{comp} F \varphi i_0 u b i \Rightarrow ([i = i_0 \mapsto b \mid \varphi \mapsto u i] F i)_{\Gamma}} \quad (x = \mathbf{NEWVAR}(\Gamma))$$

(Comp)

$$\overline{\Gamma; \Theta \vdash \mathbf{N} \Rightarrow \mathbf{U}} \quad (\text{Nat})$$

$$\overline{\Gamma; \Theta \vdash \mathbf{Z} \Rightarrow \mathbf{N}} \quad (\text{Zero})$$

$$\frac{\Gamma; \Theta \vdash n \Leftarrow \mathbf{N}}{\Gamma; \Theta \vdash \mathbf{S} n \Rightarrow \mathbf{N}} \quad (\text{Succ})$$

$$\frac{\Gamma; \Theta \vdash F \Leftarrow \mathbf{N} \rightarrow \mathbf{U} \quad \Gamma; \Theta \vdash c_0 \Leftarrow (F \mathbf{Z})_{\Gamma} \quad \Gamma; \Theta \vdash n \Leftarrow \mathbf{N} \quad \Gamma; \Theta \vdash c_s \Leftarrow ([m : \mathbf{N}] F m \rightarrow F (\mathbf{S} m))_{\Gamma}}{\Gamma; \Theta \vdash \mathbf{ind} F c_0 c_s n \Rightarrow (F n)_{\Gamma}} \quad (m = \mathbf{NEWVAR}(\Gamma))$$

(Ind)

$$\frac{\Gamma; \Theta \vdash F \Leftarrow \mathbf{N} \rightarrow \mathbf{U} \quad \Gamma; \Theta \vdash c_0 \Leftarrow (F \mathbf{Z})_{\Gamma} \quad \Gamma; \Theta \vdash n \Leftarrow [\vec{\psi} \mapsto \vec{\mathbf{m}}]\mathbf{N} \quad \Gamma; \Theta \vdash c_s \Leftarrow ([m : \mathbf{N}] F m \rightarrow F (\mathbf{S} m))_{\Gamma}}{\Gamma; \Theta \vdash \mathbf{ind} F c_0 c_s n \Rightarrow [\vec{\psi} \mapsto \mathbf{IND}((F)_{\Gamma}, (c_0)_{\Gamma}, (c_s)_{\Gamma}, \vec{\mathbf{m}})](F n)_{\Gamma}} \quad (m = \mathbf{NEWVAR}(\Gamma))$$

(Ind-Restr)



$$\frac{\Gamma; \Theta \vdash F \Leftarrow \mathbb{N} \rightarrow \mathbb{U} \quad \Gamma; \Theta \vdash c_0 \Leftarrow (F \ Z)_\Gamma \quad \Gamma; \Theta \vdash n \Leftarrow [\varphi]\mathbb{N} \quad \Gamma; \Theta \vdash c_s \Leftarrow ([m : \mathbb{N}] \ F \ m \rightarrow F \ (\mathbb{S} \ m))_\Gamma}{\Gamma; \Theta \vdash \text{ind } F \ c_0 \ c_s \ n \Rightarrow [\varphi](F \ n)_\Gamma} \quad (m = \text{NEWVAR}(\Gamma))$$

(Ind-Partial)

$$\overline{\Gamma; \Theta \vdash 0 \Rightarrow \mathbb{I}} \quad (\text{Interval-0})$$

$$\overline{\Gamma; \Theta \vdash 1 \Rightarrow \mathbb{I}} \quad (\text{Interval-1})$$

### Type checking

$$\frac{\Gamma; \Theta \vdash ty \Leftarrow \mathbb{U} \quad \Gamma; \Theta \vdash e \Leftarrow (ty)_\Gamma \quad \Gamma, x : ty = e; \Theta \vdash t \Leftarrow \mathbf{A}}{\Gamma; \Theta \vdash [x : ty = e]t \Leftarrow \mathbf{A}} \quad (\text{Def})$$

$$\frac{\Gamma; \Theta \vdash ty \Leftarrow \mathbb{U} \quad \Gamma, x : ty; \Theta \vdash e \Leftarrow \mathbb{U}}{\Gamma; \Theta \vdash [x : ty]e \Leftarrow \mathbb{U}} \quad (\text{Pi})$$

$$\frac{\Gamma, x : \mathbb{I}; \Theta \vdash e \Leftarrow \mathbb{U}}{\Gamma; \Theta \vdash [x : \mathbb{I}]e \Leftarrow \mathbb{U}} \quad (\text{Pi-II})$$

$$\frac{\Gamma; \Theta \vdash ty \Leftarrow \mathbb{U} \quad \Gamma, x : ty; \Theta \vdash e \Leftarrow \mathbb{U}}{\Gamma; \Theta \vdash \langle x : ty \rangle e \Leftarrow \mathbb{U}} \quad (\text{Sigma})$$

$$\frac{\Gamma; \Theta \vdash ty \Leftarrow \mathbb{U} \quad (ty)_\Gamma \sim_{\tau(\Gamma)}^\Theta (ty_1)_{\Gamma_1} \quad \Gamma, x : ty, x \mapsto v; \Theta \vdash e \Leftarrow \text{APP}(\text{closure}([x_1 : ty_1]e_1, \Gamma_1), v^{(ty_1)_{\Gamma_1}})}{\Gamma; \Theta \vdash [x : ty]e \Leftarrow \text{closure}([x_1 : ty_1]e_1, \Gamma_1)} \quad (v = \text{NEWVAR}(\Gamma_1))$$

(Abstraction)

$$\frac{\Gamma; \Theta \vdash s \Leftarrow (ty)_{\Gamma'} \quad \Gamma; \Theta \vdash t \Leftarrow (e)_{\Gamma', x \mapsto (s)_\Gamma}}{\Gamma; \Theta \vdash (s, t) \Leftarrow \text{closure}(\langle x : ty \rangle e, \Gamma')} \quad (\text{Pair})$$

$$\frac{\Gamma; \Theta \vdash A \Leftarrow \mathbb{U} \quad \Gamma; \Theta \vdash B \Leftarrow \mathbb{U}}{\Gamma; \Theta \vdash A + B \Leftarrow \mathbb{U}} \quad (\text{Sum})$$

$$\frac{\Gamma; \Theta \vdash t_1 \Leftarrow \mathbf{A}}{\Gamma; \Theta \vdash \text{inl } t_1 \Leftarrow \mathbf{A} + \mathbf{B}} \quad (\text{Inl})$$

$$\frac{\Gamma; \Theta \vdash t_2 \Leftarrow \mathbf{B}}{\Gamma; \Theta \vdash \text{inr } t_2 \Leftarrow \mathbf{A} + \mathbf{B}} \quad (\text{Inr})$$

$$\frac{\Gamma \vdash \psi_i : \mathbb{F} \quad \varphi \sim^\Theta (\psi_1 \vee \dots \vee \psi_n) \quad \Gamma; \Theta \vdash t_i \Leftarrow [\psi_i] \mathbf{A} \quad (t_i)_\Gamma \sim_{\tau(\Gamma)}^{\Theta, \psi_i \wedge \psi_j} (t_j)_\Gamma \quad (1 \leq i, j \leq n)}{\Gamma \vdash [\psi_1 \mapsto t_1, \dots, \psi_n \mapsto t_n] \Leftarrow [\varphi] \mathbf{A}} \quad (\text{System})$$

$$\frac{\Gamma \vdash \psi_i : \mathbb{F} \quad \Gamma; \Theta \vdash A \Leftarrow \mathbf{U}}{\Gamma; \Theta \vdash [\psi_1 \vee \dots \vee \psi_n] A \Leftarrow \mathbf{U}} \quad (1 \leq i \leq n) \quad (\text{Partial-U})$$

$$\frac{\Gamma; \Theta, \varphi \vdash t \Leftarrow \mathbf{A}}{\Gamma; \Theta \vdash t \Leftarrow [\varphi] \mathbf{A}} \quad (\text{Partial})$$

$$\frac{\Gamma; \Theta \vdash A \Leftarrow \mathbf{U} \quad \Gamma \vdash \psi_i : \mathbb{F} \quad \Gamma; \Theta \vdash t_i \Leftarrow [\psi_i](A)_\Gamma \quad (1 \leq i \leq n)}{\Gamma; \Theta \vdash [\psi_1 \mapsto t_1, \dots, \psi_n \mapsto t_n] A \Leftarrow \mathbf{U}} \quad (\text{Restr-U})$$

$$\frac{\Gamma; \Theta \vdash e \Leftarrow \mathbf{A} \quad (e)_\Gamma \sim_{\tau(\Gamma)}^{\Theta, \psi_i} \mathbf{t}_i}{\Gamma; \Theta \vdash e \Leftarrow [\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n] \mathbf{A}} \quad (1 \leq i \leq n) \quad (\text{Restr})$$

$$\frac{\Gamma \vdash e \Rightarrow [\psi'] \mathbf{A}' \quad \psi \leq^\Theta \psi' \quad \mathbf{A} \sim_{\tau(\Gamma)}^\Theta \mathbf{A}'}{\Gamma \vdash e \Leftarrow [\psi] \mathbf{A}} \quad (\text{Weak-Partial})$$

$$\frac{\Gamma \vdash e \Rightarrow [\vec{\psi}' \mapsto \vec{\mathbf{t}}'] \mathbf{A}' \quad [\vec{\psi} \mapsto \vec{\mathbf{t}}] \sim_{\tau(\Gamma)}^{\Theta, \psi_1 \vee \dots \vee \psi_n} [\vec{\psi}' \mapsto \vec{\mathbf{t}}'] \quad \mathbf{A} \sim_{\tau(\Gamma)}^\Theta \mathbf{A}'}{\Gamma \vdash e \Leftarrow [\vec{\psi} \mapsto \vec{\mathbf{t}}] \mathbf{A}} \quad (\text{Weak-Restr})$$

$$\frac{\Gamma; \Theta \vdash e \Rightarrow \mathbf{A} \quad \mathbf{A} \sim_{\tau(\Gamma)}^\Theta \mathbf{A}'}{\Gamma; \Theta \vdash e \Leftarrow \mathbf{A}'} \quad (\text{Infer})$$

## 1.4 Evaluation

We now extend evaluation, first presented in section 1.1.4, to handle the new cubical constructs.

We denote with  $(\varphi)_\Gamma$  the substitution in the formula  $\varphi$  of the bindings stored in  $\Gamma$ ,<sup>50</sup> which is thought as the evaluation of the formula  $\varphi$ .

$$\begin{aligned}
 (\mathbb{I})_\Gamma &= \mathbb{I} \\
 (0)_\Gamma &= 0 \\
 (1)_\Gamma &= 1 \\
 ([\vec{\psi} \mapsto \vec{M}])_\Gamma &= \begin{cases} (M_i)_\Gamma & \text{if } (\psi_i)_\Gamma \text{ is true} \\ [(\vec{\psi})_\Gamma \mapsto (\vec{M})_\Gamma] & \text{otherwise} \end{cases} \\
 ([\varphi]A)_\Gamma &= \text{FOLDPARTIAL}([\varphi]_\Gamma)(A)_\Gamma \\
 ([\vec{\psi} \mapsto \vec{M}]A)_\Gamma &= \text{FOLDRESTR}([\vec{\psi}]_\Gamma \mapsto (\vec{M})_\Gamma)(A)_\Gamma \\
 (\text{comp } F \ \varphi \ i_0 \ u \ b \ i)_\Gamma &= \text{COMP}(\Gamma, F, \varphi, i_0, u, b, i)
 \end{aligned}$$

Note than when evaluating systems, if at least a formula is true, the type-checking assures that we can choose any value associated to a true formula, being them all convertible to each other.

The evaluation function uses some helpers:

- The routine `FOLDRESTR` collapses all the terms or values the form

$$[\vec{\psi}_1 \mapsto \vec{M}_1] \dots [\vec{\psi}_n \mapsto \vec{M}_n]A,$$

where  $A$  is not a restriction type, to

$$[\vec{\psi}_1 \mapsto \vec{M}_1, \dots, \vec{\psi}_n \mapsto \vec{M}_n]A.$$

The routine `FOLDPARTIAL` works analogously. This simplifies the type-checker since we put restriction and partial types in a kind of normal form, so that we don't need explicit rules to handle this problem.

- `SIMPLIFY-NV` gets as input a neutral value, and if its type is a restriction type with a true formula, then the corresponding value is returned, otherwise the value is left untouched. Note that `SIMPLIFY-NV` does not

---

<sup>50</sup>This is used also for interval variables renaming, which is needed since, for example, if  $q : \text{Path } A \ b \ c \equiv [i : \mathbb{I}][i = 0 \mapsto b, i = 1 \mapsto c]A$ , then  $q \ j$  should be annotated with the type  $[j = 0 \mapsto b, j = 1 \mapsto c]A$ .

depend on the directions environment, and indeed SIMPLIFY-NV is used solely during evaluation.

$$\begin{aligned} \text{SIMPLIFY-NV}(\mathbf{v}^{[\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n]} \mathbf{A}) &= \mathbf{t}_i && (\text{if } \psi_i \text{ is true}) \\ \text{SIMPLIFY-NV}(\mathbf{v}) &= \mathbf{v} && (\text{otherwise}) \end{aligned}$$

Since we use FOLDRESTR, the function SIMPLIFY-NV need not be recursive, as  $\mathbf{t}_i$  must be of type  $[\psi] \mathbf{A}$ .

We now have to revisit the helpers introduced in section 1.1.4, handling the possibility that the argument is a neutral value with a partial or restriction type, which requires attention.

- APP applied to  $\mathbf{f}$  and  $\mathbf{a}$  first checks if  $\mathbf{f}$  is a closure, in which case it evaluates it, otherwise  $\mathbf{f} \mathbf{a}$  must be a neutral application which gets annotated with its type, handling the eventual partial or restriction type. The need for SIMPLIFY-NV is easily explained: suppose that  $\mathbf{p}$  is neutral with type  $\text{Path } A \ a \ b$ , that is  $[i : \mathbb{I}] [i = 0 \mapsto \mathbf{a}, i = 1 \mapsto \mathbf{b}] \mathbf{A}$ . Then the application  $\text{APP}(\mathbf{p}, 0)$  shall reduce to the neutral value  $(\mathbf{p} \ 0)$  annotated with the type  $[\text{True} \mapsto \mathbf{a}, \text{False} \mapsto \mathbf{b}] \mathbf{A}$ , which means that  $(\mathbf{p} \ 0)$  has to be simplified to  $\mathbf{a}$ . When the function is neutral with a restriction type, e.g.  $\mathbf{f}^{[\psi \mapsto \mathbf{g}]} (\mathbf{A} \rightarrow \mathbf{B})$ , then  $\text{APP}(\mathbf{f}, \mathbf{a})$  shall reduce to  $(\mathbf{f} \ \mathbf{a})$  annotated with the type  $[\psi \mapsto \text{APP}(\mathbf{g}, \mathbf{a})] \mathbf{B}$ ; we invoke FOLDRESTR to handle the case where  $\mathbf{B}$  is itself a restriction type.

$$\begin{aligned} \text{APP}(\text{closure}([x : ty]e, \Gamma), \mathbf{a}) &= (e)_{\Gamma, x \mapsto \mathbf{a}} \\ \text{APP}(\mathbf{f}^{\text{closure}([x : ty]e, \Gamma)}, \mathbf{a}) &= \text{SIMPLIFY-NV}((\mathbf{f} \ \mathbf{a})^{(e)_{\Gamma, x \mapsto \mathbf{a}}}) \\ \text{APP}(\mathbf{f}^{[\vec{\psi} \mapsto \vec{\mathbf{g}}]} \text{closure}([x : ty]e, \Gamma), \mathbf{a}) &= \text{SIMPLIFY-NV}((\mathbf{f} \ \mathbf{a})^{\mathbf{v}}) \\ & \quad (\text{where } \mathbf{v} = \text{FOLDRESTR}([\vec{\psi} \mapsto \text{APP}(\vec{\mathbf{g}}, \mathbf{a})](e)_{\Gamma, x \mapsto \mathbf{a}})) \end{aligned}$$

A drawback of our unified syntax for  $\lambda$ - and  $\Pi$ -abstractions is that the APP function must handle both, which may be a bit confusing. We have then to add the case where a restricted neutral  $\Pi$ -type is applied to an argument.

$$\text{APP}([\vec{\psi} \mapsto \vec{\mathbf{g}}] \mathbf{f}, \mathbf{a}) = \text{FOLDRESTR}([\vec{\psi} \mapsto \text{APP}(\vec{\mathbf{g}}, \mathbf{a})] \text{APP}(\mathbf{f}, \mathbf{a}))$$

Lastly we handle partial types, that is the cases of a system of functions, and of a neutral function with partial type.

$$\begin{aligned} \text{APP}([\vec{\psi} \mapsto \vec{\mathbf{f}}], \mathbf{a}) &= [\vec{\psi} \mapsto \text{APP}(\vec{\mathbf{f}}, \mathbf{a})] \\ \text{APP}(\mathbf{f}^{[\varphi] \text{closure}([x : ty]e, \Gamma)}, \mathbf{a}) &= (\mathbf{f} \ \mathbf{a})^{\text{FOLDPARTIAL}([\varphi](e)_{\Gamma, x \mapsto \mathbf{a}})} \end{aligned}$$

- FST and SND return respectively the first and the second component of a pair, if the value is not neutral; otherwise they annotate the whole value with the corresponding type, handling the eventual partial or restriction type. Similarly to APP, the case of neutral values requires some explanation: suppose that  $\mathbf{v}$  is neutral with type  $([\psi_1 \mapsto \mathbf{a}]A) * ([\psi_2 \mapsto \mathbf{b}]B)$ , where  $\psi_1$  is true. Then  $\text{FST}(\mathbf{v})$  should be neutral with type  $([\psi_1 \mapsto \mathbf{a}]A)$  and so the whole value shall reduce to  $\mathbf{a}$ ; this is why we need to invoke SIMPLIFY-NV. Analogous is the case of  $\text{FST}(\mathbf{v})$ , when  $\psi_2$  is true. When  $\mathbf{v}$  has a restriction type, e.g.  $[\vec{\psi} \mapsto \vec{\mathbf{w}}](\mathbf{A} * \mathbf{B})$  for simplicity, then  $\text{FST}(\mathbf{v})$  shall have type  $[\vec{\psi} \mapsto \text{FST}(\vec{\mathbf{w}})]\mathbf{A}$ ; we call FOLDRESTR as  $\mathbf{A}$  may be a restriction type too, and finally we still invoke SIMPLIFY-NV for the same reason as the simpler (i.e. non-restricted) case. Analogously for partial types.

$$\begin{aligned}
\text{FST}((\mathbf{v}_1, \mathbf{v}_2)) &= \mathbf{v}_1 \\
\text{FST}(\mathbf{v}^{\text{closure}(\langle x:ty \rangle e, \Gamma)}) &= \text{SIMPLIFY-NV}((\mathbf{v}.1)^{(ty)_\Gamma}) \\
\text{FST}(\mathbf{v}^{[\vec{\psi} \mapsto \vec{\mathbf{w}}]\text{closure}(\langle x:ty \rangle e, \Gamma)}) &= \text{SIMPLIFY-NV}((\mathbf{v}.1)^{\mathbf{v}}) \\
&\quad (\text{where } \mathbf{v} = \text{FOLDRESTR}([\vec{\psi} \mapsto \text{FST}(\vec{\mathbf{w}})](ty)_\Gamma)) \\
\text{FST}([\vec{\psi} \mapsto \vec{\mathbf{v}}]) &= [\vec{\psi} \mapsto \text{FST}(\vec{\mathbf{v}})] \\
\text{FST}(\mathbf{v}^{[\varphi]\text{closure}(\langle x:ty \rangle e, \Gamma)}) &= (\mathbf{v}.1)^{\text{FOLDPARTIAL}([\varphi](ty)_\Gamma)}
\end{aligned}$$

$$\begin{aligned}
\text{SND}((\mathbf{v}_1, \mathbf{v}_2)) &= \mathbf{v}_2 \\
\text{SND}(\mathbf{v}^{\text{closure}(\langle x:ty \rangle e, \Gamma)}) &= \text{SIMPLIFY-NV}((\mathbf{v}.2)^{(e)_{\Gamma, x \mapsto \text{FST}(\mathbf{v})}}) \\
\text{SND}(\mathbf{v}^{[\vec{\psi} \mapsto \vec{\mathbf{w}}]\text{closure}(\langle x:ty \rangle e, \Gamma)}) &= \text{SIMPLIFY-NV}((\mathbf{v}.2)^{\mathbf{v}}) \\
&\quad (\text{where } \mathbf{v} = \text{FOLDRESTR}([\vec{\psi} \mapsto \text{SND}(\vec{\mathbf{w}})](e)_{\Gamma, x \mapsto \text{FST}(\mathbf{v})}) \\
\text{SND}([\vec{\psi} \mapsto \vec{\mathbf{v}}]) &= [\vec{\psi} \mapsto \text{SND}(\vec{\mathbf{v}})] \\
\text{SND}(\mathbf{v}^{[\varphi]\text{closure}(\langle x:ty \rangle e, \Gamma)}) &= (\mathbf{v}.2)^{\text{FOLDPARTIAL}([\varphi](e)_{\Gamma, x \mapsto \text{FST}(\mathbf{v})})}
\end{aligned}$$

- SPLIT does by-case analysis on the given argument, if not neutral, otherwise the whole term becomes neutral, handling the neutral cases analogously to the previous helpers.

$$\begin{aligned}
\text{SPLIT}(\mathbf{F}, \mathbf{f}_1, \mathbf{f}_2, \text{inl } \mathbf{v}_1) &= \text{APP}(\mathbf{f}_1, \mathbf{v}_1) \\
\text{SPLIT}(\mathbf{F}, \mathbf{f}_1, \mathbf{f}_2, \text{inr } \mathbf{v}_2) &= \text{APP}(\mathbf{f}_2, \mathbf{v}_2) \\
\text{SPLIT}(\mathbf{F}, \mathbf{f}_1, \mathbf{f}_2, \mathbf{v}^{\mathbf{A}+\mathbf{B}}) &= \text{SIMPLIFY-NV}((\text{split } \mathbf{F} \ \mathbf{f}_1 \ \mathbf{f}_2 \ \mathbf{v})^{\text{APP}(\mathbf{F}, \mathbf{v})}) \\
\text{SPLIT}(\mathbf{F}, \mathbf{f}_1, \mathbf{f}_2, \mathbf{v}^{[\vec{\psi} \mapsto \vec{\mathbf{w}}]\mathbf{A}+\mathbf{B}}) &= \text{SIMPLIFY-NV}((\text{split } \mathbf{F} \ \mathbf{f}_1 \ \mathbf{f}_2 \ \mathbf{v})^{\mathbf{v}})
\end{aligned}$$

$$\begin{aligned}
& (\text{where } \mathbf{v} = \text{FOLDRESTR}([\vec{\psi} \mapsto \text{SPLIT}(\mathbf{F}, \mathbf{f}_1, \mathbf{f}_2, \vec{\mathbf{w}})] \text{APP}(\mathbf{F}, \mathbf{v}))) \\
& \text{SPLIT}(\mathbf{F}, \mathbf{f}_1, \mathbf{f}_2, [\vec{\psi} \mapsto \vec{\mathbf{v}}]) = [\vec{\psi} \mapsto \text{SPLIT}(\mathbf{F}, \mathbf{f}_1, \mathbf{f}_2, \vec{\mathbf{v}})] \\
& \text{SPLIT}(\mathbf{F}, \mathbf{f}_1, \mathbf{f}_2, \mathbf{v}^{[\varphi](\mathbf{A}+\mathbf{B})}) = (\text{split } \mathbf{F} \ \mathbf{f}_1 \ \mathbf{f}_2 \ \mathbf{v})^{\text{FOLDPARTIAL}([\varphi] \text{APP}(\mathbf{F}, \mathbf{v}))}
\end{aligned}$$

- IND evaluates an induction by pattern-matching on the argument  $n$ ; if  $n$  is neutral, then the whole induction is neutral and so it gets annotated with its type. The partial and restriction type cases are handled analogously.

$$\begin{aligned}
& \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \mathbf{Z}) = \mathbf{c}_0 \\
& \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \mathbf{S} \ \mathbf{m}) = \text{APP}(\text{APP}(\mathbf{c}_s, \mathbf{m}), \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \mathbf{m})) \\
& \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \mathbf{n}^{\mathbf{N}}) = \text{SIMPLIFY-NV}((\text{ind } \mathbf{F} \ \mathbf{c}_0 \ \mathbf{c}_s \ \mathbf{n})^{\text{APP}(\mathbf{F}, \mathbf{n})}) \\
& \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \mathbf{n}^{[\vec{\psi} \mapsto \vec{\mathbf{m}}] \mathbf{N}}) = \text{SIMPLIFY-NV}((\text{ind } \mathbf{F} \ \mathbf{c}_0 \ \mathbf{c}_s \ \mathbf{n})^{\mathbf{v}}) \\
& \quad (\text{where } \mathbf{v} = \text{FOLDRESTR}([\vec{\psi} \mapsto \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \vec{\mathbf{m}})] \text{APP}(\mathbf{F}, \mathbf{n}))) \\
& \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, [\vec{\psi} \mapsto \vec{\mathbf{n}}]) = [\vec{\psi} \mapsto \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \vec{\mathbf{n}})] \\
& \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \mathbf{n}^{[\varphi] \mathbf{N}}) = \text{IND}(\mathbf{F}, \mathbf{c}_0, \mathbf{c}_s, \mathbf{n})^{\text{FOLDPARTIAL}([\varphi] \text{APP}(\mathbf{F}, \mathbf{n}))}
\end{aligned}$$

- COMP is more complex than the previous helpers:<sup>51</sup> the main problem with evaluating composition is that one must do pattern matching on the type family  $F$ , which is inside an  $\mathbb{I}$ -abstraction, and that means that one must first introduce a fresh variable  $v : \mathbb{I}$ , evaluate  $F \ v$  and then pattern match; to call COMP recursively, one must then read-back to get the new type family. This naive approach is inefficient because of this problem, but an efficient implementation has still to be engineered. Reporting the actual working of COMP would complicate a lot the notation, hence we now give the rules for the various type formers only in an informal way (i.e. only syntactical). We refer to chapter 3, section 3.4, for the actual implementation. As already said, the definition is by structural induction of the type former  $F$  inside the  $\mathbb{I}$ -abstraction, i.e.  $[v : \mathbb{I}] F$ .<sup>52</sup> If the type family is a neutral value, as usual the whole composition becomes neutral, annotated with its type. We denote with  $t(x/y)$  the simultaneous substitution of all the free occurrences of  $x$  in  $t$  by  $y$ .

- $F \equiv [x : A] B$  (with  $A \neq \mathbb{I}$ ). Given  $b : [\varphi \mapsto u \ i_0][x : A(v/i_0)] B(v/i_0)$ , the result of the composition shall be the function

$$A(v/i) \rightarrow [i = i_0 \mapsto b, \varphi \mapsto u \ i_0] B(x/y_i, v/i)$$

<sup>51</sup>COMP is also conceptually different from the others, as it is not a type eliminator.

<sup>52</sup>The definitions for  $\Pi$ ,  $\Sigma$  and  $\mathbf{N}$  formers are as in [CCHM15]; the others have been found by the author while working on the implementation.

$$y_i \mapsto \text{comp} ([v : I]B(x/\tilde{y})) \varphi i_0 u' (b \tilde{y}_0) i$$

where

$$\begin{aligned}\tilde{y}_0 &\equiv \text{comp} ([v : \mathbb{I}]A) (\text{False}) i (\mathbb{I} \rightarrow []) y_i i_0 \\ \tilde{y} &\equiv \text{comp} ([v : \mathbb{I}]A) (\text{False}) i (\mathbb{I} \rightarrow []) y_i v\end{aligned}$$

$u'$  is obtained by applying the functions to  $\tilde{y}$  inside the abstraction.<sup>53</sup> Note that what we do is first transporting  $y_i$  to get  $\tilde{y}_0$  (the other end at  $i_0$ ) and the whole filler  $\tilde{y}$ , so that we obtain a value  $b \tilde{y}_0$  in  $B(v/i_0)$  and we can do transport in  $B$ .

- $F \equiv [x : \mathbb{I}]B$ . Given  $b : [\varphi \mapsto u i_0][x : \mathbb{I}]B(v/i_0)$ , the result of the composition shall be the function

$$\begin{aligned}\mathbb{I} &\rightarrow [i = i_0 \mapsto b, \varphi \mapsto u i_0]B(v/i) \\ x &\mapsto \text{comp} ([v : \mathbb{I}]B) \varphi i_0 u' (b x) i\end{aligned}$$

$u'$  is obtained by applying the functions to  $x$  inside the abstraction.

- $F \equiv \langle x : A \rangle B$ . Given  $b : [\varphi \mapsto u i_0]\langle x : A(v/i_0) \rangle B(v/i_0)$ , the result of composition shall be a pair  $(c_1, c_2)$ , i.e. composition is done component-wise. We put:

$$\text{comp} ([v : \mathbb{I}]\langle x : A \rangle B) \varphi i_0 u b i \equiv (c_0, c_1)$$

with

$$\begin{aligned}c_1 &\equiv \text{comp} ([v : \mathbb{I}]A) \varphi i_0 u_1 (b.1) i \\ \tilde{c}_1 &\equiv \text{comp} ([v : \mathbb{I}]A) \varphi i_0 u_1 (b.1) v \\ c_2 &\equiv \text{comp} ([v : \mathbb{I}]B(x/\tilde{c}_1)) \varphi i_0 u_2 (b.2) i\end{aligned}$$

$u_1$  and  $u_2$  are obtained from  $u$  by applying the projections inside the abstraction.

- $F \equiv A + B$ . Given  $b : [\varphi \mapsto u i_0](A(v/i_0) + B(v/i_0))$ , the composition is done ‘inside the injection’ if the value is not neutral, otherwise the whole composition becomes neutral.

$$\begin{aligned}\text{comp} ([v : \mathbb{I}]A + B) \varphi i_0 u (\text{inl } b) i &\equiv \text{inl } (\text{comp} ([v : \mathbb{I}]A) \varphi i_0 u' b i) \\ \text{comp} ([v : \mathbb{I}]A + B) \varphi i_0 u (\text{inr } b) i &\equiv \text{inr } (\text{comp} ([v : \mathbb{I}]B) \varphi i_0 u'' b i)\end{aligned}$$

$u'$  and  $u''$  are obtained from  $u$  by removing respectively the left and right outermost injection inside the abstraction.<sup>54</sup>

<sup>53</sup>In other words,  $u' \equiv [x : \mathbb{I}] u x \tilde{y}$ .

<sup>54</sup>If the base point is of the form  $\text{inl } b$ , then the body of  $u$  shall be a system of the form  $[\vec{\psi} \mapsto \text{inl } \vec{v}]$ , due to type-checking. Similarly for  $\text{inr}$ .

- $F \equiv \mathbb{N}$ . Given  $b : [\varphi \mapsto u \ i_0] \mathbb{N}$ , the composition is done by induction if the value is not neutral, otherwise the whole composition becomes neutral.

$$\begin{aligned} \text{comp } (\mathbb{I} \rightarrow \mathbb{N}) \ \varphi \ i_0 \ u \ Z \ i &\equiv Z \\ \text{comp } (\mathbb{I} \rightarrow \mathbb{N}) \ \varphi \ i_0 \ u \ (\mathbf{S} \ b) \ i &\equiv \mathbf{S} \ (\text{comp } (\mathbb{I} \rightarrow \mathbb{N}) \ \varphi \ i_0 \ u' \ b \ i) \end{aligned}$$

$u'$  is obtained from  $u$  by removing the left-most  $\mathbf{S}$  inside the abstraction.<sup>55</sup>

- $F \equiv [\vec{\psi}]A$  (with  $i \notin \text{vars}(\vec{\psi})$ ). The constraint on the formula requires some explanation: if we allowed  $i \in \text{vars}(\vec{\psi})$ , then by considering the family  $F \equiv [i = 0] \mathbb{N}$ , we could transport  $Z$  from  $F(i/0) \equiv \mathbb{N}$  to  $F(i/1) \equiv \perp$ , which is inconsistent.<sup>56</sup>

We define the composition as a system, doing a composition under each conjunction of the formula.

$$\begin{aligned} &\text{comp } ([v : \mathbb{I}][\vec{\psi}]A) \ \varphi \ i_0 \ u \ b \ i \\ &\equiv [\vec{\psi} \mapsto \text{comp } ([v : \mathbb{I}] A) \ \varphi \ i_0 \ u \ b \ i] \end{aligned}$$

- $F \equiv [\vec{\psi} \mapsto \vec{w}]A$  (with  $i \notin \text{vars}(\vec{\psi})$ ). As the case of partial types, the constraint on the formula is necessary:<sup>57</sup> if we allowed  $i \in \text{vars}(\vec{\psi})$ , then by considering the family  $F \equiv [i = 1 \wedge j = 0 \mapsto \text{true}, i = 1 \wedge j = 1 \mapsto \text{false}] \text{bool}$ , we could transport  $\text{true}$  from  $F(i/0) \equiv [] \text{bool} \equiv \text{bool}$ <sup>58</sup> to  $F(i/1) \equiv [j = 0 \mapsto \text{true}, j = 1 \mapsto \text{false}] \text{bool} \equiv \perp$ ,<sup>59</sup> which is

<sup>55</sup> $u$  has to be of that form, for the same reason explained for coproducts.

<sup>56</sup>With  $\perp$  or **empty** we denote the empty type. The transport function **transp** has type  $[F : \mathbb{I} \rightarrow \mathbb{U}] F \ 0 \rightarrow F \ 1$ , defined by  $[F : \mathbb{I} \rightarrow \mathbb{U}][a : F \ 0] \text{comp } F \ (\text{False}) \ 0 \ (\mathbb{I} \rightarrow []) \ a \ 1$ , i.e. composition in a trivial (1-dimensional) hypercube.

<sup>57</sup>Note that the check on the variable should be done during type-checking, but this is not at all trivial to do; it is not sufficient to check it just when type-checking a **comp** expression: suppose that **transp** is defined as in the footnote 56; then when type-checking **transp**  $([i : \mathbb{I}][i = 0] \mathbb{N}) \ Z$ , the program only checks that  $([i : \mathbb{I}][i = 0] \mathbb{N})$  has type  $\mathbb{I} \rightarrow \mathbb{U}$ , as required by the type of **transp**, which is true. This problem is not present in the theory of [CCHM15], as there all types are *fibrant*, i.e. admit a composition operation. Since composition is only experimental in this thesis, we have not addressed this problem, which could be a direction for future work (along with the implementation of composition for the universe).

<sup>58</sup>Do not confuse  $[] \text{bool}$ , which is a restriction type with no constraints, with the partial type with a false formula, which is equivalent to the empty type.

<sup>59</sup>This is the empty type because of disjointness of constructors. It can be proved for coproducts (for us, **bool** is **unit** + **unit**) as explained in [Uni13] 2.12, with small changes (some equalities that are judgmental in HOTT need to be proved as propositional in CTT, due to the fact that path types do not satisfy the computation rule for path induction judgmentally). See the appendix C for the proof using our implementation.



inconsistent. If the constraint is fulfilled, we put:

$$\begin{aligned} & \text{comp} ([v : \mathbb{I}] [\vec{\psi} \mapsto \vec{w}] A) \varphi i_0 u b i \\ & \equiv \text{comp} ([v : \mathbb{I}] A) (\varphi \vee \vec{\psi}) i_0 [j : \mathbb{I}] [\varphi \mapsto u j, \vec{\psi} \mapsto \vec{w}(v/j)] b i \end{aligned}$$

with  $j$  a fresh variable.

Using the above computational rules for composition one may easily derive the rule for path types as given in [CCHM15], i.e.

$$\begin{aligned} & \text{comp} ([v : \mathbb{I}] \text{Path } A w_1 w_2) \varphi i_0 u p_0 i \\ & \equiv [x : \mathbb{I}] \text{comp} ([v : \mathbb{I}] A) (\varphi \vee x = 0 \vee x = 1) i_0 \\ & \quad [j : \mathbb{I}] [\varphi \mapsto u j, x = 0 \mapsto w_1(v/j), x = 1 \mapsto w_2(v/j)] (p_0 x) i \end{aligned}$$

with  $x$  and  $j$  fresh variables.

### Reading back

We now extend straightforwardly the read-back function  $\mathcal{R}$  introduced in section 1.1.4 to handle the new syntactical constructs.

$$\begin{aligned} \mathcal{R}_{ns}(\mathbb{I}) &= \mathbb{I} \\ \mathcal{R}_{ns}(0) &= 0 \\ \mathcal{R}_{ns}(1) &= 1 \\ \mathcal{R}_{ns}([\vec{\psi} \mapsto \vec{M}]) &= [\vec{\psi} \mapsto \mathcal{R}_{ns}(\vec{M})] \\ \mathcal{R}_{ns}([\varphi] A) &= \text{FOLDPARTIAL}([\varphi] \mathcal{R}_{ns}(A)) \\ \mathcal{R}_{ns}([\vec{\psi} \mapsto \vec{M}] A) &= \text{FOLDRESTR}([\vec{\psi} \mapsto \mathcal{R}_{ns}(\vec{M})] \mathcal{R}_{ns}(A)) \\ \mathcal{R}_{ns}(\text{comp } F \varphi i_0 u b i) &= \text{comp } \mathcal{R}_{ns}(F) \varphi \mathcal{R}_{ns}(i_0) \mathcal{R}_{ns}(u) \mathcal{R}_{ns}(b) \mathcal{R}_{ns}(i) \end{aligned}$$

## 1.5 $\alpha\eta$ -conversion

The function  $\cdot \sim_{ns}^\Theta \cdot$  tests  $\alpha$ - and  $\eta$ -conversion between two values,<sup>60</sup> given a directions environment  $\Theta$ ; it keeps track of the list of already used names, to avoid conflicts when reading back closures. The rules assume that the two values being tested have the same type, which means that conversion may be tested between two values only after type-checking.

<sup>60</sup>It is natural to implement conversion for values and not for terms, because values, unlike terms, are in a canonical (i.e.  $\beta$ -) normal form.

There is one point which requires special attention: even if values are in canonical form (that's the point of evaluation), it may happen that in systems  $[\psi_1 \mapsto \mathbf{v}_1, \dots, \psi_n \mapsto \mathbf{v}_n]$  and neutral values of the form  $\mathbf{k}^{\mathbf{A}[\psi_1 \mapsto \mathbf{v}_1, \dots, \psi_n \mapsto \mathbf{v}_n]}$ , one of the formulas  $\psi_i$  becomes true under **dirs**, so that they shall be reduced to  $\mathbf{v}_i$ .

### Non-neutral values

$$\overline{U \sim_{ns}^\Theta U}$$

$$\frac{(ty)_\Gamma \sim_{ns}^\Theta (ty')_{\Gamma'} \quad (e)_{\Gamma, x \mapsto v^{(ty)_\Gamma}} \sim_{ns, v}^\Theta (e')_{\Gamma', y \mapsto v^{(ty')_{\Gamma'}}}}{\text{closure}([x : ty]e, \Gamma) \sim_{ns}^\Theta \text{closure}([y : ty']e', \Gamma')} \quad (v = \text{NEWVAR}(ns))$$

$$\frac{(e)_{\Gamma, x \mapsto v^{(ty)_\Gamma}} \sim_{ns, v}^\Theta \text{APP}(\mathbf{v}_2, v^{(ty)_\Gamma})}{\text{closure}([x : ty]e, \Gamma) \sim_{ns}^\Theta \mathbf{v}_2} \quad (v = \text{NEWVAR}(ns))$$

$$\frac{\text{APP}(\mathbf{v}_1, v^{(ty)_\Gamma}) \sim_{ns, v}^\Theta (e)_{\Gamma, x \mapsto v^{(ty)_\Gamma}}}{\mathbf{v}_1 \sim_{ns}^\Theta \text{closure}([x : ty]e, \Gamma)} \quad (v = \text{NEWVAR}(ns))$$

$$\frac{(ty)_\Gamma \sim_{ns}^\Theta (ty')_{\Gamma'} \quad (e)_{\Gamma, x \mapsto v^{(ty)_\Gamma}} \sim_{ns, v}^\Theta (e')_{\Gamma', y \mapsto v^{(ty')_{\Gamma'}}}}{\text{closure}(\langle x : ty \rangle e, \Gamma) \sim_{ns}^\Theta \text{closure}(\langle y : ty' \rangle e', \Gamma')} \quad (v = \text{NEWVAR}(ns))$$

$$\frac{s \sim_{ns}^\Theta t}{s.1 \sim_{ns}^\Theta t.1}$$

$$\frac{s \sim_{ns}^\Theta t}{s.2 \sim_{ns}^\Theta t.2}$$

$$\frac{s \sim_{ns}^\Theta s' \quad t \sim_{ns}^\Theta t'}{(s, t) \sim_{ns}^\Theta (s', t')}$$

$$\frac{\text{FST}(\mathbf{v}) \sim_{ns}^{\Theta} \mathbf{s} \quad \text{SND}(\mathbf{v}) \sim_{ns}^{\Theta} \mathbf{t}}{\mathbf{v} \sim_{ns}^{\Theta} (\mathbf{s}, \mathbf{t})}$$

$$\frac{\mathbf{s} \sim_{ns}^{\Theta} \text{FST}(\mathbf{v}) \quad \mathbf{t} \sim_{ns}^{\Theta} \text{SND}(\mathbf{v})}{(\mathbf{s}, \mathbf{t}) \sim_{ns}^{\Theta} \mathbf{v}}$$

$$\frac{\mathbf{A} \sim_{ns}^{\Theta} \mathbf{A}' \quad \mathbf{B} \sim_{ns}^{\Theta} \mathbf{B}'}{\mathbf{A} + \mathbf{B} \sim_{ns}^{\Theta} \mathbf{A}' + \mathbf{B}'}$$

$$\frac{\mathbf{v} \sim_{ns}^{\Theta} \mathbf{v}'}{\text{inl } \mathbf{v} \sim_{ns}^{\Theta} \text{inl } \mathbf{v}'}$$

$$\frac{\mathbf{v} \sim_{ns}^{\Theta} \mathbf{v}'}{\text{inr } \mathbf{v} \sim_{ns}^{\Theta} \text{inr } \mathbf{v}'}$$

$$\overline{\mathbf{N} \sim_{ns}^{\Theta} \mathbf{N}} \quad \overline{\mathbf{Z} \sim_{ns}^{\Theta} \mathbf{Z}} \quad \overline{\mathbf{S} \mathbf{n} \sim_{ns}^{\Theta} \mathbf{S} \mathbf{n}'}$$

$$\overline{\mathbb{I} \sim_{ns}^{\Theta} \mathbb{I}} \quad \overline{0 \sim_{ns}^{\Theta} 0} \quad \overline{1 \sim_{ns}^{\Theta} 1}$$

$$\frac{\psi_i \sim^{\Theta} \text{True} \quad \mathbf{t}_i \sim_{ns}^{\Theta} \mathbf{v}}{[\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n] \sim_{ns}^{\Theta} \mathbf{v}} \quad \frac{\psi_i \sim^{\Theta} \text{True} \quad \mathbf{v} \sim_{ns}^{\Theta} \mathbf{t}_i}{\mathbf{v} \sim_{ns}^{\Theta} [\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n]}$$

$$\frac{(\psi_1 \vee \dots \vee \psi_n) \sim^{\Theta} (\psi'_1 \vee \dots \vee \psi'_n) \quad \mathbf{t}_i \sim_{ns}^{\Theta, \psi_i \wedge \psi'_j} \mathbf{t}'_j}{[\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n] \sim_{ns}^{\Theta} [\psi'_1 \mapsto \mathbf{t}'_1, \dots, \psi'_m \mapsto \mathbf{t}'_m]} \quad (1 \leq i \leq n, 1 \leq j \leq m)^{61}$$

$$\frac{\varphi \sim^{\Theta} \varphi' \quad \mathbf{A} \sim_{ns}^{\Theta} \mathbf{A}'}{[\varphi] \mathbf{A} \sim_{ns}^{\Theta} [\varphi'] \mathbf{A}'}$$

<sup>61</sup>With  $(1 \leq i \leq n, 1 \leq j \leq m)$  we mean that the assumptions must hold for any such  $i$  and  $j$ .

$$\frac{[\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n] \sim_{ns}^\Theta [\psi'_1 \mapsto \mathbf{t}'_1, \dots, \psi'_m \mapsto \mathbf{t}'_m] \quad \mathbf{A} \sim_{ns}^\Theta \mathbf{A}'}{[\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n] \mathbf{A} \sim_{ns}^\Theta [\psi'_1 \mapsto \mathbf{t}'_1, \dots, \psi'_m \mapsto \mathbf{t}'_m] \mathbf{A}'}$$

Neutral values

$$\overline{\mathbf{x} \sim_{ns}^\Theta \mathbf{x}}$$

$$\frac{(x = y) \sim^\Theta \text{True}}{\mathbf{x}^\mathbb{I} \sim_{ns}^\Theta \mathbf{y}^\mathbb{I}} \quad \frac{(x = 0) \sim^\Theta \text{True}}{\mathbf{x}^\mathbb{I} \sim_{ns}^\Theta 0} \quad \frac{(x = 1) \sim^\Theta \text{True}}{\mathbf{x}^\mathbb{I} \sim_{ns}^\Theta 1} \quad \frac{(x = 0) \sim^\Theta \text{True}}{0 \sim_{ns}^\Theta \mathbf{x}^\mathbb{I}} \quad \frac{(x = 1) \sim^\Theta \text{True}}{1 \sim_{ns}^\Theta \mathbf{x}^\mathbb{I}}$$

$$\frac{\mathbf{f} \sim_{ns}^\Theta \mathbf{f}' \quad \mathbf{a} \sim_{ns}^\Theta \mathbf{a}'}{\mathbf{f} \mathbf{a} \sim_{ns}^\Theta \mathbf{f}' \mathbf{a}'}$$

$$\frac{\mathbf{F} \sim_{ns}^\Theta \mathbf{F}' \quad \mathbf{c}_0 \sim_{ns}^\Theta \mathbf{c}'_0 \quad \mathbf{c}_s \sim_{ns}^\Theta \mathbf{c}'_s \quad \mathbf{n} \sim_{ns}^\Theta \mathbf{n}'}{\text{ind } \mathbf{F} \mathbf{c}_0 \mathbf{c}_s \mathbf{n} \sim_{ns}^\Theta \text{ind } \mathbf{F}' \mathbf{c}'_0 \mathbf{c}'_s \mathbf{n}'}$$

$$\frac{\text{ty} \sim_{ns}^\Theta \text{ty}' \quad \mathbf{f}_1 \sim_{ns}^\Theta \mathbf{f}'_1 \quad \mathbf{f}_2 \sim_{ns}^\Theta \mathbf{f}'_2 \quad \mathbf{x} \sim_{ns}^\Theta \mathbf{x}'}{\text{split ty } \mathbf{f}_1 \mathbf{f}_2 \mathbf{x} \sim_{ns}^\Theta \text{split ty}' \mathbf{f}'_1 \mathbf{f}'_2 \mathbf{x}'}$$

$$\frac{\mathbf{F} \sim_{ns}^\Theta \mathbf{F}' \quad \varphi \sim^\Theta \varphi' \quad \mathbf{i}_0 \sim_{ns}^\Theta \mathbf{i}'_0 \quad \mathbf{u} \sim_{ns}^\Theta \mathbf{u}' \quad \mathbf{b} \sim_{ns}^\Theta \mathbf{b}' \quad \mathbf{i} \sim_{ns}^\Theta \mathbf{i}'}{\text{comp } \mathbf{F} \varphi \mathbf{i}_0 \mathbf{u} \mathbf{b} \mathbf{i} \sim_{ns}^\Theta \text{comp } \mathbf{F}' \varphi' \mathbf{i}'_0 \mathbf{u}' \mathbf{b}' \mathbf{i}'}$$

$$\frac{\psi_i \sim^\Theta \text{True} \quad \mathbf{t}_i \sim_{ns}^\Theta \mathbf{v}}{\mathbf{k}^{[\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n]} \mathbf{A} \sim_{ns}^\Theta \mathbf{v}} \quad \frac{\psi_i \sim^\Theta \text{True} \quad \mathbf{v} \sim_{ns}^\Theta \mathbf{t}_i}{\mathbf{v} \sim_{ns}^\Theta \mathbf{k}^{[\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n]} \mathbf{A}}$$

$$\frac{\psi_i \not\sim^\Theta \text{True} \quad \psi'_j \not\sim^\Theta \text{True} \quad \mathbf{k} \sim_{ns}^\Theta \mathbf{k}' \quad (1 \leq i \leq n)}{\mathbf{k}^{[\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n]} \mathbf{A} \sim_{ns}^\Theta \mathbf{k}'^{[\psi'_1 \mapsto \mathbf{t}'_1, \dots, \psi'_m \mapsto \mathbf{t}'_m]} \mathbf{A}' \quad (1 \leq j \leq m)}$$

$$\frac{\text{PROFIRRELEVANT}_\Theta(\mathbf{A})}{\mathbf{k}^{\mathbf{A}} \sim_{ns}^\Theta \mathbf{k}'^{\mathbf{A}'}}$$

### Proof irrelevance

When two values have a type that can be simplified (i.e. a restriction type with a true formula), then both values shall reduce to the same value and so they are  $\alpha\eta$ -equivalent.<sup>62</sup> We generalize this by introducing a predicate called `PROFIRRELEVANT`: when we test  $\alpha\eta$ -equivalence between two neutral values, if their type is proof irrelevant it means that they shall reduce to the same value, and so they are automatically convertible (from this comes the name ‘proof irrelevance’, since we don’t have to look inside the value/proof).

$$\frac{\psi_i \sim^\Theta \text{True}}{\text{PROFIRRELEVANT}([\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n] \mathbf{A})}$$

$$\frac{\text{PROFIRRELEVANT}(\mathbf{A})}{\text{PROFIRRELEVANT}([\psi_1 \mapsto \mathbf{t}_1, \dots, \psi_n \mapsto \mathbf{t}_n] \mathbf{A})}$$

$$\frac{\text{PROFIRRELEVANT}((e)_{\Gamma, x \mapsto v(ty)_\Gamma})}{\text{PROFIRRELEVANT}(\text{closure}([x : ty]e, \Gamma))} \quad (v = \text{NEWVAR}(\Gamma))$$

$$\frac{\text{PROFIRRELEVANT}((ty)_\Gamma) \quad \text{PROFIRRELEVANT}((e)_{\Gamma, x \mapsto v(ty)_\Gamma})}{\text{PROFIRRELEVANT}(\text{closure}([x : ty]e, \Gamma))} \quad (v = \text{NEWVAR}(\Gamma))$$

## 1.6 Metatheoretical results

We now extend the results given for the basic type theory in section 1.1.5, handling the cubical constructs. As in the simpler theory, for the theoretical study we use an infinite hierarchy of cumulative universes instead of a single (inconsistent) universe, and we forget about the composition operation, i.e. we augment the basic type theory only with the interval, formulas, systems, partial and restriction types. This type theory is very similar the one described in [GSA<sup>+</sup>22], except for the lack of explicit partial types, and we think that the normalization result proved there could be easily adapted to our theory.

**Claim 1** (Strong normalization).

*Every term reduces to an unique normal term.*

<sup>62</sup>This works because when we test  $\alpha\eta$ -equivalence, the two values being tested are assumed to have the same type.

Strong normalization implies the following results, albeit they are clear from the given implementation.

**Theorem 4** (Decidability of  $\alpha\eta$ -conversion).

*For any two terms of the same type, it is decidable whether they are  $\alpha\eta$ -equivalent or not.*

**Theorem 5** (Decidability of type-checking).

*Given a context  $\Gamma$  and terms  $a$  and  $A$ , it is decidable whether  $\Gamma \vdash a \Leftarrow A$ .*

As for the basic type theory, the canonicity property shall hold (i.e. that functions  $\mathbb{N} \rightarrow \mathbb{N}$ , when applied to a numeral, reduce to a numeral in a computable way), which is particularly interesting for the full cubical type theory (i.e. extended with the composition operation for all types), so that a constructive justification of the univalence axiom is given. Canonicity for the usual presentation of cubical type theory, that is without explicit partial and restriction type, is given in [Hub16].

## 1.7 Examples

We can now show some examples exploiting the full theory developed so far.

### 1.7.1 Equivalence of two product types

First of all, we show how to model the unit type, as promised in section 1.1.6. For the unit type we choose  $[\mathbf{True} \mapsto \mathbb{Z}]\mathbb{N}$ , i.e. the subtype of naturals which ‘contain’ only  $\mathbb{Z}$ . As we don’t have a constant  $\mathbf{True}$  in the syntax, we introduce a dummy variable  $\_i$  which we don’t use anywhere else, so that  $\mathbf{True}$  can be replaced by  $\_i = \_i$ .<sup>63</sup> The induction principle is then trivial to prove: if  $x : \mathbf{unit}$ , then  $x$  is convertible to  $\mathbb{Z}$  and so  $C \mathbf{tt}$  is convertible to  $C x$ , which is the type of  $p$ . We also prove by induction the propositional uniqueness principle for  $\mathbf{unit}$ .

$$\begin{aligned} \_i &: \mathbb{I} \\ \mathbf{unit} : \mathbb{U} &= [\_i = \_i \rightarrow \mathbb{Z}]\mathbb{N} \\ \mathbf{tt} : \mathbf{unit} &= \mathbb{Z} \\ \mathbf{unitInd} : [C : \mathbf{unit} \rightarrow \mathbb{U}] \ C \ \mathbf{tt} &\rightarrow [x : \mathbf{unit}] \ C \ x \\ &= [C : \mathbf{unit} \rightarrow \mathbb{U}] [p : C \ \mathbf{tt}] [x : \mathbf{unit}] \ p \\ \mathbf{unitEq} : [x : \mathbf{unit}] \ \mathbf{Path} \ \mathbf{unit} \ \mathbf{tt} \ x & \end{aligned}$$

<sup>63</sup>We chose not to add the constant  $\mathbf{True}$  to the language, as it would be useful only in this case, and it would complicate the implementation.

$$= [x : \text{unit}] \text{unitInd } ([y : \text{unit}] \text{Path unit tt } y) (\text{refl unit tt}) x$$

As remarked in the introduction, we can prove function extensionality, even in the dependent case.

$$\begin{aligned} \text{funext} &: [A, B : \mathbb{U}] [f, g : A \rightarrow B] \\ &\quad ([x : A] \text{Path } B (f x) (g x)) \rightarrow \text{Path } (A \rightarrow B) f g \\ &= [A, B : \mathbb{U}] [f, g : A \rightarrow B] [p : [x : A] \text{Path } B (f x) (g x)] \\ &\quad [i : \mathbb{I}] [x : A] (p x i) \end{aligned}$$

$$\begin{aligned} \text{dfunext} &: [A : \mathbb{U}] [B : A \rightarrow \mathbb{U}] [f, g : [x : A] B x] \\ &\quad ([x : A] \text{Path } (B x) (f x) (g x)) \rightarrow \text{Path } ([x : A] B x) f g \\ &= [A : \mathbb{U}] [B : A \rightarrow \mathbb{U}] [f, g : [x : A] B x] \\ &\quad [p : [x : A] \text{Path } (B x) (f x) (g x)] [i : \mathbb{I}] [x : A] (p x i) \end{aligned}$$

The first use of composition is in proving *transport*,<sup>64</sup> which can be thought as the case of extension in a 1-cube, i.e. a structure with only two points. We first derive the function **transp**, which is very general, and then we use it to define transport in the usual formulation.

$$\begin{aligned} \text{transp} &: [F : \mathbb{I} \rightarrow \mathbb{U}] F 0 \rightarrow F 1 \\ &= [F : \mathbb{I} \rightarrow \mathbb{U}] [a : F 0] \text{comp } F () 0 (\mathbb{I} \rightarrow []) a 1 \end{aligned}$$

$$\begin{aligned} \text{transport} &: [B : \mathbb{U}] [P : B \rightarrow \mathbb{U}] [x, y : B] \text{Path } B x y \rightarrow P x \rightarrow P y \\ &= [B : \mathbb{U}] [P : B \rightarrow \mathbb{U}] [x, y : B] [pB : \text{Path } B x y] \\ &\quad [u : P x] \text{transp } ([i : \mathbb{I}] P (pB i)) u \end{aligned}$$

Using (dependent) function extensionality, we can prove the propositional  $\eta$ -law and the induction/elimination principle for **prod** types (introduced in section 1.1.6).

$$\begin{aligned} \text{prodEta} &: [A, B : \mathbb{U}] [p : \text{prod } A B] \text{Path } (\text{prod } A B) \\ &\quad (\text{couple } A B (\text{pi1 } A B p) (\text{pi2 } A B p)) p \\ &= [A, B : \mathbb{U}] [p : \text{prod } A B] \text{dfunext bool } ([x : \text{bool}] \text{boolRec U } A B x) \\ &\quad (\text{couple } A B (\text{pi1 } A B p) (\text{pi2 } A B p)) p \\ &\quad (\text{boolInd } ([y : \text{bool}] \text{Path } (\text{boolRec U } A B y) \\ &\quad (\text{couple } A B (\text{pi1 } A B p) (\text{pi2 } A B p) y) (p y)) \\ &\quad (\text{refl } A (p \text{ false})) (\text{refl } B (p \text{ true}))) \end{aligned}$$

$$\begin{aligned}
\text{prodInd} &: [A, B : \mathbb{U}] [C : \text{prod } A \ B \rightarrow \mathbb{U}] \\
&\quad ([a : A][b : B] \ C \ (\text{couple } A \ B \ a \ b)) \rightarrow [p : \text{prod } A \ B] \ C \ p \\
&= [A, B : \mathbb{U}] [C : \text{prod } A \ B \rightarrow \mathbb{U}] [f : [a : A][b : B] \ C \ (\text{couple } A \ B \ a \ b)] \\
&= [p : \text{prod } A \ B] \ \text{transport} \ (\text{prod } A \ B) \ C \\
&\quad (\text{couple } A \ B \ (\text{pi1 } A \ B \ p) \ (\text{pi2 } A \ B \ p)) \ p \ (\text{prodEta } A \ B \ p) \\
&\quad (f \ (\text{pi1 } A \ B \ p) (\text{pi2 } A \ B \ p))
\end{aligned}$$

We now want to prove that the built-in product type  $A * B$  and the derived one  $\text{prod } A \ B$  are equivalent, in the sense of [Uni13] 2.4. First we give the basic definitions.

$$\text{id} : [A : \mathbb{U}] \ A \rightarrow A = [A : \mathbb{U}] [x : A] \ x$$

$$\begin{aligned}
\text{fcomp} &: [A, B, C : \mathbb{U}] [f : B \rightarrow C] [g : A \rightarrow B] \ A \rightarrow C \\
&= [A, B, C : \mathbb{U}] [f : B \rightarrow C] [g : A \rightarrow B] [a : A] \ f \ (g \ a)
\end{aligned}$$

$$\begin{aligned}
\text{isEquiv} &: [A, B : \mathbb{U}] \ (A \rightarrow B) \rightarrow \mathbb{U} \\
&= [A, B : \mathbb{U}] [f : A \rightarrow B] \\
&\quad (\langle g : B \rightarrow A \rangle \ \text{Path} \ (B \rightarrow B) \ (\text{fcomp } B \ A \ B \ f \ g) \ (\text{id } B)) \\
&\quad * \ (\langle h : B \rightarrow A \rangle \ \text{Path} \ (A \rightarrow A) \ (\text{fcomp } A \ B \ A \ h \ f) \ (\text{id } A))
\end{aligned}$$

$$\text{equiv} : \mathbb{U} \rightarrow \mathbb{U} \rightarrow \mathbb{U} = [A, B : \mathbb{U}] \langle f : A \rightarrow B \rangle \ \text{isEquiv } A \ B \ f$$

Now we define two functions **to** and **from**, and then we prove that they are one the inverse of the other.

$$\begin{aligned}
\text{to} &: [A, B : \mathbb{U}] \ A * B \rightarrow \text{prod } A \ B \\
&= [A, B : \mathbb{U}] [p : A * B] \ \text{couple } A \ B \ (p.1) \ (p.2)
\end{aligned}$$

$$\begin{aligned}
\text{from} &: [A, B : \mathbb{U}] \ \text{prod } A \ B \rightarrow A * B \\
&= [A, B : \mathbb{U}] [p : \text{prod } A \ B] \ (\text{pi1 } A \ B \ p, \text{pi2 } A \ B \ p)
\end{aligned}$$

First we prove that applying **from** and then **to** is (propositionally) pointwise equal to the identity.

$$\begin{aligned}
\text{to\_from'} &: [A, B : \mathbb{U}] [p : \text{prod } A \ B] \ \text{Path} \ (\text{prod } A \ B) \ (\text{to } A \ B \ (\text{from } A \ B \ p)) \ p \\
&= [A, B : \mathbb{U}] \ \text{prodInd } A \ B
\end{aligned}$$



$$\begin{aligned}
& ([p' : \text{prod } A \ B] \text{ Path } (\text{prod } A \ B) (\text{to } A \ B (\text{from } A \ B \ p')) \ p') \\
& ([a : A][b : B] \text{ refl } (\text{prod } A \ B) (\text{couple } A \ B \ a \ b))
\end{aligned}$$

And then we use function extensionality to get half of what we need to prove the aforementioned equivalence.

$$\begin{aligned}
& \text{to\_from} : [A, B : \mathbb{U}] \text{ Path } (\text{prod } A \ B \rightarrow \text{prod } A \ B) \\
& \quad (\text{fcomp } (\text{prod } A \ B) (A * B) (\text{prod } A \ B) (\text{to } A \ B) (\text{from } A \ B)) \\
& \quad (\text{id } (\text{prod } A \ B)) \\
& = [A, B : \mathbb{U}] \text{ funext } (\text{prod } A \ B) (\text{prod } A \ B) \\
& \quad (\text{fcomp } (\text{prod } A \ B) (A * B) (\text{prod } A \ B) (\text{to } A \ B) (\text{from } A \ B)) \\
& \quad (\text{id } (\text{prod } A \ B)) (\text{to\_from}' \ A \ B)
\end{aligned}$$

Vice versa now we show that applying first **to** and then **from** is (propositionally) pointwise equal to the identity.

$$\begin{aligned}
& \text{from\_to}' : [A, B : \mathbb{U}][p : A * B] \text{ Path } (A * B) (\text{from } A \ B (\text{to } A \ B \ p)) \ p \\
& = [A, B : \mathbb{U}] \text{ recSigma } A \ B \\
& \quad ([p' : A * B] \text{ Path } (A * B) (\text{from } A \ B (\text{to } A \ B \ p')) \ p') \\
& \quad ([a : A][b : B] \text{ refl } (A * B) (a, b))
\end{aligned}$$

And then we can prove the other half of the equivalence.

$$\begin{aligned}
& \text{from\_to} : [A, B : \mathbb{U}] \text{ Path } (A * B \rightarrow A * B) \\
& \quad (\text{fcomp } (A * B) (\text{prod } A \ B) (A * B) (\text{from } A \ B) (\text{to } A \ B)) \\
& \quad (\text{id } (A * B)) \\
& = [A, B : \mathbb{U}] \text{ funext } (A * B) (A * B) \\
& \quad (\text{fcomp } (A * B) (\text{prod } A \ B) (A * B) (\text{from } A \ B) (\text{to } A \ B)) \\
& \quad (\text{id } (A * B)) (\text{from\_to}' \ A \ B)
\end{aligned}$$

Finally, using what we proved till now, we get the equivalence between the two product types.

$$\begin{aligned}
& \text{prodEquiv} : [A, B : \mathbb{U}] \text{ equiv } (A * B) (\text{prod } A \ B) \\
& = [A, B : \mathbb{U}] (\text{to } A \ B, \\
& \quad ((\text{from } A \ B, \text{to\_from } A \ B), (\text{from } A \ B, \text{from\_to } A \ B)))
\end{aligned}$$

---

<sup>64</sup>We follow the notation of [Uni13] 2.3.

### 1.7.2 Path operations

We have already defined transport and the concatenation operation of two paths (see section 1.7); we give now some more examples, following [Ben21], beginning with the path inversion operation, which we derive by composition.

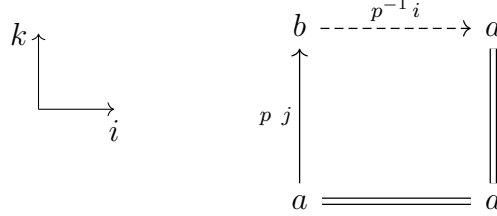


Figure 1.2: Inversion of a path,  $p \mapsto p^{-1}$ .

$$\begin{aligned}
 \text{inv} &: [A : \mathbb{U}][a, b : A] \text{ Path } A \ a \ b \rightarrow \text{Path } A \ b \ a \\
 &= [A : \mathbb{U}][a, b : A][p : \text{Path } A \ a \ b][i : \mathbb{I}] \\
 &\quad \text{comp } (\mathbb{I} \rightarrow A) \ (i = 0 \wedge i = 1) \ 0 \ ([j : \mathbb{I}][i = 0 \rightarrow p \ j, i = 1 \rightarrow a]) \ a \ 1
 \end{aligned}$$

We shall now prove the right and left unit laws; the former is easier, since it is already given by the filler of the composition operation (when  $q \equiv \text{refl } A \ b$ ), which we basically already derived in section 1.2.2.

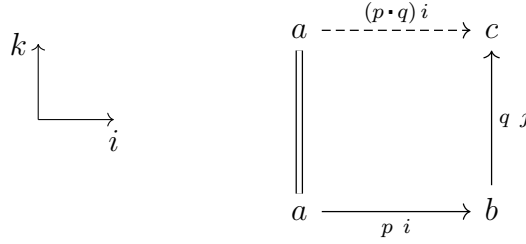


Figure 1.3: Concatenation of two paths.

$$\begin{aligned}
 \text{concatFill} &: [A : \mathbb{U}][a, b, c : A][p : \text{Path } A \ a \ b][q : \text{Path } A \ b \ c] \\
 &\quad [i, j : \mathbb{I}][j = 0 \mapsto p \ i, i = 0 \mapsto a, i = 1 \rightarrow q \ j] A
 \end{aligned}$$

$$\begin{aligned}
&= [A : \mathbb{U}][a, b, c : A][p : \text{Path } A \ a \ b][q : \text{Path } A \ b \ c][i, j : \mathbb{I}] \\
&\quad \text{comp } (\mathbb{I} \rightarrow A) \ (i = 0 \vee i = 1) \ 0 \\
&\quad ([j' : \mathbb{I}][i = 0 \mapsto a, i = 1 \mapsto q \ j']) \ (p \ i) \ j
\end{aligned}$$

Therefore to get `rightUnit` we only have to swap the dimensions and specialize  $q$  to `refl A b`.

$$\begin{aligned}
\text{rightUnit} &: [A : \mathbb{U}][a, b, c : A][p : \text{Path } A \ a \ b] \\
&\quad \text{Path } (\text{Path } A \ a \ b) \ p \ (\text{concat } A \ a \ b \ b \ p \ (\text{refl } A \ b)) \\
&= [A : \mathbb{U}][a, b, c : A][p : \text{Path } A \ a \ b][i, j : \mathbb{I}] \\
&\quad \text{concatFill } A \ a \ b \ b \ p \ (\text{refl } A \ b) \ j \ i
\end{aligned}$$

The derivation of the left unit law is more intricate; we shall first state a lemma, i.e. obtain the filler of a composition figure which we will need later. The idea is to mimic the meet connection of the interval which is built-in in De Morgan CTT but not in the Cartesian one,<sup>65</sup> that is we want a function  $p(- \vee -)$  given by the figure 1.4.

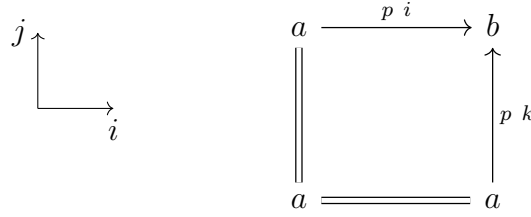
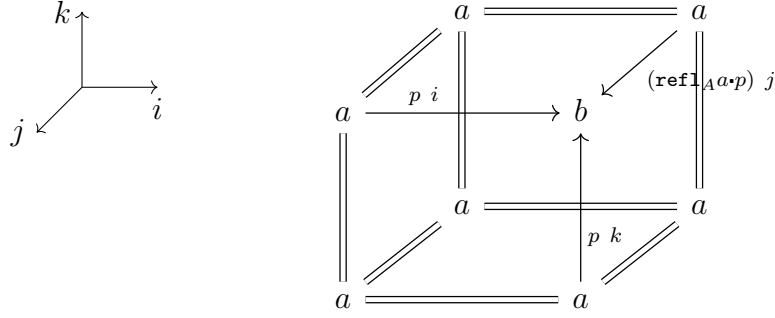


Figure 1.4: Weak meet.

We call it ‘weak meet’ because the computational rules hold only up to homotopy and not judgmentally. To derive it, we need a 2-dimensional composition, so we have to work on a 3-dimensional hypercube; putting the square we want to obtain on the  $j = 1$  face, we compose from  $j = 0$  to  $j = 1$ , defining all the other faces of the cube as reflexivity apart from the  $i = 1$  and  $k = 1$  faces which are given by the filler of `concat`, as one may check by comparing with the figure 1.3.

$$\text{weakMeet} : [A : \mathbb{U}][a, b : A][p : \text{Path } A \ a \ b][i, k : \mathbb{I}]$$

<sup>65</sup>The ‘De Morgan’ version of cubical type type [CCHM15], has also operations on the interval, called connections ( $\wedge, \vee : \mathbb{I} \rightarrow \mathbb{I} \rightarrow \mathbb{I}$ ) and reversal ( $: \mathbb{I} \rightarrow \mathbb{I}$ ); the ‘Cartesian’ version [ABC<sup>+</sup>21] does not include them, but has the diagonal constraints.

Figure 1.5: Composition for **weakMeet**.

$$\begin{aligned}
& [i = 0 \mapsto a, i = 1 \mapsto p \cdot k, k = 0 \mapsto a, k = 1 \mapsto p \cdot i] A \\
&= [A : \mathbb{U}][a, b : A][p : \text{Path } A \ a \ b][i, k : \mathbb{I}] \\
&\quad \text{comp } (\mathbb{I} \rightarrow A) \ (i = 0 \vee i = 1 \vee k = 0 \vee k = 1) \ 0 \\
&\quad ([j : \mathbb{I}][i = 0 \mapsto a, \\
&\quad \quad i = 1 \mapsto \text{concatFill } A \ a \ a \ b \ (\text{refl } A \ a) \ p \ j \ k, \\
&\quad \quad k = 0 \mapsto a, \\
&\quad \quad k = 1 \mapsto \text{concatFill } A \ a \ a \ b \ (\text{refl } A \ a) \ p \ j \ i]) \\
&\quad a \ 1
\end{aligned}$$

Note that the type of **weakMeet** can be seen as a *dependent path* between  $\text{refl } A \ a$  and  $p$ , as they both start at  $a$ , and their endpoint follows  $p \cdot i$ .

$$\begin{aligned}
&\text{PathD} : [A : \mathbb{I} \rightarrow \mathbb{U}] \ A \ 0 \rightarrow A \ 1 \rightarrow \mathbb{U} \\
&= [A : \mathbb{I} \rightarrow \mathbb{U}][a_0 : A \ 0][a_1 : A \ 1][i : \mathbb{I}][i = 0 \rightarrow a_0, i = 1 \rightarrow a_1] A \ i
\end{aligned}$$

$$\begin{aligned}
&\text{weakMeetDP} : [A : \mathbb{U}][a, b : A][p : \text{Path } A \ a \ b] \\
&\quad \text{PathD } ([i : \mathbb{I}] \ \text{Path } A \ a \ (p \cdot i)) \ (\text{refl } A \ a) \ p
\end{aligned}$$

Turning back to the left unit law, as before we work in a 3-dimensional hypercube, with the  $j = 1$  face (which is the one that we want to obtain with composition) being a path between  $p$  (at  $k = 0$ ) and  $\text{refl } A \ a \cdot p$  (at  $k = 1$ ). We complete the cube with the filler of the inverse on the  $j = 0$  face, reflexivity for the  $i = 0$  face, the filler of concatenation on the  $k = 1$  face,  $p \cdot i$  on the  $k = 0$  face and finally a term  $\gamma$ , which we shall derive again by composition, on the  $i = 1$  face.

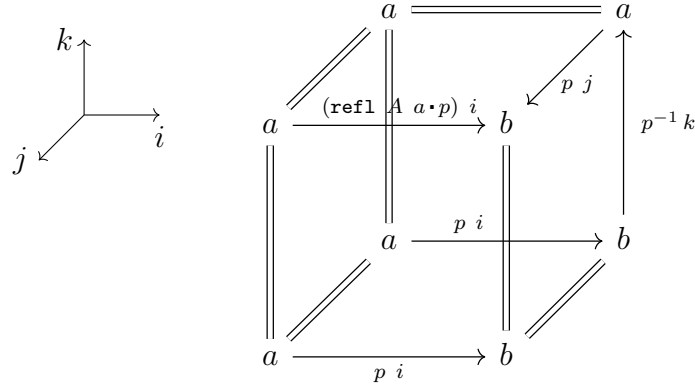


Figure 1.6: Composition for the left unit law.

```

leftUnit : [A : U][a, b, c : A][p : Path A a b]
  Path (Path A a b) p (concat A a a b (refl A a) p)
= [A : U][a, b, c : A][p : Path A a b][k, i : I]
  comp (I → A) (i = 0 ∨ i = 1 ∨ k = 0 ∨ k = 1) 0
  ([j : I][i = 0 → a,
    i = 1 → gamma A a b p j k,
    k = 0 → p i,
    k = 1 → concatFill A a a b (refl A a) p i j])
  (invFill A a b p k i) 1

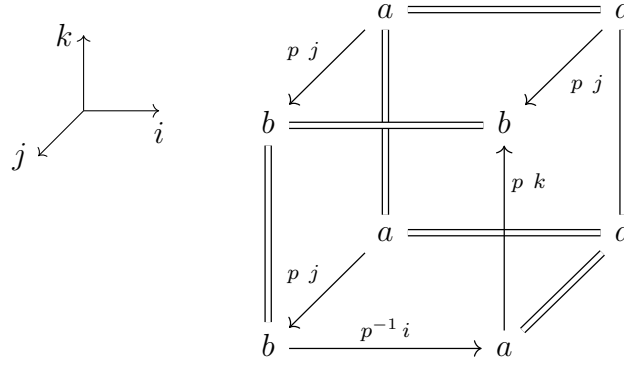
```

We now show how to derive the square  $\gamma$ ; as usual we work in a 3-dimensional hypercube (figure 1.7), defining its sides using the faces we already have at disposal.

```

gamma : [A : U][a, b : A][p : Path A a b][k, i : I]
  [k = 0 → inv A a b p i, k = 1 → b, i = 0 → b, i = 1 → p k] A
= [A : U][a, b : A][p : Path A a b][k, i : I]
  comp (I → A) (i = 0 ∨ i = 1 ∨ k = 0 ∨ k = 1) 0
  ([j : I][i = 0 → p j,
    i = 1 → weakMeet A a b p j k,
    k = 0 → invFill A a b p i j,
    k = 1 → p j])
  a 1

```

Figure 1.7: Composition for  $\gamma$ .

As a last example, we show how to derive the induction rule for path types, which asserts that for each predicate  $C : [x : A] \text{Path } A \ a \ x \rightarrow \mathbb{U}$ , from  $c : C \ a \ (\text{refl } A \ a)$  one may get  $C \ x \ p$  for each  $x : A$  and  $p : \text{Path } A \ a \ x$ . The idea is simply to transport  $c$  along a ‘type line’  $C \ a \ (\text{refl } A \ a) \rightarrow C \ x \ p$ , that is we have to find a  $D : \mathbb{I} \rightarrow \mathbb{U}$  such that  $D \ 0 \equiv C \ a \ (\text{refl } A \ a)$  and  $D \ 1 \equiv C \ x \ p$ . Using the weak meet operation, we choose

$$D \equiv [i : \mathbb{I}] \ C \ (p \ i) \ ([j : \mathbb{I}] \ p \ (i \wedge j)),$$

so that

$$\begin{aligned} D \ 0 &\equiv C \ (p \ 0) \ ([j : \mathbb{I}] \ p \ (0 \wedge j)) \equiv C \ a \ ([j : I] \ a) \equiv C \ a \ (\text{refl } A \ a), \\ D \ 1 &\equiv C \ (p \ 1) \ ([j : \mathbb{I}] \ p \ (1 \wedge j)) \equiv C \ x \ ([j : I] \ p \ j) \equiv C \ x \ p \end{aligned}$$

Therefore, we obtain path induction.

$$\begin{aligned} \text{pathInd} &: [A : \mathbb{U}][a : A][C : [x : A] \text{Path } A \ a \ x \rightarrow \mathbb{U}] \\ &\quad [x : A][p : \text{Path } A \ a \ x] \ C \ a \ (\text{refl } A \ a) \rightarrow C \ x \ p \\ &= [A : \mathbb{U}][a : A][C : [x : A] \text{Path } A \ a \ x \rightarrow \mathbb{U}] \\ &\quad [x : A][p : \text{Path } A \ a \ x][c : C \ a \ (\text{refl } A \ a)] \\ &\quad \text{transp} \ ([i : \mathbb{I}] \ C \ (\text{weakMeet } A \ a \ x \ p \ i \ 1) \ ([j : \mathbb{I}] \ \text{weakMeet } A \ a \ x \ p \ i \ j)) \ c \end{aligned}$$

Using similar ideas, it is also possible to derive the propositional computational rule for path induction, which is shown in [Ben21].

# Chapter 2

## Semantics

In this chapter we study the semantics of dependent type theory with partial elements. First we introduce the notion of ‘categories with families’ [Hof97], which is an abstract semantics based on category theory and is now the de facto standard in type theory semantics. Most interpretations of dependent type theory (e.g. groupoid [HS96], simplicial [KL21], cubical [CCHM15]) can be seen as particular cases of the aforementioned abstract semantics. We also describe presheaf models, that is categories with families induced by the category of presheaves over a base category. The category of cubical sets (cf. section 2.3) is an example of a presheaf category. Lastly, we show how to model partial and restriction types in presheaf models and we define an interpretation of the syntax, stating a soundness theorem.

### 2.1 Categories with families

First of all we define the category of families of sets, which is used to model dependency.

**Definition 2.1** (Fam). *The category **Fam** of families of sets is defined by:*

1. *Objects of the form  $(A, B)$ , where  $A$  is a set and  $B = (B_a)_{a \in A}$  is a family of sets indexed by  $A$ .*
2. *Morphisms of the form  $(f, g) : (A, B) \rightarrow (A', B')$ , where  $f : A \rightarrow A'$  is a function and  $g = \{g_a : a \in A\}$  is a family of functions  $g_a : B_a \rightarrow B'_{f(a)}$  indexed by  $A$ . Composition, for  $(f^1, g^1) : (A, B) \rightarrow (A', B')$  and  $(f^2, g^2) : (A', B') \rightarrow (A'', B'')$ , is defined by  $(f^2 \circ f^1, g')$ , with  $g'_a = g^2_{f^1(a)} \circ g^1_a$ .*

Before giving the main definition, let us fix the postfix notation for the composition of functions, i.e. writing  $fg$  for  $g \circ f$ , which will make the notation more intuitive as morphisms in CwFs are substitutions.

**Definition 2.2** (CwF). *A category with families (CwF) is given by:*

1. *A category  $\mathcal{C}$  with objects  $\Gamma, \Delta, \dots$  called contexts, morphisms  $\sigma, \tau, \dots$  called substitutions and a terminal object  $1$ .<sup>66</sup> We write  $\Gamma \vdash_s$  to mean that  $\Gamma$  is a context of  $\mathcal{C}$ .<sup>67</sup>*
2. *A functor  $\mathcal{F} : \mathcal{C}^{op} \rightarrow \mathbf{Fam}$ . Given a context  $\Gamma$ , we write the indexed family  $\mathcal{F}(\Gamma)$  as  $(\mathbf{Type}(\Gamma), (\mathbf{Term}(\Gamma; A))_{A \in \mathbf{Type}(\Gamma)})$ . If  $A \in \mathbf{Type}(\Gamma)$ , we say that  $A$  is a type in context  $\Gamma$  and write  $\Gamma \vdash_s A$ ; if  $a \in \mathbf{Term}(\Gamma; A)$ , we say that  $a$  is a term of type  $A$  in context  $\Gamma$  and write  $\Gamma \vdash_s a : A$ . For the morphisms of  $\mathcal{C}$ , given a substitution  $\sigma : \Delta \rightarrow \Gamma$ , contravariance yields  $\mathcal{F}(\sigma) : \mathcal{F}(\Gamma) \rightarrow \mathcal{F}(\Delta)$ , so  $\mathcal{F}$  acts on types  $\Gamma \vdash_s A$  as  $\Delta \vdash_s A\sigma$  and on terms  $\Gamma \vdash_s a : A$  as  $\Delta \vdash_s a\sigma : A\sigma$ . Since  $\mathcal{F}$  is a functor, we also have:*

$$A1 = A, \quad (A\sigma)\tau = A(\sigma\tau), \quad a1 = a, \quad (a\sigma)\tau = a(\sigma\tau).$$

3. *An operation of context extension: if  $\Gamma \vdash_s A$ , then there exists a context  $\Gamma.A$  with a substitution  $\mathbf{p}_{\Gamma,A} : \Gamma.A \rightarrow \Gamma$  and a term  $\Gamma.A \vdash_s \mathbf{q}_{\Gamma,A} : A\mathbf{p}_{\Gamma,A}$  such that for each context  $\Delta$ , substitution  $\sigma : \Delta \rightarrow \Gamma$  and term  $\Delta \vdash_s a : A\sigma$ , there exists a substitution  $(\sigma, a) : \Delta \rightarrow \Gamma.A$  such that:*

$$\mathbf{p}_{\Gamma,A}(\sigma, a) = \sigma, \quad \mathbf{q}_{\Gamma,A}(\sigma, a) = a, \quad (\sigma, a)\tau = (\sigma\tau, a\tau), \quad (\mathbf{p}_{\Gamma,A}, \mathbf{q}_{\Gamma,A}) = \mathbf{1}_{\Gamma.A}.$$

*Usually we will simply write  $\mathbf{p}$  and  $\mathbf{q}$  if  $\Gamma$  and  $A$  are clear.*

The definitions given above for a CwF can be presented as rules, and this is the notation we will use from now on. Pay attention not to confuse them with the formal syntactical rules of type theory; that's why we use the symbol  $\vdash_s$  ('s' is short for 'semantics').

- Context formation:

$$\frac{}{1 \vdash_s} \qquad \frac{\Gamma \vdash_s \quad \Gamma \vdash_s A}{\Gamma.A \vdash_s}$$

- Substitution in types and terms:

$$\frac{\Gamma \vdash_s A \quad \sigma : \Delta \rightarrow \Gamma}{\Delta \vdash_s A\sigma} \qquad \frac{\Gamma \vdash_s a : A \quad \sigma : \Delta \rightarrow \Gamma}{\Delta \vdash_s a\sigma : A\sigma}$$

<sup>66</sup>We denote by  $\mathbf{1}_A$ , or even by  $\mathbf{1}$ , the constant substitution  $A \rightarrow A$ .

<sup>67</sup> $\mathcal{C}$  will always be clear from the context.



- Context manipulation:

$$\frac{\Gamma \vdash_s A}{p : \Gamma.A \rightarrow \Gamma} \quad \frac{\Gamma \vdash_s A}{\Gamma.A \vdash_s q : Ap} \quad \frac{\Gamma \vdash_s A \quad \Delta \vdash_s a : A\sigma \quad \sigma : \Delta \rightarrow \Gamma}{(\sigma, a) : \Delta \rightarrow \Gamma.A}$$

Using these rules, we can derive the first ‘operation’, which is substitution with a term, as shown by the following remark.

**Remark 2.3** (Substitution by a term). *If we have an element  $\Gamma \vdash_s a : A$  and a dependent type over  $A$ , i.e.  $\Gamma.A \vdash_s B$ , then there is a ‘substitution by  $a$ ’ operation in the  $CwF$ ; indeed, given the identity substitution  $\mathbf{1} : \Gamma \rightarrow \Gamma$ , using the context extension property we can form  $(\mathbf{1}, a) : \Gamma \rightarrow \Gamma.A$ , usually denoted by  $[a] : \Gamma \rightarrow \Gamma.A$ , which gives  $\Gamma \vdash_s B[a]$ . Similarly for terms, i.e. from  $\Gamma.A \vdash_s b : B$  we obtain  $\Gamma \vdash_s b[a] : B[a]$ .*

The following is a technical remark which we will use in the subsequent arguments; it allows to extend a substitution.

**Remark 2.4.** *If we have a type  $\Gamma \vdash_s A$  and a substitution  $\sigma : \Delta \rightarrow \Gamma$ , then we can find a composition  $\Delta.A\sigma \rightarrow \Gamma.A$  as follows: first we form  $\sigma p_{\Delta, A\sigma} : \Delta.A\sigma \rightarrow \Gamma$ , with  $\Delta.A\sigma \vdash_s q_{\Delta, A\sigma} : A\sigma p_{\Delta, A\sigma}$ ; then we use the context comprehension property to get  $(\sigma p_{\Delta, A\sigma}, q_{\Delta, A\sigma}) : \Delta.A\sigma \rightarrow \Gamma.A$ .*

We now explain how to model type formers in a  $CwF$ , by first defining  $\Pi$ -types.

**Definition 2.5** ( $\Pi$ -types). *A  $CwF$  supports  $\Pi$ -types if the following rules are admissible.<sup>68</sup>*

$$\frac{\Gamma \vdash_s A \quad \Gamma.A \vdash_s B}{\Gamma \vdash_s \Pi_A B} \quad \frac{\Gamma.A \vdash_s b : B}{\Gamma \vdash_s \lambda b : \Pi_A B} \quad \frac{\Gamma \vdash_s u : \Pi_A B \quad \Gamma \vdash_s a : A}{\Gamma \vdash_s \text{app}(u, a) : B[a]}$$

and they satisfy the  $\beta$ -rule

$$\text{app}(\lambda b, a) = b[a]$$

and the laws for commutation with substitutions

$$(\Pi_A B)\sigma = \Pi_{A\sigma} B(\sigma p, q), \quad (\lambda b)\sigma = \lambda b(\sigma p, q), \quad \text{app}(u, a)\sigma = \text{app}(u\sigma, a\sigma).$$

**Remark 2.6.** *The above three equations can be justified by the following considerations,<sup>69</sup> given  $\sigma : \Delta \rightarrow \Gamma$ .*

<sup>68</sup>For example, stating that the first rule is admissible means that for each pair of types  $A \in \text{Type}(\Gamma)$  and  $B \in \text{Type}(\Gamma.A)$ , there is a type  $\Pi_A B \in \text{Type}(\Gamma)$  in the  $CwF$ .

<sup>69</sup>For brevity we do this only for the  $\Pi$ -type former, as it can be done analogously for the others type formers.

- Given a derivation

$$\frac{\Gamma \vdash_s A \quad \Gamma.A \vdash_s B}{\Gamma \vdash_s \Pi_A B}$$

then we can form

$$\frac{\frac{\Gamma \vdash_s A}{\Delta \vdash_s A\sigma} \quad \frac{\Gamma.A \vdash_s B}{\Delta.A\sigma \vdash_s B(\sigma\mathbf{p}, \mathbf{q})}}{\Delta \vdash_s \Pi_{A\sigma} B(\sigma\mathbf{p}, \mathbf{q})}$$

which is exactly how we defined  $(\Pi_A B)\sigma$ .

- Given a derivation

$$\frac{\Gamma.A \vdash_s b : B}{\Gamma \vdash_s \lambda b : \Pi_A B}$$

then we can form

$$\frac{\frac{\Gamma.A \vdash_s b : B}{\Delta.A\sigma \vdash_s b(\sigma\mathbf{p}, \mathbf{q}) : B(\sigma\mathbf{p}, \mathbf{q})}}{\Delta \vdash_s \lambda b(\sigma\mathbf{p}, \mathbf{q}) : \Pi_{A\sigma} B(\sigma\mathbf{p}, \mathbf{q})}$$

The last line is the same as  $\Delta \vdash_s (\lambda b)\sigma : (\Pi_A B)\sigma$ .

- Given a derivation

$$\frac{\Gamma \vdash_s u : \Pi_A B \quad \Gamma \vdash_s a : A}{\Gamma \vdash_s \mathbf{app}(u, a) : B[a]}$$

then we can form

$$\frac{\frac{\Gamma \vdash_s u : \Pi_A B}{\Delta \vdash_s u\sigma : \Pi_{A\sigma} B(\sigma\mathbf{p}, \mathbf{q})} \quad \frac{\Gamma \vdash_s a : A}{\Delta \vdash_s a\sigma : A\sigma}}{\Delta \vdash_s \mathbf{app}(u\sigma, a\sigma) : B(\sigma\mathbf{p}, \mathbf{q})[a]}$$

but  $B(\sigma\mathbf{p}, \mathbf{q})[a\sigma] = B(\sigma\mathbf{p}, \mathbf{q})(\mathbf{1}, a\sigma) = B(\sigma\mathbf{p}(\mathbf{1}, a\sigma), \mathbf{q}(\mathbf{1}, a\sigma)) = B(\sigma, a\sigma)$ , meaning that the last line in the derivation is the same as  $\Delta \vdash_s (\mathbf{app}(u, a))\sigma : B[a]\sigma$ , since  $B[a]\sigma = B(\mathbf{1}, a)\sigma = B(\mathbf{1}\sigma, a\sigma) = B(\sigma, a\sigma)$  too.

Similarly to  $\Pi$ -types, we now introduce  $\Sigma$ -types, whose definition is a bit simpler.

**Definition 2.7** ( $\Sigma$ -types). A *CwF* supports  $\Sigma$ -types if the following rules are admissible:

$$\frac{\Gamma \vdash_s A \quad \Gamma.A \vdash_s B}{\Gamma \vdash_s \Sigma_A B} \qquad \frac{\Gamma \vdash_s a : A \quad \Gamma \vdash_s b : B[a]}{\Gamma \vdash_s \langle a, b \rangle : \Sigma_A B}$$

$$\frac{\Gamma \vdash_s u : \Sigma_A B}{\Gamma \vdash_s \pi_1 u : A} \qquad \frac{\Gamma \vdash_s u : \Sigma_A B}{\Gamma \vdash_s \pi_2 u : B[\pi_1 u]}$$

and they satisfy the  $\beta$ -rules

$$\pi_1 \langle a, b \rangle = a, \qquad \pi_2 \langle a, b \rangle = b$$

and the laws for commutation with substitutions

$$\begin{aligned} (\Sigma_A B)\sigma &= \Sigma(A\sigma)(B(\sigma\mathbf{p}, \mathbf{q})), & \langle a, b \rangle\sigma &= \langle a\sigma, b(\sigma\mathbf{p}, \mathbf{q}) \rangle, \\ (\pi_1 u)\sigma &= \pi_1(u\sigma), & (\pi_2 u)\sigma &= \pi_2(u\sigma). \end{aligned}$$

One can define analogously the rules for the other type formers, as coproducts, naturals, etc. For brevity, here and in the following sections, we treat only the case of  $\Pi$  and  $\Sigma$  types.

Lastly, we discuss universes in CwFs. A universe contains codes for types, with two functions to get codes from actual types (encoding) and vice versa (decoding).<sup>70</sup>

**Definition 2.8** (Semantic universe). *A universe in a CwF  $(\mathcal{C}, \mathcal{F})$  is another CwF  $(\mathcal{C}, \mathcal{F}_0)$  on the same category  $\mathcal{C}$ , such that all the context operations are inherited from  $(\mathcal{C}, \mathcal{F})$  and for each context  $\Gamma$ ,  $\text{Type}_{\mathcal{F}_0}(\Gamma) \subseteq \text{Type}_{\mathcal{F}}(\Gamma)$ ;<sup>71</sup> moreover we require that for each type  $A \in \text{Type}_{\mathcal{F}_0}(\Gamma)$  (called small type, written  $\Gamma \vdash_s A \text{Type}_0$ ), the terms are the same, i.e.  $\text{Term}_{\mathcal{F}_0}(\Gamma; A) = \text{Term}_{\mathcal{F}}(\Gamma; A)$ . We require a type  $\vdash_s \mathbf{U}_0$  such that the following forming rules hold:<sup>72</sup>*

$$\frac{}{\vdash_s \mathbf{U}_0} \qquad \frac{\Gamma \vdash_s A \text{Type}_0}{\Gamma \vdash_s \ulcorner A \urcorner : \mathbf{U}_0} \qquad \frac{\Gamma \vdash_s T : \mathbf{U}_0}{\Gamma \vdash_s \text{El}T \text{Type}_0}$$

We also require commutation with substitutions

$$\mathbf{U}_0\sigma = \mathbf{U}_0 \qquad \ulcorner A \urcorner\sigma = \ulcorner A\sigma \urcorner \qquad (\text{El}T)\sigma = \text{El}(T\sigma)$$

and the following two structural equations:

$$\text{El}\ulcorner A \urcorner = A \qquad \ulcorner \text{El}T \urcorner = T.$$

<sup>70</sup>This is usually called a universe á la Tarski, opposed to the approach á la Russell, where the universe contains actual types.

<sup>71</sup>With the subscript we mean the collection given by the specified functor.

<sup>72</sup>We also write  $\mathbf{U}_0$  instead of  $\mathbf{U}_0\sigma$  for the unique substitution  $\sigma : \Gamma \rightarrow 1$ , for each  $\Gamma$ .

Type formers in the CwF can be ‘lifted’ to type formers inside  $\mathbf{U}_0$ , for example given

$$\Gamma \vdash_s a : \mathbf{U}_0, \quad \Gamma.\text{El } a \vdash_s b : \mathbf{U}_0,$$

then one may introduce  $\Gamma \vdash_s \pi_a b : \mathbf{U}_0$  given by

$$\pi_a b = \ulcorner \Pi_{(\text{El } a)}(\text{El } b) \urcorner,$$

which means that  $\Gamma \vdash_s \text{El } (\pi_a b)$ , with  $\text{El } (\pi_a b) = \Pi_{(\text{El } a)}(\text{El } b)$ . The type operations (in this case  $\lambda$  and **app**) are then exactly the same.

## 2.2 Presheaf models

In this section we show how the presheaf category on a fixed category  $\mathcal{C}$  induces a CwF; this will be used in section 2.3 to handle the cubical constructs by suitably choosing the base category  $\mathcal{C}$ .

**Definition 2.9.** *A presheaf on a category  $\mathcal{C}$  is a functor  $\mathcal{C}^{op} \rightarrow \mathbf{Set}$ . The category  $\hat{\mathcal{C}}$  of presheaves on  $\mathcal{C}$  is the functor category  $[\mathcal{C}^{op}, \mathbf{Set}]$ , which has presheaves on  $\mathcal{C}$  as objects and natural transformations between them as arrows.*

A presheaf  $\Gamma$  will be thought as a context  $\Gamma \vdash_s$ , with sets  $\Gamma(I)$  for each  $I \in \mathcal{C}$  and functions  $\Gamma_f : \Gamma(I) \rightarrow \Gamma(J)$  for each  $f : J \rightarrow I$ , usually written  $\rho \mapsto \rho f$  instead of  $\rho \mapsto \Gamma_f(\rho)$ , satisfying the functor laws

$$\rho \mathbf{1} = \rho, \quad (\rho)fg = \rho(fg).$$

We now explain how to define a CwF from  $\hat{\mathcal{C}}$ :

- Contexts are given by presheaves, with the terminal object  $\mathbf{1}$  defined by the constant presheaf  $\mathbb{1}$  such that  $\mathbb{1}(I) = \{\star\}$  for all  $I \in \mathcal{C}$ .<sup>73</sup>
- A substitution  $\sigma : \Delta \rightarrow \Gamma$  is a morphism between functors  $\Delta$  and  $\Gamma$ , i.e. a natural transformation  $\sigma = (\sigma_I : \Delta(I) \rightarrow \Gamma(I))_{I \in \mathcal{C}}$ , such that the naturality condition holds:

$$\Gamma_f \circ \sigma_I = \sigma_J \circ \Delta_f$$

usually written as

$$(\sigma \rho)f = \sigma(\rho f)$$

for all  $\rho \in \Delta(I)$ .

---

<sup>73</sup>The set  $\{\star\}$  is ‘the’ singleton set.

- A type  $\Gamma \vdash_s A$  is given by sets  $A\rho$  for all  $I \in \mathcal{C}$  and  $\rho \in \Gamma(I)$  and by functions  $A\rho \rightarrow A(\rho f)$  for each  $f : J \rightarrow I$ , as usual written as  $a \mapsto af$ , such that the functorial laws hold:

$$a\mathbf{1} = a, \quad (af)g = a(fg).$$

Substitutions on types are defined as follows: given  $\Gamma \vdash_s A$  and  $\sigma : \Delta \rightarrow \Gamma$ ,  $\Delta \vdash_s A\sigma$  is given by sets  $(A\sigma)\rho = A(\sigma\rho)$  and by the induced map  $(A\sigma)\rho = A(\sigma\rho) \rightarrow A((\sigma\rho)f) = A(\sigma(\rho f)) = (A\sigma)(\rho f)$ .

- A term  $\Gamma \vdash_s a : A$  is given by an element  $a\rho \in A\rho$  for each  $I \in \mathcal{C}$  and  $\rho \in \Gamma(I)$ , such that the following law hold for all  $f : J \rightarrow I$ :

$$(a\rho)f = a(\rho f).$$

Substitutions on terms are defined as follows: given  $\Gamma \vdash_s a : A$  and  $\sigma : \Delta \rightarrow \Gamma$ , the term  $\Delta \vdash_s a\sigma : A\sigma$  is given by sets  $(a\sigma)\rho = a(\sigma\rho)$ .

- The extended context  $\Gamma.A \vdash_s$ , given  $\Gamma \vdash_s A$ , is defined by the sets

$$(\Gamma.A)(I) = \{(\rho, u) : \rho \in \Gamma(I), u \in A\rho\}$$

for each  $I \in \mathcal{C}$  and by the functions  $(\Gamma.A)_f : (\Gamma.A)(I) \rightarrow (\Gamma.A)(J)$  defined by

$$(\rho, u)f = (\rho f, uf)$$

for each morphism  $f : J \rightarrow I$ . The projections  $\mathbf{p} : \Gamma.A \rightarrow \Gamma$  and  $\Gamma.A \vdash_s \mathbf{q} : A\mathbf{p}$  are defined as to satisfy the required equations, i.e.

$$\mathbf{p}(\rho, u) = \rho \quad \mathbf{q}(\rho, u) = u.^{74}$$

Given  $\sigma : \Delta \rightarrow \Gamma$  and  $\Delta \vdash a : A\sigma$ , for the substitution  $(\sigma, a) : \Delta \rightarrow \Gamma.A$  we put, for  $\rho \in \Delta(I)$ ,

$$(\sigma, a)\rho = (\sigma\rho, a\rho).$$

It is straightforward now to verify that the required equations hold:

- $\mathbf{p}(\sigma, a) = \sigma$ , since  $\mathbf{p}(\sigma, a)\rho = \mathbf{p}(\sigma\rho, a\rho) = \sigma\rho$ ;
- $\mathbf{q}(\sigma, a) = a$ , since  $\mathbf{q}(\sigma, a)\rho = \mathbf{q}(\sigma\rho, a\rho) = a\rho$ ;
- $(\sigma, a)\tau = (\sigma\tau, a\tau)$ , since  $(\sigma, a)\tau\rho = (\sigma, a)(\tau\rho) = (\sigma(\tau\rho), a(\tau\rho)) = (\sigma\tau\rho, a\tau\rho)$ ;
- $(\mathbf{p}, \mathbf{q}) = \mathbf{1}$ , since  $(\mathbf{p}, \mathbf{q})(\rho, u) = (\mathbf{p}(\rho, u), \mathbf{q}(\rho, u)) = (\rho, u)$ .

---

<sup>74</sup>Remember that to give a term  $\Gamma.A \vdash_s \mathbf{q} : A\mathbf{p}$  we must specify an element  $\mathbf{q}(\rho, u) \in A\rho$  for each  $(\rho, u) \in \Gamma.A$ .

### 2.2.1 $\Pi$ -types

First of all, following [Hub16], we give a motivation for the definition of  $\Pi$ -types in presheaf categories, by exploiting the intuitive idea that function types should be modelled by their categorical counterpart which are exponentials. If  $\Gamma$  and  $\Delta$  are presheaves and the exponential  $\Delta^\Gamma$  exists, then by the Yoneda lemma (see appendix A) and the fact that exponentiation is right adjoint to the product, we get

$$(\Delta^\Gamma)(I) \cong \text{Hom}_{\mathcal{C}}(\mathbf{y}I, \Delta^\Gamma) \cong \text{Hom}_{\mathcal{C}}(\mathbf{y}I \times \Gamma, \Delta).$$

This can then be taken as a definition, so that the elements of the presheaf  $\Delta^\Gamma$  are natural transformations  $w : \mathbf{y}I \times \Gamma \rightarrow \Delta$ , i.e.  $w = (w_J : \text{Hom}_{\mathcal{C}}(J, I) \times \Gamma(J) \rightarrow \Delta(J))_{J \in \mathcal{C}}$  satisfying the naturality condition

$$\Delta_g \circ w_J = w_K \circ ((\mathbf{y}I)_g, \Gamma_g)$$

for each  $g : K \rightarrow J$ , which means that for every  $(f, \rho) \in \text{Hom}_{\mathcal{C}}(J, I) \times \Gamma(J)$ , the following holds:

$$(w_J(f, \rho))g = w_K(fg, \rho g).$$

$$\begin{array}{ccc} \text{Hom}_{\mathcal{C}}(J, I) \times \Gamma(J) & \xrightarrow{(\mathbf{y}I)_g \times \Gamma_g} & \text{Hom}_{\mathcal{C}}(K, I) \times \Gamma(K) \\ \downarrow w_J & & \downarrow w_K \\ \Delta(J) & \xrightarrow{\Delta_g} & \Delta(K) \end{array}$$

Figure 2.1: Naturality condition for  $w$ .

Now we show how a presheaf category supports  $\Pi$ -types in the induced CwF:

1. (Type formation) Given  $\Gamma \vdash_s A$  and  $\Gamma.A \vdash_s B$ , we shall define the type  $\Gamma \vdash_s \Pi_A B$ . Let  $I \in \mathcal{C}$  and  $\rho \in \Gamma(I)$ ; we define the set  $(\Pi_A B)\rho$  as composed by the families  $w = (w_f)_{J \in \mathcal{C}, f: J \rightarrow I}$ , such that for each  $u \in A(\rho f)$ ,

$$w_f u \in B(\rho f, u)$$

and for each  $g : K \rightarrow J$ , the following holds:

$$(w_f u)g = w_{fg}(ug).$$

The last equation is well typed since  $(w_f u)g \in B(\rho f, u)g = B(\rho f g, u g)$ . We also have to specify a function  $(\Pi_A B)\rho \rightarrow (\Pi_A B)(\rho f)$  for each  $f : J \rightarrow I$ , mapping  $w \in (\Pi_A B)\rho \mapsto w f \in (\Pi_A B)(\rho f)$ . The latter is defined by

$$(w f)_g u = w_{fg} u \in B(\rho f g, u)$$

for each  $g : K \rightarrow J$  and  $u \in A(\rho f g)$ . This definition satisfies the required functorial equations:

- $w \mathbf{1} = w$ , since  $(w \mathbf{1})_g u = w_{\mathbf{1}g} u = w_g u$ .
  - $(w f)g = w(fg)$ , since  $((w f)g)_h u = (w f)_{gh} u = w_{fgh} u$  and  $(w(fg))_h u = w_{fgh} u$ .
2. (Abstraction) Given  $\Gamma.A \vdash_s b : B$ , we shall define a term  $\Gamma \vdash_s \lambda b : \Pi_A B$  by giving a set  $(\lambda b)\rho \in (\Pi_A B)\rho$  for each  $I \in \mathcal{C}$  and  $\rho \in \Gamma(I)$ ; if  $f : J \rightarrow I$  and  $u \in A(\rho f)$ , we put

$$((\lambda b)\rho)_f u = b(\rho f, u) \in B(\rho f, u).^{75}$$

We have to check that  $((\lambda b)\rho)f = (\lambda b)(\rho f)$ , indeed

$$(((\lambda b)\rho)f)_g u = ((\lambda b)\rho)_{fg} u = b(\rho f g, u)$$

which is equal to  $((\lambda b)(\rho f))_g u = b(\rho f g, u)$  by definition.

3. (Application) Given  $\Gamma \vdash_s u : \Pi_A B$  and  $\Gamma \vdash_s v : A$ , we shall define a term  $\Gamma \vdash_s \mathbf{app}(u, v) : B[v]$ , remembering that  $B[v]$  is short for  $B(\mathbf{1}, v)$ . For each  $I \in \mathcal{C}$  and  $\rho \in \Gamma(I)$  we define the element  $\mathbf{app}(u, v)\rho \in B(\mathbf{1}, v)\rho$  by

$$\mathbf{app}(u, v)\rho = (u\rho)_{\mathbf{1}}(v\rho) \in B(\rho \mathbf{1}, v\rho) = (B[v])\rho$$

since  $u\rho \in (\Pi_A B)\rho$  and  $v\rho \in A\rho$ .

It is now easy to check that the CwF equations for  $\Pi$ -types hold:

- ( $\beta$ -reduction)  $\mathbf{app}(\lambda b, v) = b[v]$  since

$$\mathbf{app}(\lambda b, v)\rho = ((\lambda b)\rho)_{\mathbf{1}}(v\rho) = b(\rho, v\rho) = b[v]\rho.$$

- (Substitution 1)  $(\Pi_A B)\sigma = \Pi_{A\sigma} B(\sigma \mathbf{p}, \mathbf{q})$  holds since  $((\Pi_A B)\sigma)\rho = (\Pi_A B)(\sigma\rho)$  and any element  $w$  of that set is such that for all  $f : J \rightarrow I$  and  $u \in A(\sigma\rho f) = A(\sigma(\rho f))$ ,  $w_f u \in B(\sigma\rho f, u) = B(\sigma \mathbf{p}, \mathbf{q})(\rho f, u)$ , which means that  $w$  is also an element of  $\Pi_{A\sigma} B(\sigma \mathbf{p}, \mathbf{q})$ . The other inclusion is proved analogously.

---

<sup>75</sup>Remember that  $\Gamma.A \vdash_s b : B$  and  $(\rho f, u) \in (\Gamma.A)(J)$ , so that  $b(\rho f, u) \in B(\rho f, u)$ .

- (Substitution 2)  $(\lambda b)\sigma = \lambda b(\sigma\mathbf{p}, \mathbf{q})$  holds since

$$\begin{aligned} (((\lambda b)\sigma)\rho)_f u &= ((\lambda b)(\sigma\rho))_f u = b(\sigma\rho f, u) \\ &= b(\sigma\mathbf{p}, \mathbf{q})(\rho f, u) = ((\lambda b(\sigma\mathbf{p}, \mathbf{q}))\rho)_f u. \end{aligned}$$

- (Substitution 3)  $\mathbf{app}(u, v)\sigma = \mathbf{app}(u\sigma, v\sigma)$  holds since

$$\begin{aligned} (\mathbf{app}(u, v)\sigma)\rho &= \mathbf{app}(u, v)(\sigma\rho) = (u(\sigma\rho))_1(v(\sigma\rho)) \\ &= ((u\sigma)\rho)_1((v\sigma)\rho) = \mathbf{app}(u\sigma, v\sigma)\rho. \end{aligned}$$

### 2.2.2 $\Sigma$ -types

We show how a presheaf category supports  $\Sigma$ -types in the induced CwF:

1. (Type formation) Given  $\Gamma \vdash_s A$  and  $\Gamma.A \vdash_s B$ , we shall define the type  $\Gamma \vdash_s \Sigma_A B$ . For  $I \in \mathcal{C}$  and  $\rho \in \Gamma(I)$ , let

$$(\Sigma_A B)\rho = \{(a, b) : a \in A\rho, b \in B(\rho, a)\}$$

with the mapping  $(\Sigma_A B)\rho \rightarrow (\Sigma_A B)(\rho f)$  given by

$$(a, b)f \mapsto (af, bf).$$

2. (Pairing) Given  $\Gamma \vdash_s a : A$  and  $\Gamma.A \vdash_s b : B[a]$ , we shall define the term  $\Gamma \vdash_s \langle a, b \rangle : \Sigma_A B$ . For  $I \in \mathcal{C}$  and  $\rho \in \Gamma(I)$ , let

$$\langle a, b \rangle \rho = (a\rho, b\rho).$$

3. (Projections) Given  $\Gamma \vdash_s u : \Sigma_A B$ , we shall define the two projections  $\Gamma \vdash_s \pi_1 u : A$  and  $\Gamma \vdash_s \pi_2 u : B[\pi_1 u]$  by

$$(\pi_1 u)\rho = a, \quad (\pi_2 u)\rho = b,$$

where  $u\rho = (a, b) \in (\Sigma_A B)\rho$ .

It can be easily shown that  $\beta$ -reduction and the commutation with substitutions hold, analogously to what we have done in section 2.2.1 for  $\Pi$ -types.



### 2.2.3 Universes

To model a universe of types we require a Grothendieck universe,<sup>76</sup> which we denote by  $\mathbf{Set}_0$ . For a type  $\Gamma \vdash_s A$ , we put  $\Gamma \vdash_s A \text{ Type}_0$  iff  $A\rho \in \mathbf{Set}_0$  for all  $I \in \mathcal{C}$  and  $\rho \in \Gamma(I)$  (small types). In this way small types form a CwF supporting all the types formers available in the larger CwF.<sup>77</sup>

Next we define the type  $\vdash_s \mathbf{U}_0$ , which is the same as giving a context  $\mathbf{U}_0 \vdash_s$ . We use the Yoneda embedding  $y$  (see appendix A). For objects  $I \in \mathcal{C}$ , we put  $\mathbf{U}_0(I) = \{A \mid yI \vdash_s A \text{ Type}_0\}$ ; for morphisms  $f : J \rightarrow I$  and  $A \in \mathbf{U}_0(I)$ ,  $Af \in \mathbf{U}_0(J)$  is given by  $yJ \vdash_s Ayf \text{ Type}_0$  (since  $yf : yI \rightarrow yJ$ ,  $A \mapsto Ayf$ ).

Defined it this way, each  $\mathbf{U}_0(I)$  is composed by small types  $yI \vdash_s A \text{ Type}_0$ , which means that for each  $f : J \rightarrow I$  there is a small set  $A_f$  with maps  $A_f \rightarrow A_{fg}$ ,  $a \mapsto ag$ , such that  $a\mathbf{1} = a$  and  $(ag)h = a(gh)$  for each  $g : K \rightarrow J$  and  $h : M \rightarrow K$ . With this notation, the map  $\mathbf{U}_0(I) \rightarrow \mathbf{U}_0(J)$  is  $A \mapsto Af$ , with  $(Af)_g = A_{yfg} = A_{gf}$ .

Finally we define the encoding and decoding functions:

- (Encoding) If  $\Gamma \vdash_s A \text{ Type}_0$ , we define  $\Gamma \vdash_s \ulcorner A \urcorner : \mathbf{U}_0$  by  $\ulcorner A \urcorner \rho \in \mathbf{U}_0(I)$  as the small type  $yI \vdash_s \ulcorner A \urcorner \rho$  given by sets  $(\ulcorner A \urcorner \rho)_f = A(\rho f)$ , with the induced map  $(\ulcorner A \urcorner \rho)_f \rightarrow (\ulcorner A \urcorner \rho)_{fg}$  given by  $A(\rho f) \rightarrow A(\rho f)g$ , since  $(\ulcorner A \urcorner \rho)_f = A(\rho f)$  and  $(\ulcorner A \urcorner \rho)_{fg} = A(\rho(fg)) = A(\rho f)g$ . It is easy to verify that  $\ulcorner A \urcorner \sigma = \ulcorner A \sigma \urcorner$ .
- (Decoding) If  $\Gamma \vdash_s T : \mathbf{U}_0$ , we define the small type  $\Gamma \vdash_s \text{El } T \text{ Type}_0$  by  $(\text{El } T)\rho = (T\rho)_{\mathbf{1}_I}$ , with the induced map  $(\text{El } T)\rho \rightarrow (\text{El } T)(\rho f)$  given by  $(T\rho)_{\mathbf{1}} \rightarrow (T\rho)_f$ , since  $(\text{El } T)\rho = (T\rho)_{\mathbf{1}}$  and  $(\text{El } T)(\rho f) = (T(\rho f))_{\mathbf{1}} = ((T\rho)f)_{\mathbf{1}} = (T\rho)_f$ . It is easy to verify that  $(\text{El } T)\sigma = \text{El } (T\sigma)$ .

The two structural equations hold:

$$(\text{El } \ulcorner A \urcorner)\rho = (\ulcorner A \urcorner \rho)_{\mathbf{1}} = A(\rho\mathbf{1}) = A\rho,$$

$$((\ulcorner \text{El } T \urcorner)\rho)_f = (\text{El } T)(\rho f) = (T(\rho f))_{\mathbf{1}} = ((T\rho)f)_{\mathbf{1}} = (T\rho)_f.$$

Note that for a hierarchy of Grothendieck universes  $\mathbf{Set}_0 \in \mathbf{Set}_1 \in \mathbf{Set}_2 \in \dots \in \mathbf{Set}$ , the same construction can be iterated to obtain a hierarchy of uni-

<sup>76</sup>A Grothendieck universe is a transitive set containing pairs and power sets of all its elements, along with the union of any family in the universe indexed by an element of the universe. The existence of a Grothendieck universe in ZFC is equivalent to the existence of a strongly inaccessible cardinal, which is independent from ZFC.

<sup>77</sup>This is possible since  $\mathbf{Set}_0$  is closed under all the ordinary set-theoretic operations; this is the reason of choosing a Grothendieck universe.

verses  $U_0, U_1, U_2, \dots$  in the type theory, each with its own encoding/decoding functions.

## 2.3 Cubical sets

In this section we introduce cubical sets, which is the presheaf category on the category of cubes  $\mathcal{C}$ .

**Definition 2.10** (Category of cubes). *Fix a discrete and countably infinite set of names, usually denoted by  $x, y, z, \dots$ . The category of cubes  $\mathcal{C}$  has as objects the finite subsets of names, usually denoted by  $I, J, K, \dots$ , and as morphisms  $f : I \rightarrow J$  set-theoretic functions  $f : I \rightarrow J \cup \mathbf{2}$  which are injective on the set  $\text{def}(f) = \{x \in I : \tilde{f}(x) \notin \mathbf{2}\}$ . Composition of morphisms is defined as*

$$(fg)(x) = \begin{cases} \tilde{g}(\tilde{f}(x)) & \text{if } x \in \text{def}(f) \\ \tilde{f}(x) & \text{otherwise} \end{cases}$$

**Example 2.11.** *Using the notation  $I, x_1, \dots, x_n$  for  $I \cup \{x_1, \dots, x_n\}$  and  $I - x_1, \dots, x_n$  for  $I \setminus \{x_1, \dots, x_n\}$ , we name a few particular morphisms:*

- *Face maps  $(x = 0), (x = 1) : I \rightarrow I - x$  which are the identity except that they map  $x$  to 0 or 1. It holds that  $\text{def}(x = 0) = \text{def}(x = 1) = I - x$ .*
- *Degeneracy map  $s_x : I \rightarrow I, x$  for  $x \notin I$ , which is the inclusion map  $I \subseteq I, x$ .*
- *Renaming map  $(x = y) : I, x \rightarrow I, y$  for  $x, y \notin I$ , which is the identity except that  $x$  gets mapped to  $y$ .*

**Definition 2.12.** *A cubical set  $X$  is a functor  $X : \mathcal{C} \rightarrow \mathbf{Set}$ , where  $\mathcal{C}$  is the category of cubes. In other words, a cubical set is a presheaf on  $\mathcal{C}^{\text{op}}$ .*

As any other presheaf category,  $\widehat{\mathcal{C}^{\text{op}}}$  induces a CwF, as described in section 2.2.<sup>78</sup> Note that every cubical set  $X$  can be seen as a type  $\Gamma \vdash_s X'$ , putting  $X'\rho = X(I)$  for each  $I \in \mathcal{C}$  and  $\rho \in \Gamma(I)$ ; for simplicity we shall write  $X$  for both.

Now we show how to model the formal interval  $\mathbb{I}$  as a cubical set.

<sup>78</sup>A trivial but important point is that cubical sets are covariant functors, so that  $\cdot^{\text{op}}$  is applied twice to form the presheaf category of cubical sets, which means that all the arrows get reversed, i.e. if  $\Gamma$  is a cubical set and  $f : I \rightarrow J$  is a map in the category of cubes, then  $\Gamma_f : \Gamma(I) \rightarrow \Gamma(J)$ . The same applies to the Yoneda embedding for  $\mathcal{C}^{\text{op}}$ , i.e. in the context of cubical sets,  $yI = \text{Hom}_{\mathcal{C}^{\text{op}}}(-, I) \cong \text{Hom}_{\mathcal{C}}(I, -)$ .

**Example 2.13.** The interval  $\mathbb{I}$  is defined on objects by  $\mathbb{I}(I) = I \cup \{0, 1\}$  and on morphisms  $f : I \rightarrow J$  by  $\mathbb{I}_f : I \cup \{0, 1\} \rightarrow J \cup \{0, 1\}$  obtained extending  $f$  with  $\mathbb{I}_f(0) = 0$  and  $\mathbb{I}_f(1) = 1$ . It is important to note that  $\mathbb{I}$  is a representable functor, as

$$\mathbf{y}\{x\} = \text{Hom}_{\mathcal{C}}(\{x\}, -) \cong \mathbb{I}$$

since for example  $\mathbf{y}\{x\}\{y_1, \dots, y_n\} = \text{Hom}_{\mathcal{C}}(\{x\}, \{y_1, \dots, y_n\})$  which is composed by the morphisms  $(x = 0)$ ,  $(x = 1)$  and  $(x = y_i)$  for each  $i$ , and is isomorphic to  $\mathbb{I}(\{y_1, \dots, y_n\})$ . More generally, instead of defining the square, the cube, etc. ‘manually’, we can use the Yoneda embedding (see appendix A) to define them using  $\mathbf{y}$ , so we set

$$\square_I = \mathbf{y}I,$$

for any set of names  $I$ , called the standard  $I$ -cube. By the Yoneda lemma, it holds that

$$\text{Hom}_{\widehat{\mathcal{C}^{op}}}(\square_I, X) \cong X(I).$$

**Example 2.14.** The set of formulas induces a cubical set  $\mathbb{F}$  defined by the sets  $\mathbb{F}(I) = \{\varphi \mid \text{vars}(\varphi) \subseteq I\}$  on objects and on morphisms  $f : I \rightarrow J$  by  $\mathbb{F}_f : \mathbb{F}(I) \rightarrow \mathbb{F}(J)$ ,  $\varphi \mapsto \varphi f$  which substitutes the symbols  $i \in I$  by  $f(i) \in J$ .

## 2.4 Semantics of the full theory

Having introduced all the general concepts we need (CwFs, presheaf categories, cubical sets), we now start to use them to give a semantics for the type theory. Actually, for simplicity we consider a slightly less powerful theory, that is:

1. A single universe instead of the (tacitly presupposed) infinite cumulative hierarchy of universes. This means that impredicative definitions are not allowed (obviously we do not consider the inconsistent axiom  $\mathbf{U} : \mathbf{U}$ ).
2. No coproducts, which means only naturals, function and pair types as the basic type formers.<sup>79</sup>
3. No composition operation.
4. No ‘diagonals’ constraints, which means that atomic formulas are only the ones of the form  $(i = 0)$  and  $(i = 1)$ .

<sup>79</sup>Adding coproducts and other type formers, such as the empty type which is not definable any more (the definition  $\text{empty} : \mathbf{U} = [X : \mathbf{U}]X$  is impredicative!), poses no difficulty, but we avoid it for brevity.

Moreover, we forget the distinction between the context and the directions environment, so that formulas are now added to the context, e.g.  $\Gamma, \varphi$ .<sup>80</sup> We also write  $s \sim^\Gamma t$  instead of  $s \sim_{\tau(\Gamma)}^\Theta t$  (see section 1.5), where as usual  $\tau(\Gamma)$  is the list of names declared in  $\Gamma$ . Typing rules are now seen as unidirectional, i.e.  $\Gamma \vdash t \Leftarrow A$  and  $\Gamma \vdash t \Rightarrow A$  are read as  $\Gamma \vdash t : A$ .<sup>81</sup>

### 2.4.1 Modelling formulas

We now explain how to model formulas in the semantics, that is for each  $\Gamma \vdash \varphi : \mathbb{F}$  we define a  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; \varphi \rrbracket : \mathbb{F}$ .<sup>82</sup> To avoid confusion from now on we shall always use the  $\llbracket \cdot \rrbracket$  notation (see section 2.5); for a syntactical context  $\Gamma$ , we write  $\llbracket \Gamma \rrbracket$  to denote the (semantic) context in the CwF induced by cubical sets, and  $\llbracket \Gamma; t \rrbracket$  for the interpretation of a syntactical term  $t$  in context  $\Gamma$ . It is important to keep in mind the statement of the soundness theorem (2.15), which says in particular that for types  $\Gamma \vdash A : \mathbb{U}$ , the interpretation is such that  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; A \rrbracket : \mathbb{U}_0$ , so that  $\llbracket \Gamma \rrbracket \vdash_s \text{El } \llbracket \Gamma; A \rrbracket$ ; for terms  $\Gamma \vdash a : A$ , the interpretation is such that  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; a \rrbracket : \text{El } \llbracket \Gamma; A \rrbracket$ . Definitions are given such that the aforementioned results shall be proved.<sup>83</sup>

The definition of  $\llbracket \Gamma; \varphi \rrbracket$  is by induction on the structure of  $\varphi$  and  $\Gamma$ , and is such that  $\llbracket \Gamma; \varphi \rrbracket \rho \in \mathbb{F} \rho = \mathbb{F}(I)$  whenever  $\rho \in \Gamma(I)$ . Note that in the first case, the empty context case is not needed, since a formula must have all of its variables declared in the context.

- For  $(i = 0)$ , let:

$$\begin{aligned} \llbracket \Gamma, i : \mathbb{I}; i = 0 \rrbracket(\rho, z) &= \begin{cases} \text{True} & \text{if } z = 0 \\ \text{False} & \text{if } z = 1 \\ z = 0 & \text{if } z \in I \end{cases} \quad (\rho \in \llbracket \Gamma \rrbracket(I) \text{ and } z \in \mathbb{I}(I)) \\ \llbracket \Gamma, j : \mathbb{I}; i = 0 \rrbracket(\rho, z) &= \llbracket \Gamma; i = 0 \rrbracket \rho \quad (\rho \in \llbracket \Gamma \rrbracket(I) \text{ and } z \in \mathbb{I}(I)) \end{aligned}$$

<sup>80</sup>The aforementioned distinction is very useful for the implementation, but is unnatural when defining the semantics, making the notation more complex. Remember that the context  $\Gamma, \varphi_1, x : A, \varphi_2$  is ‘equivalent’ to  $\Gamma, x : A, \varphi_1 \wedge \varphi_2$ , and indeed it can be easily checked that this holds in the interpretation of contexts as cubical sets.

<sup>81</sup>Likewise, the distinction was very useful for the implementation, but not at all when defining the semantics.

<sup>82</sup> $\mathbb{I}$  and  $\mathbb{F}$  remain the same in the interpretation, so we avoid writing  $\llbracket \mathbb{I} \rrbracket$  and  $\llbracket \mathbb{F} \rrbracket$ . Also we use the same symbol to denote both the cubical set and the type, as it makes no ambiguity.

<sup>83</sup>The most formal way to present the semantics would be to give the definitions of  $\llbracket \cdot \rrbracket$  for all the cases altogether, but this makes the presentation harder to understand. Therefore, we give now the definition for interpreting formulas, even if e.g. the interpretation of contexts is given later in section 2.5.

$$\begin{aligned}
\llbracket \Gamma, x : A; i = 0 \rrbracket(\rho, u) &= \llbracket \Gamma; i = 0 \rrbracket \rho & (\rho \in \llbracket \Gamma \rrbracket(I) \text{ and } u \in \llbracket A \rrbracket(I)) \\
\llbracket \Gamma, \varphi; i = 0 \rrbracket \rho &= \llbracket \Gamma; i = 0 \rrbracket \rho & (\rho \in \llbracket \Gamma \rrbracket(I), \llbracket \Gamma; \varphi \rrbracket \rho = \mathbf{True}) \\
\llbracket \Gamma, x : A = t; i = 0 \rrbracket &= \llbracket \Gamma; i = 0 \rrbracket
\end{aligned}$$

- For  $(i = 1)$ , the definition is totally analogous to the previous one, swapping 0 with 1 and 0 with 1.<sup>84</sup>
- For  $\psi_1 \wedge \psi_2$  and  $\rho \in \Gamma(I)$ , we put

$$\llbracket \Gamma; \psi_1 \wedge \psi_2 \rrbracket \rho = (\llbracket \Gamma; \psi_1 \rrbracket \rho) \wedge (\llbracket \Gamma; \psi_2 \rrbracket \rho).^{85}$$

- For  $\varphi_1 \vee \varphi_2$  and  $\rho \in \Gamma(I)$ , we put

$$\llbracket \Gamma; \varphi_1 \vee \varphi_2 \rrbracket \rho = (\llbracket \Gamma; \varphi_1 \rrbracket \rho) \vee (\llbracket \Gamma; \varphi_2 \rrbracket \rho).$$

It is routine to check that  $(\llbracket \Gamma; \varphi \rrbracket \rho)f = \llbracket \Gamma; \varphi \rrbracket(\rho f)$  holds.

We also define, for each formula  $\Gamma \vdash \varphi : \mathbb{F}$ , a subsingleton type  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; [\varphi] \rrbracket$  whose inhabitation corresponds to  $\varphi$  being true in  $\Gamma$ . Keeping in mind that for each  $I \in \mathcal{C}$  and  $\rho \in \Gamma(I)$  we have a  $\llbracket \Gamma; \varphi \rrbracket \rho \in \mathbb{F}(I)$ , we put:<sup>86</sup>

$$\llbracket \Gamma; [\varphi] \rrbracket \rho = \begin{cases} \{\star\} & \text{if } \llbracket \Gamma; \varphi \rrbracket \rho = \mathbf{True} \\ \emptyset & \text{otherwise} \end{cases}$$

The restriction  $\llbracket \Gamma; [\varphi] \rrbracket \rho \rightarrow \llbracket \Gamma; [\varphi] \rrbracket(\rho f)$  is defined in the obvious manner.

Note what a context extension with a formula looks like:

$$\begin{aligned}
(\llbracket \Gamma \rrbracket. \llbracket \Gamma; [\varphi] \rrbracket)(I) &= \{(\rho, -) \mid \rho \in \llbracket \Gamma \rrbracket(I), - \in \llbracket \Gamma; [\varphi] \rrbracket \rho\} \\
&= \{\rho \mid \rho \in \Gamma(I), \llbracket \Gamma; \varphi \rrbracket \rho = \mathbf{True}\}
\end{aligned}$$

This means that for example:

$$\begin{aligned}
\llbracket \Gamma \rrbracket. \llbracket \Gamma; [\mathbf{True}] \rrbracket &= \llbracket \Gamma \rrbracket, \\
\llbracket \Gamma \rrbracket. \llbracket \Gamma; [\mathbf{False}] \rrbracket &= \llbracket () \rrbracket,
\end{aligned}$$

<sup>84</sup>0 and 1 are elements of  $\mathbb{I}(I)$ , 0 and 1 are syntactical objects of the type theory.

<sup>85</sup>It is understood that the resulting value is **False** if one of the two is false. Similarly for the  $\varphi_1 \vee \varphi_2$  case below.

<sup>86</sup>The apparent circularity in the definitions of  $\llbracket \cdot \rrbracket$  (e.g  $\llbracket \Gamma; [\varphi] \rrbracket$  depends on  $\llbracket \Gamma; \varphi \rrbracket$ , which depends on  $\llbracket \Gamma, \varphi \rrbracket$ , which depends on  $\llbracket \Gamma; [\varphi] \rrbracket$ ) can be removed by giving all the definitions at the same time (although this requires care, see the footnote 91). We preferred to give them as separate definitions to improve clarity.

$$\llbracket \Gamma \rrbracket. \llbracket \Gamma; [\varphi_1] \rrbracket. \llbracket \Gamma, \varphi_1; [\varphi_2] \rrbracket = \llbracket \Gamma; \llbracket \Gamma; [\varphi_1 \wedge \varphi_2] \rrbracket \rrbracket.$$

After defining formally the interpretation of contexts in section 2.5, the last three equations will be respectively  $\llbracket \Gamma, \mathbf{True} \rrbracket$ ,  $\llbracket \Gamma, \mathbf{False} \rrbracket$  and  $\llbracket \Gamma, \varphi_1 \wedge \varphi_2 \rrbracket$ .

We need not give an ad-hoc semantics to path types (like in [CCHM15]), since they are a derived notion in our theory. We will indeed show how to model them in section 2.4.2, as they are defined using restriction types.

## 2.4.2 Modelling partial and restriction types

In this section we show how to model partial and restriction types in cubical sets. First note that by using the subobject classifier  $\Omega$  (see appendix B), which is available in any presheaf category, we can define a natural transformation  $\hat{\cdot} : \mathbb{F} \rightarrow \Omega$  such that for any  $I \in \mathcal{C}$ , each  $\varphi \in \mathbb{F}(I)$  is sent into the sieve  $\hat{\varphi} \in \Omega(I)$  of all the  $f : I \rightarrow J$  that make  $\varphi$  true, i.e.  $\varphi f = \mathbf{True}$ ; indeed, if  $h : J \rightarrow K$ , then  $\varphi(fh) = (\varphi f)h = \mathbf{True}h = \mathbf{True}$ , so that  $fh \in \hat{\varphi}$ .<sup>87</sup>

Now we define partial types, systems and restriction types.

- Given a type  $\Gamma \vdash A$  and a formula  $\Gamma \vdash \varphi : \mathbb{F}$ , we define  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; [\varphi]A \rrbracket : \mathbf{U}_0$  to be (the code for) the function type  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; [\varphi] \rrbracket \rightarrow \llbracket \Gamma; A \rrbracket$ , i.e.<sup>88</sup>

$$\llbracket \Gamma; [\varphi]A \rrbracket = \ulcorner \Pi_{\text{El } \llbracket \Gamma; [\varphi] \rrbracket} \text{El } \llbracket \Gamma; A \rrbracket \urcorner$$

More explicitly, as explained in section 2.2.1, each set  $(\Pi_{\text{El } \llbracket \Gamma; [\varphi] \rrbracket} \text{El } \llbracket \Gamma; A \rrbracket)\rho = (\text{El } \llbracket \Gamma; [\varphi]A \rrbracket)\rho$  is given by families

$$u = (u_f \in \text{El } \llbracket \Gamma; A \rrbracket(\rho f) \mid \llbracket \Gamma; \varphi \rrbracket \rho f = \mathbf{True}, (u_f)g = u_{fg} \forall g : K \rightarrow J)_{f:J \rightarrow I}$$

- Systems  $\Gamma \vdash [\vec{\psi} \mapsto \vec{t}] : [\vec{\psi}]A$  are interpreted as follows: each  $\llbracket \Gamma; [\vec{\psi} \mapsto \vec{t}] \rrbracket \rho$  is given by the family

$$((t_i \rho)_f \mid \llbracket \Gamma; \psi_i \rrbracket \rho f = \mathbf{True}, (t_i \rho)_{fg} = (t_i \rho)_f g \forall g : K \rightarrow J)_{f:J \rightarrow I, i=1 \dots n}$$

where each  $(t_i \rho)_f$  is given by the term  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; t_i \rrbracket : \text{El } \llbracket \Gamma; [\psi_i]A \rrbracket$ ; we assume the uniqueness condition  $\llbracket \Gamma; t_i \rrbracket \rho = \llbracket \Gamma; t_j \rrbracket \rho$  for each  $\rho \in \Gamma(I)$  such that  $\llbracket \Gamma; \psi_i \wedge \psi_j \rrbracket \rho = \mathbf{True}$ , which assures that the definition is well-posed.

<sup>87</sup>Pay attention to the fact that cubical sets are covariant functors, so that arrows get reversed in sieves. More generally, arrows get reversed when one uses the presheaf model notation in the special case of cubical sets.

<sup>88</sup>Remember that the  $\llbracket \cdot \rrbracket$  interpretation of a type shall be a term of  $\mathbf{U}_0$  and not a type itself. We need therefore to work with the encoding and decoding functions of  $\mathbf{U}_0$ .

- Lastly, for restriction types of the form  $\Gamma \vdash [\vec{\psi} \mapsto \vec{t}]A$ , we define  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; [\vec{\psi} \mapsto \vec{t}]A \rrbracket : \mathbf{U}_0$ , putting

$$\llbracket \Gamma; [\vec{\psi} \mapsto \vec{t}]A \rrbracket = \ulcorner \text{Restr}([\vec{\psi} \mapsto \vec{t}], A) \urcorner,$$

with  $\text{Restr}([\vec{\psi} \mapsto \vec{t}], A)\rho$  being the subset of the  $u \in \text{El } \llbracket \Gamma; A \rrbracket \rho$  such that  $uf = (t_i\rho)_f$  for each  $i$  and  $f : J \rightarrow I$  such that  $\llbracket \Gamma; \psi_i \rrbracket \rho f = \text{True}$ . The map  $\text{Restr}([\vec{\psi} \mapsto \vec{t}], A)\rho \rightarrow \text{Restr}([\vec{\psi} \mapsto \vec{t}], A)(\rho h)$ , for  $h : J \rightarrow I$ , is the induced map  $\text{El } \llbracket \Gamma; A \rrbracket \rho \rightarrow \text{El } \llbracket \Gamma; A \rrbracket (\rho h)$ ,  $u \mapsto uh$ , because if  $(\llbracket \Gamma; \psi_i \rrbracket \rho h)f = \text{True}$  for  $f : K \rightarrow J$ , then  $(\llbracket \Gamma; \psi_i \rrbracket \rho)(hf) = \text{True}$  and so  $(uh)f = u(hf) = (t_i\rho)_{hf} = (t_i\rho)(hf) = (t_i\rho h)f$ .

Having described the semantics of partial and restriction types, we can now show how path types (that is, of the form  $\Gamma \vdash [i : \mathbb{I}][i = 0 \mapsto u, i = 1 \mapsto v]A : \mathbf{U}$ ) are modelled.<sup>89</sup> Suppose we have this derivation in the type theory:

$$\frac{\Gamma, i : \mathbb{I} \vdash A : \mathbf{U} \quad \Gamma, i : \mathbb{I} \vdash u : [i = 0]A \quad \Gamma, i : \mathbb{I} \vdash v : [i = 1]A}{\frac{\Gamma, i : \mathbb{I} \vdash [i = 0 \mapsto u, i = 1 \mapsto v]A : \mathbf{U}}{\Gamma \vdash [i : \mathbb{I}][i = 0 \mapsto u, i = 1 \mapsto v]A : \mathbf{U}} \text{ (Pi-}\mathbb{I}\text{)}} \text{ (Restr-U)}$$

First, given  $I \in \mathcal{C}$ , note what the context extension  $\llbracket \Gamma.\mathbb{I} \rrbracket$  looks like:

$$\llbracket (\Gamma.\mathbb{I}) \rrbracket(I) = (\llbracket \Gamma \rrbracket.\mathbb{I})(I) = \{(\rho, z) \mid \rho \in \llbracket \Gamma \rrbracket(I), z \in \mathbb{I}\rho = \mathbb{I}(I) = I \cup \{0, 1\}\}.$$

From  $\Gamma, i : \mathbb{I} \vdash u : [i = 0]A$ , for each  $\rho \in \llbracket \Gamma \rrbracket(I)$  and  $z \in \mathbb{I}(I)$  we get a family  $\tilde{u}(\rho, z) \equiv \llbracket \Gamma, i : \mathbb{I}; u \rrbracket(\rho, z)$  composed by

$$(\tilde{u}(\rho, z)_f \mid (i = 0)(\rho, z)f = \text{True}, \tilde{u}(\rho, z)_{fg} = \tilde{u}(\rho, z)_{fg} \forall g : K \rightarrow J)_{f : J \rightarrow I}$$

Note that

$$(i = 0)(\rho, z)f = \text{True} \iff zf = 0 \iff f(z) = 0$$

And similarly  $(i = 1)(\rho, z)f = \text{True} \iff f(z) = 1$ .<sup>90</sup>

Therefore  $\tilde{u}$  is given by families

$$\tilde{u}(\rho, z) = (\tilde{u}(\rho, z)_f \mid f(z) = 0, \tilde{u}(\rho, z)_{fg} = \tilde{u}(\rho, z)_{fg} \forall g : K \rightarrow J)_{f : J \rightarrow I}$$

<sup>89</sup>Of course we assume the soundness theorem (2.15). This example should be made after stating the theorem, but we expound it here for a clearer presentation.

<sup>90</sup>Pay attention not to confuse the symbols  $0/1$  (syntactical components of formulas) and  $0/1$  (elements of the semantic unit interval  $\mathbb{I}(I)$ ). Likewise,  $i = 0$  is a syntactical formula,  $(i = 0)$  is a morphism in the category of cubes.

Analogously for  $\Gamma, i : \mathbb{I} \vdash v : [i = 0]A$ , from which we obtain  $\tilde{v}$ .

This means that  $\text{El} \llbracket \Gamma, i : \mathbb{I}; [i = 0 \mapsto u, i = 1 \mapsto v]A \rrbracket$  is given by the elements  $s \in \text{El} \llbracket \Gamma, i : \mathbb{I}; A \rrbracket(\rho, z)$  such that

$$sf = \begin{cases} \tilde{u}(\rho, z)_f & \forall f : J \rightarrow I \text{ such that } f(z) = 0 \\ \tilde{v}(\rho, z)_f & \forall f : J \rightarrow I \text{ such that } f(z) = 1 \end{cases}$$

To get  $\llbracket \Gamma; [i : \mathbb{I}][i = 0 \mapsto u, i = 1 \mapsto v]A \rrbracket$  from  $\llbracket \Gamma, i : \mathbb{I}; [i = 0 \mapsto u, i = 1 \mapsto v]A \rrbracket$  one simply has to follow the construction of  $\lambda(\cdot)$  given in 2.2.1.

## 2.5 Interpretation of the syntax

Lastly we give the definition of the semantic interpretation of the syntax into the CwF of cubical sets, extending what we have done for formulas. We follow closely [CCHM15].<sup>91</sup> We assume two Grothendieck universes  $\mathbf{Set}_0 \in \mathbf{Set}_1$  which give rise to two semantic universes  $\mathbf{U}_0$  and  $\mathbf{U}_1$  (called respectively small and large); the latter is used to define the interpretation of  $\mathbf{U}$ , since  $\vdash_s \mathbf{U}_0 : \mathbf{U}_1$ .

It is important to remark that what is being defined is an a priori *partial* interpretation of *raw* contexts and terms (also called pre-contexts/terms),<sup>92</sup> and only afterwards, in the soundness theorem, it is shown that the interpretation is defined and correct for every well-typed context or term.

First we define the interpretation of (syntactical) contexts, that is we associate to each context  $\Gamma$  a cubical set  $\llbracket \Gamma \rrbracket$ . The recursive definitions given below have to be understood such that the interpretation of the left-hand side is defined whenever all the interpretations in the right-hand side are defined and make sense.

$$\begin{aligned} \llbracket () \rrbracket &= \mathbb{1} \\ \llbracket \Gamma, i : \mathbb{I} \rrbracket &= \llbracket \Gamma \rrbracket.\mathbb{I} \\ \llbracket \Gamma, x : A \rrbracket &= \llbracket \Gamma \rrbracket.\text{El} \llbracket \Gamma; A \rrbracket \\ \llbracket \Gamma, \varphi \rrbracket &= \llbracket \Gamma \rrbracket.\llbracket \Gamma; [\varphi] \rrbracket \end{aligned}$$

<sup>91</sup>See also [Str91] for a broader and deeper treatment of type theory semantics. In particular, in chapter 3 it is explained how to properly and formally give the recursive definition of  $\llbracket \cdot \rrbracket$ , by first defining a ‘depth’ function on terms and contexts; by doing so, the given interpretation of a context/term of height  $d+1$  depends only on the interpretation of contexts/terms of height  $\leq d$ .

<sup>92</sup>Here by ‘term’ we mean a syntactical object which is not a context, e.g. a term in the narrower sense, a type, the universe or a formula. Recall that in dependent type theory the set of well formed terms and types cannot be defined independently from the context and the rules (and indeed that’s why here we use the word ‘term’ in a broader sense).



$$\llbracket \Gamma, x : A = t \rrbracket = \llbracket \Gamma \rrbracket$$

Then we define the interpretation of terms, associating to each (syntactical) term  $t$  in context  $\Gamma$  a family of sets  $\llbracket \Gamma; t \rrbracket \rho$  for each  $I \in \mathcal{C}$  and  $\rho \in \Gamma(I)$ . What we want to obtain is that if  $\Gamma \vdash A : \mathbb{U}$  in the type theory, then  $\llbracket \Gamma; A \rrbracket \in \mathbf{Term}(\llbracket \Gamma \rrbracket; \mathbb{U}_0)$ , so that  $\mathbf{El} \llbracket \Gamma; A \rrbracket \in \mathbf{Type}(\llbracket \Gamma \rrbracket)$ , and similarly if  $\Gamma \vdash a : A$  in the type theory, then  $\llbracket \Gamma; t \rrbracket \in \mathbf{Type}(\llbracket \Gamma \rrbracket; \mathbf{El} \llbracket \Gamma; A \rrbracket)$ .

First we define the interpretation of the universe.

$$\llbracket \Gamma; \mathbb{U} \rrbracket = \ulcorner \mathbb{U}_0 \urcorner \in \mathbf{Term}(\llbracket \Gamma \rrbracket; \mathbb{U}_1)$$

For variables, we define it by recursion on the structure of the context.

$$\begin{aligned} \llbracket \Gamma, x : A; x \rrbracket \rho &= \mathbf{q}(\rho) & \llbracket \Gamma, \varphi; x \rrbracket &= \llbracket \Gamma; x \rrbracket \\ \llbracket \Gamma, y : A; x \rrbracket \rho &= \llbracket \Gamma; x \rrbracket (\mathbf{p}(\rho)) & \llbracket \Gamma, x : A = t; x \rrbracket &= \llbracket \Gamma; t \rrbracket \\ \llbracket \Gamma, i : \mathbb{I}; x \rrbracket \rho &= \llbracket \Gamma; x \rrbracket (\mathbf{p}(\rho)) & \llbracket \Gamma, y : A = t; x \rrbracket \rho &= \llbracket \Gamma; x \rrbracket \rho \end{aligned}$$

$\Pi$ -types (of which path types are a particular case).

$$\begin{aligned} \llbracket \Gamma; [x : A] B \rrbracket &= \ulcorner \Pi_{\mathbf{El} \llbracket \Gamma; A \rrbracket} (\mathbf{El} \llbracket \Gamma, x : A; B \rrbracket) \urcorner \\ \llbracket \Gamma; [i : \mathbb{I}] B \rrbracket &= \ulcorner \Pi_{\mathbb{I}} (\mathbf{El} \llbracket \Gamma, i : \mathbb{I}; B \rrbracket) \urcorner \\ \llbracket \Gamma; [x : A] t \rrbracket &= \lambda \llbracket \Gamma, x : A; t \rrbracket \\ \llbracket \Gamma; t \ u \rrbracket &= \mathbf{app} (\llbracket \Gamma; t \rrbracket, \llbracket \Gamma; u \rrbracket) \end{aligned}$$

$\Sigma$ -types.

$$\begin{aligned} \llbracket \Gamma; \langle x : A \rangle B \rrbracket &= \ulcorner \Sigma_{\mathbf{El} \llbracket \Gamma; A \rrbracket} (\mathbf{El} \llbracket \Gamma, x : A; B \rrbracket) \urcorner \\ \llbracket \Gamma; (t, u) \rrbracket \rho &= (\llbracket \Gamma; t \rrbracket \rho, \llbracket \Gamma; u \rrbracket \rho) \\ \llbracket \Gamma; t.1 \rrbracket \rho &= \pi_1 (\llbracket \Gamma; t \rrbracket \rho) \\ \llbracket \Gamma; t.2 \rrbracket \rho &= \pi_2 (\llbracket \Gamma; t \rrbracket \rho) \end{aligned}$$

Naturals; we assume that in the CwF we have a type **Nat** with constructors **zero** and **succ**, along with an induction principle **ind**, which we omit for brevity.<sup>93</sup>

$$\begin{aligned} \llbracket \Gamma; \mathbb{N} \rrbracket &= \ulcorner \mathbf{Nat} \urcorner \\ \llbracket \Gamma; Z \rrbracket &= \mathbf{zero} \\ \llbracket \Gamma; S \ t \rrbracket \rho &= \mathbf{succ} (\llbracket \Gamma; t \rrbracket \rho) \end{aligned}$$

<sup>93</sup>It requires some sophistication to write the induction principle in the CwF rules syntax. See [Hof97] for a formalization of naturals in CwFs.

Interval and the endpoints.<sup>94</sup>

$$\llbracket \Gamma; \mathbb{I} \rrbracket = \mathbb{I} \quad \llbracket \Gamma; 0 \rrbracket \rho = 0 \in \mathbb{I}(I) \quad \llbracket \Gamma; 1 \rrbracket \rho = 1 \in \mathbb{I}(I)$$

Formulas, systems, partial and restriction types are interpreted as explained in section 2.4.2, which means that the definition of

$$\llbracket \Gamma; \varphi \rrbracket \quad \llbracket \Gamma; [\vec{\psi} \mapsto \vec{t}] \rrbracket \quad \llbracket \Gamma; [\varphi]A \rrbracket \quad \llbracket \Gamma; [\vec{\psi} \mapsto \vec{t}]A \rrbracket$$

is given, completing the definition of  $\llbracket \Gamma; t \rrbracket$  for any  $t$ .

We can now state the soundness theorem, which should be proved by induction on the constructions/derivations, using some suitable lemmas (i.e. weakening and substitution lemmas), as stated in [CCHM15] and proved in [Str91].

**Theorem 2.15** (Soundness theorem). *The following hold:*

1. *If  $\Gamma$  is a context, then  $\llbracket \Gamma \rrbracket$  is a cubical set;*
2. *If  $\Gamma \vdash A : \mathbb{U}$ , then  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; A \rrbracket : \mathbb{U}_0$ ;*
3. *If  $\Gamma \vdash a : A$ , then  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; a \rrbracket : El \llbracket \Gamma; A \rrbracket$ ;*
4. *If  $\Gamma \vdash i : \mathbb{I}$ , then  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; i \rrbracket : \mathbb{I}$ ;*
5. *If  $\Gamma \vdash \varphi : \mathbb{F}$ , then  $\llbracket \Gamma \rrbracket \vdash_s \llbracket \Gamma; \varphi \rrbracket : \mathbb{F}$ ;*
6. *If  $s \sim^\Gamma t$ , then  $\llbracket \Gamma; s \rrbracket = \llbracket \Gamma; t \rrbracket$ .*

---

<sup>94</sup>We have already remarked that we use  $\mathbb{I}$  both as a formal symbol and as the cubical set which interprets it.

# Chapter 3

## Implementation

In this chapter we discuss the actual software implementation of the type theory described in chapter 1, using the Haskell programming language.

The full code can be found at <https://github.com/mattia-furlan/MasterThesisCTT>.

We use the tools Alex and Happy to handle the lexical analyzer and the parser.<sup>95</sup> Instead of writing them from scratch, we initially wrote a simple grammar using the BNFC tool, which then automatically produces the files (one `.x` and one `.y`) which are given in input to Alex and Happy.<sup>96</sup>

The files which do all the main work are the following:<sup>97</sup>

- In `Interval.hs` we define formulas and the directions environment structure, along with all the utility functions needed to handle them (e.g. updating the directions environment, substitution in a formula).
- In `CoreCTT.hs` we define the abstract syntax of terms and values, the context and the functions which check term shadowing.
- In `Eval.hs` we implement the evaluation function for terms and formulas, with an handler for each type eliminator (e.g. function application, projections). Moreover, there we also implement the printing functions and the read-back procedure.

---

<sup>95</sup>Alex and Happy are the Haskell version of the celebrated Lex and Yacc for C.

<sup>96</sup>BNFC is useful especially for the lexer, as it does under the hood all the hard-work of treating special characters and Unicode. Moreover, from the basic parser produced by BNFC one obtains a sketch which will then be refined manually, handling for example the shift/reduce conflicts.

<sup>97</sup>Listed in order of dependencies (e.g. `TypeChecker.hs` needs `Interval.hs`, `CoreCTT.hs`, `Eval.hs` and `Conv.hs`).

- In `Conv.hs` we implement the the convertibility (i.e.  $\alpha\eta$ -conversion) predicate.
- In `TypeChecker.hs` we implement the bidirectional type-checker, with one function for type-inference and one for type-checking. We also handle type-checking under a formula.
- In `MainCTT.hs` we implement the main REPL loop which reads declarations from the input (or from some files) and processes them.

### 3.1 Lexical analysis and parsing

As explained in the introduction of the chapter, we use a lexer automatically generated by BNFC, which we don't report here due to the excess of technical details.<sup>98</sup> Instead we give here the code for the parser, initially generated by BNFC and then refined manually. The syntax that the parser recognizes is the one shown in chapter 1, allowing also multiple identifiers in abstractions (e.g. one can write  $[a, b, c : A] B$  instead of  $[a : A][b : A][c : A] B$ ).

The abstract syntax is defined in `CoreCTT.hs` for terms and top-levels, and in `Interval.hs` for formulas.

All the files use a wrapper data structure for strings, called `Ident`, defined in the homonym file.

Source file `Ident.hs`.

```
{-# LANGUAGE GeneralizedNewtypeDeriving #-}

module Ident where

import Data.String

newtype Ident = Ident String
  deriving (Eq, Ord, IsString)

instance Show Ident where
  show (Ident s) = s
```

Source file `ParCTT.y`.

```
{
module ParCTT ( happyError, myLexer, pProgram, pToplevel, pTerm )
where
```

---

<sup>98</sup>The file is `LexCTT.x`.

```

import Prelude
import qualified Data.Map as Map

import Ident
import qualified CoreCTT
import Interval
import LexCTT
}

%name pProgram Program
%name pToplevel Toplevel
%name pTerm Term
%monad { Err } { (>>=) } { return }
%tokentype {Token}
%token
  '(' { PT _ (TS _ 1) }
  ')' { PT _ (TS _ 2) }
  '*' { PT _ (TS _ 3) }
  '+' { PT _ (TS _ 4) }
  ',' { PT _ (TS _ 5) }
  '->' { PT _ (TS _ 6) }
  '.1' { PT _ (TS _ 7) }
  '.2' { PT _ (TS _ 8) }
  '/\\' { PT _ (TS _ 9) }
  '0' { PT _ (TS _ 10) }
  '1' { PT _ (TS _ 11) }
  ':' { PT _ (TS _ 12) }
  ';' { PT _ (TS _ 13) }
  '<' { PT _ (TS _ 14) }
  '=' { PT _ (TS _ 15) }
  '>' { PT _ (TS _ 16) }
  'I' { PT _ (TS _ 17) }
  'N' { PT _ (TS _ 18) }
  'S' { PT _ (TS _ 19) }
  'U' { PT _ (TS _ 20) }
  'Z' { PT _ (TS _ 21) }
  '[' { PT _ (TS _ 22) }
  '\\/' { PT _ (TS _ 23) }
  ']' { PT _ (TS _ 24) }
  'comp' { PT _ (TS _ 25) }
  'ind' { PT _ (TS _ 26) }
  'inl' { PT _ (TS _ 27) }
  'inr' { PT _ (TS _ 28) }
  'split' { PT _ (TS _ 29) }
  '|' { PT _ (TS _ 30) }
  L_Ident { PT _ (TV $$) }

%%

```

```

Ident :: { Ident }
Ident  : L_Ident { Ident $1 }

ListIdent :: { [Ident] }
ListIdent : Ident { [$1] }
           | Ident ',' ListIdent { (:) $1 $3 }

Program :: { CoreCTT.Program }
Program : ListToplevel { CoreCTT.Program $1 }

Term :: { CoreCTT.Term }
Term  : Term1 '->' Term { CoreCTT.Abst (Ident "") $1 $3 }
       | '[' Ident ':' Term '=' Term ']' Term { CoreCTT.TDef ($2,$4,$6) $8 }
       | '[' Ident ':' Term ']' Term { CoreCTT.Abst $2 $4 $6 }
       | '[' ListIdent ':' Term ']' Term
         { foldr (\i e -> CoreCTT.Abst i $4 e) $6 $2 }
       | Term1 { $1 }

Term1 :: { CoreCTT.Term }
Term1 : Term2 '+' Term1 { CoreCTT.Sum $1 $3 }
       | Term2 '*' Term1 { CoreCTT.Sigma (Ident "") $1 $3 }
       | '<' ListIdent ':' Term '>' Term
         { foldr (\i e -> CoreCTT.Sigma i $4 e) $6 $2 }
       | '[' DisjFormula ']' Term1 { CoreCTT.Partial $2 $4 }
       | System Term1 { CoreCTT.Restr $1 $2 }
       | Term2 ',' Term2 { CoreCTT.Pair $1 $3 }
       | Term2 { $1 }

Term2 :: { CoreCTT.Term }
Term2 : Term2 Term3 { CoreCTT.App $1 $2 }
       | 'ind' Term3 Term3 Term3 Term3 { CoreCTT.Ind $2 $3 $4 $5 }
       | 'comp' Term3 '(' DisjFormula ')' Term3 Term3 Term3 Term3
         { CoreCTT.Comp $2 $4 $6 $7 $8 $9 }
       | 'comp' Term3 '(' ' ' ')' Term3 Term3 Term3 Term3
         { CoreCTT.Comp $2 fFalse $5 $6 $7 $8 }
       | 'S' Term3 { CoreCTT.Succ $2 }
       | 'inl' Term3 { CoreCTT.InL $2 }
       | 'inr' Term3 { CoreCTT.InR $2 }
       | 'split' Term3 Term3 Term3 Term3 { CoreCTT.Split $2 $3 $4 $5 }
       | Term3 { $1 }

Term3 :: { CoreCTT.Term }
Term3 : Ident { CoreCTT.Var $1 }
       | 'U' { CoreCTT.Universe }
       | 'N' { CoreCTT.Nat }
       | 'Z' { CoreCTT.Zero }
       | 'I' { CoreCTT.I }
       | Term3 '.1' { CoreCTT.Fst $1 }
       | Term3 '.2' { CoreCTT.Snd $1 }

```

```

    | System { CoreCTT.Sys $1 }
    | '0' { CoreCTT.I0 }
    | '1' { CoreCTT.I1 }
    | '(' Term ')' { $2 }

Toplevel :: { CoreCTT.Toplevel }
Toplevel : Ident ':' Term '=' Term { CoreCTT.Definition $1 $3 $5 }
         | Ident ':' Term { CoreCTT.Declaration $1 $3 }
         | Term { CoreCTT.Example $1 }

ListToplevel :: { [CoreCTT.Toplevel] }
ListToplevel : {- empty -} { [] }
              | Toplevel ';' ListToplevel { (:) $1 $3 }

AtomicFormula :: { AtomicFormula }
AtomicFormula : Ident '=' '0' { Eq0 $1 }
              | Ident '=' '1' { Eq1 $1 }
              | Ident '=' Ident { Diag $1 $3 }

ConjFormula1 :: { [AtomicFormula] }
ConjFormula1 : AtomicFormula { [$1] }
              | AtomicFormula '/' ConjFormula1 { $1 : $3 }

ConjFormula :: { ConjFormula }
ConjFormula : ConjFormula1 { Conj $1 }
             | '(' ConjFormula ')' { $2 }

DisjFormula1 :: { [ConjFormula] }
DisjFormula1 : ConjFormula { [$1] }
              | ConjFormula '\\' DisjFormula1 { $1 : $3 }

DisjFormula :: { DisjFormula }
DisjFormula : DisjFormula1 { Disj $1 }

System :: { CoreCTT.System }
System : '[' ListSysElem ']' { $2 }

SysElem :: { (ConjFormula,CoreCTT.Term) }
SysElem : ConjFormula '->' Term { ($1,$3) }

ListSysElem :: { [(ConjFormula,CoreCTT.Term)] }
ListSysElem : {- empty -} { [] }
             | SysElem { [$1] }
             | SysElem '|' ListSysElem { $1 : $3 }

{
type Err = Either String

```

```

happyError :: [Token] -> Err a
happyError ts = Left $
  "syntax error at " ++ tokenPos ts ++
  case ts of
    []      -> []
    [Err _] -> " due to lexer error"
    t:_     -> " before `" ++ (prToken t) ++ "'"

myLexer :: String -> [Token]
myLexer = tokens
}

```

## 3.2 Interval and formulas

In this file first we define three types of formulas: atomic ones (of the kind  $i = 0$ ,  $i = 1$  or  $i = j$ ), conjunctive ones (that is, lists of atomic formulas) and disjunctive ones (that is, lists of conjunctive formulas).<sup>99</sup> Next we define the directions environment structure, called `DirEnv`, made of three fields: one storing the variables set to zero, one storing the variables set to one, and the last one storing the equivalence classes of ‘diagonals’ (see section 1.2.3). We then implement some utility functions needed to work with directions environments, as adding a conjunction, checking if such a structure makes a formula true, etc.

Source file `Interval.hs`.

```

{-# LANGUAGE FlexibleInstances #-}

module Interval where

import Data.List (intercalate,delete)
import Ident

-- Atomic formulas are of the kind `i = 0`, `i = 1` or `i = j`
data AtomicFormula
  = Eq0 Ident
  | Eq1 Ident
  | Diag Ident Ident
  deriving (Ord)

-- Equality between atomic formulas
instance Eq AtomicFormula where
  af1 == af2 = case (af1,af2) of

```

<sup>99</sup>More precisely, the last type are the formulas in disjunctive normal form.



```

(Eq0 s1,Eq0 s2) -> s1 == s2
(Eq1 s1,Eq1 s2) -> s1 == s2
(Diag s1 s2,Diag s3 s4) -> (s1 == s3 && s2 == s4)
  || (s1 == s4 && s2 == s3)
otherwise -> False

-- A conjunctive formula is a list of atomic formulas
newtype ConjFormula = Conj [AtomicFormula]
  deriving (Eq,Ord)

-- A disjunctive formula is a list of conjunctive formulas
newtype DisjFormula = Disj [ConjFormula]
  deriving (Eq,Ord)

{- Pretty printing of atomic/conjunctive/disjunctive formulas -}

instance Show AtomicFormula where
  show af = case af of
    Eq0 s -> show s ++ " = 0"
    Eq1 s -> show s ++ " = 1"
    Diag s1 s2 -> show s1 ++ " = " ++ show s2

instance Show ConjFormula where
  show (Conj cf)
    | null cf    = "True"
    | otherwise = intercalate " /\ \" (map show cf)

instance Show DisjFormula where
  show disj@(Disj df)
    | disj == fFalse = "False"
    | disj == fTrue  = "True"
    | otherwise      = intercalate " \/ \" $
      map (\cf -> "(" ++ show cf ++ ")") df

{- Helpers -}

-- True (disjunctive) formula: just one empty conjunction
fTrue :: DisjFormula
fTrue = Disj [Conj []]

-- False formula: empty disjunction
fFalse :: DisjFormula
fFalse = Disj []

isTrue :: DisjFormula -> Bool
isTrue = (== fTrue)

isFalse :: DisjFormula -> Bool
isFalse = (== fFalse)

```

```

isTrueConj :: ConjFormula -> Bool
isTrueConj (Conj cf) = null cf

{- Implication and equivalence -}

{- A disjunctive formula implies another one if each of its conjunctions
    makes the second formula true. The case where the second formula is false
    must be handled separately. The first two checks are unnecessary, used only
    for efficiency -}
impDisj :: DirEnv -> DisjFormula -> DisjFormula -> Bool
impDisj dirs (Disj df1) disj2 = isFalse (Disj df1) || isTrue disj2 ||
    if isFalse disj2 then
        all (inconsistent . addConj dirs) df1 -- First formula must be false
    else
        all (\cf1 -> addConj dirs cf1 `makesTrueDisj` disj2) df1

-- Two formulas are equal if each one imply the other
eqFormulas :: DirEnv -> DisjFormula -> DisjFormula -> Bool
eqFormulas dirs disj1 disj2 = impDisj dirs disj1 disj2 && impDisj dirs disj2 disj1

{- Directions environment -}

-- A `DirEnv` stores the list of zeros, ones and the diagonals partitions
type DirEnv = ([Ident],[Ident],[[Ident]])

emptyDirEnv :: DirEnv
emptyDirEnv = ([],[],[[]])

-- A `DirEnv` is inconsistent if there is an identifier
-- which is set both to zero and one
inconsistent :: DirEnv -> Bool
inconsistent (zeros,ones,diags) =
    any (`elem` ones) zeros || any (`elem` zeros) ones

-- Find the partition which contains `s`, if it exists.
-- Otherwise return the fake partition [s]
findPartition :: [[Ident]] -> Ident -> [Ident]
findPartition diags s = case filter (s `elem`) diags of
    [] -> [s]
    l -> head l

-- Set an identifier to zero. Any eventual identifier which is in the same
-- partition must then be set to zero, and that partition is removed
addZero :: DirEnv -> Ident -> DirEnv
addZero (zeros,ones,diags) s =
    let toadd = findPartition diags s
    in (toadd ++ zeros,ones,delete toadd diags)

```

```

-- Set an identifier to one. Any eventual identifier which is in the same
-- partition must then be set to one, and that partition is removed
addOne :: DirEnv -> Ident -> DirEnv
addOne (zeros,ones,diags) s =
  let toadd = findPartition diags s
  in (zeros,toadd ++ ones,delete toadd diags)

-- Add a new diagonal `s1 = s2`
addDiag :: DirEnv -> Ident -> Ident -> DirEnv
addDiag dirs@(zeros,ones,diags) s1 s2
  | s1 == s2          = dirs          -- Trivial, nothing to do
  | s1 `elem` zeros    = addZero dirs s2 -- `s1` already zero -> set `s2` to zero
  | s2 `elem` zeros    = addZero dirs s1 -- `s2` already zero -> set `s1` to zero
  | s1 `elem` ones     = addOne  dirs s2 -- `s1` already one  -> set `s2` to one
  | s2 `elem` ones     = addOne  dirs s1 -- `s2` already one  -> set `s1` to zero
  | otherwise          = let
    -- Add `s1` and `s2` to the existing partitions if it's the case:
    -- it means that e.g if partition `set` contains `s1`, then `s2`
    -- shall be added to `set` too
    diags' = [if s1 `elem` set then s2 : set else if s2 `elem` set then s1 : set
              else set | set <- diags]
    -- Add a new partition if `s1` and `s2` are new (= not found in the partitions)
    diags'' = diags' ++
      [[s1,s2] | not (s1 `elem` concat diags' || s2 `elem` concat diags')]
    par1 = findPartition diags'' s1
    par2 = findPartition diags'' s2
    -- Eventually join the two partitions
    -- (e.g. [i,k] [j,k,l] gets joined into [i,j,k,l])
    diags''' = if par1 /= par2 then
      delete par2 (delete par1 diags'') ++ [par1 ++ par2]
    else
      diags''
  in (zeros,ones,diags''')

-- Add a conjunction to a `DirEnv`
addConj :: DirEnv -> ConjFormula -> DirEnv
addConj dirs (Conj conj) = foldl addAtomic dirs conj
  where
    addAtomic :: DirEnv -> AtomicFormula -> DirEnv
    addAtomic dirs' ff = case ff of
      Eq0 s      -> addZero dirs' s
      Eq1 s      -> addOne  dirs' s
      Diag s s'  -> addDiag dirs' s s'

-- Conversion from a conjunction to a `DirEnv`
conjToDirEnv :: ConjFormula -> DirEnv
conjToDirEnv = addConj emptyDirEnv

-- Test if a `DirEnv` makes an atomic formula true.

```

```

-- A diagonal is true iff both are zero, or both are true, or if
-- they are in the same partition
makesTrueAtomic :: DirEnv -> AtomicFormula -> Bool
(zeros,ones,diags) `makesTrueAtomic` af = case af of
  Eq0 s -> s `elem` zeros
  Eq1 s -> s `elem` ones
  Diag s1 s2 -> s1 == s2 || bothIn zeros || bothIn ones || any bothIn diags
    where bothIn set = s1 `elem` set && s2 `elem` set

-- A conjunction is true iff all of its atomic formulas are true
makesTrueConj :: DirEnv -> ConjFormula -> Bool
makesTrueConj dirs (Conj cf) = all (dirs `makesTrueAtomic`) cf

-- A disjunction is true iff one of its conjunctive formulas is true
makesTrueDisj :: DirEnv -> DisjFormula -> Bool
makesTrueDisj dirs (Disj df) = any (dirs `makesTrueConj`) df

-- Substitute `s'` for `s` in an atomic formula
substAtomic :: (Ident,Ident) -> AtomicFormula -> AtomicFormula
substAtomic (s,s') af = case af of
  Eq0 x | s == x -> Eq0 s'
  Eq1 x | s == x -> Eq1 s'
  Diag x y -> Diag (if x == s then s' else x) (if y == s then s' else y)
  otherwise -> af

-- Substitute into each atomic formula of the conjunction
substConj :: (Ident,Ident) -> ConjFormula -> ConjFormula
substConj (s,s') (Conj cf) = Conj $ map (substAtomic (s,s')) cf

-- Concatenation (logical AND) between two conjunctive formulas
meet :: ConjFormula -> ConjFormula -> ConjFormula
(Conj cf1) `meet` (Conj cf2) = Conj $ cf1 ++ cf2

```

### 3.3 Core language

In this file we first define the abstract syntax for terms/values and for top-levels (i.e. declarations, definitions and examples). We then define some functions to handle these syntactical aspects, e.g. getting free variables and checking eventual term shadowing. Next we define contexts as lists of pairs of the form  $(s, \text{Decl } ty)$ ,  $(s, \text{Def } ty \text{ def})$  or  $(s, \text{Val } v)$ , along with some utility functions.

Source file CoreCTT.hs.

```

{-# LANGUAGE FlexibleInstances #-}
{-# LANGUAGE LambdaCase #-}

```

```

module CoreCTT where

import Data.Maybe (fromJust)

import Ident
import Interval

{- Syntax (terms/values) -}

data Term
  = Var Ident
  | Universe
  {- Let-definition `[x:ty = e]t` -}
  | TDef (Ident,Term,Term) Term
  {-  $\Pi$  types -}
  | Abst Ident Term Term
  | App Term Term
  {-  $\Sigma$  types -}
  | Sigma Ident Term Term
  | Pair Term Term
  | Fst Term
  | Snd Term
  {- Coproducts -}
  | Sum Term Term
  | InL Term
  | InR Term
  --      fam f_0 f_1 x
  | Split Term Term Term Term
  {- Naturals -}
  | Nat
  | Zero
  | Succ Term
  --      fam c_0 c_s n
  | Ind Term Term Term Term
  {- Cubical -}
  | I | IO | I1
  | Sys System
  | Partial DisjFormula Term
  | Restr System Term
  --      fam phi i0 u base i
  | Comp Term DisjFormula Term Term Term Term
  {- For values only: -}
  | Closure Term Ctx
  --      val type
  | Neutral Value Value
  -- Just for composition (wrap a value inside a term)
  | TermV Value
deriving (Eq, Ord)

```

```

type Value = Term

newtype Program = Program [Toplevel]

data Toplevel = Definition Ident Term Term
              | Declaration Ident Term
              | Example Term
              deriving (Eq, Ord)

-- Generate a fresh name starting from 'x'
newVar :: [Ident] -> Ident -> Ident
newVar used x
  | x `elem` used = newVar used (Ident $ show x ++ "'")
  | otherwise    = x

-- For printing purposes: e.g. collectApps ((App (App f x_1) x_2) x_3) []
-- returns (f,[x_1,x_2,x_3])
collectApps :: Term -> [Term] -> (Term,[Term])
collectApps t apps = case t of
  App t1 t2' -> collectApps t1 (t2' : apps)
  otherwise  -> (t,apps)

-- Generic class for objects (terms,values,top-levels,formulas,etc.)
-- which contain variables
class SyntacticObject a where
  containsVar :: Ident -> a -> Bool
  containsVar s x = s `elem` freeVars x
  vars :: a -> [Ident]
  freeVars :: a -> [Ident]

instance SyntacticObject Ident where
  vars s = [s]
  freeVars s = [s]

instance SyntacticObject System where
  vars sys = concatMap vars (keys sys) ++ concatMap vars (elems sys)
  freeVars = vars

-- For terms only and not for values (which means we don't
-- define `vars` and `freeVars` for closures and neutral values)
instance SyntacticObject Term where
  vars = \case
    Var s          -> [s]
    Universe       -> []
    TDef (s,t,e) t' -> s : vars t ++ vars e ++ vars t'
    Abst s t e      -> s : vars t ++ vars e
    App fun arg     -> vars fun ++ vars arg
    Sigma s t e     -> s : vars t ++ vars e
    Pair t1 t2      -> vars t1 ++ vars t2

```

```

Fst t          -> vars t
Snd t          -> vars t
Sum ty1 ty2    -> vars ty1 ++ vars ty2
InL t1         -> vars t1
InR t2         -> vars t2
Split ty f1 f2 x -> vars ty ++ vars f1 ++ vars f2 ++ vars x
Nat            -> []
Zero           -> []
Succ t         -> vars t
Ind ty b s n   -> vars ty ++ vars b ++ vars s ++ vars n
I              -> []
IO             -> []
I1             -> []
Sys sys        -> vars sys
Partial phi t  -> vars phi ++ vars t
Restr sys t    -> vars sys ++ vars t
Comp fam phi i0 u b i -> vars fam ++ vars phi ++ vars i0 ++ vars u
    ++ vars b ++ vars i
TermV v        -> [] -- Dummy value (not necessary)

freeVars = \case
  Var s          -> [s]
  Universe       -> []
  TDef (s,t,e) t' -> freeVars t ++ filter (/= s)
    (freeVars e ++ freeVars t')
  Abst s t e     -> freeVars t ++ filter (/= s) (freeVars e)
  App fun arg     -> freeVars fun ++ freeVars arg
  Sigma s t e     -> freeVars t ++ filter (/= s) (freeVars e)
  Pair t1 t2      -> freeVars t1 ++ freeVars t2
  Fst t           -> freeVars t
  Snd t           -> freeVars t
  Sum ty1 ty2     -> freeVars ty1 ++ freeVars ty2
  InL t1          -> freeVars t1
  InR t2          -> freeVars t2
  Split ty f1 f2 x -> freeVars ty ++ freeVars f1 ++ freeVars f2
    ++ freeVars x
  Nat             -> []
  Zero            -> []
  Succ t          -> freeVars t
  Ind ty b s n    -> freeVars ty ++ freeVars b ++ freeVars s
    ++ freeVars n
  I              -> []
  IO              -> []
  I1              -> []
  Sys sys         -> freeVars sys
  Partial phi t   -> freeVars phi ++ freeVars t
  Restr sys t     -> freeVars sys ++ freeVars t
  Comp fam phi i0 u b i -> freeVars fam ++ freeVars phi ++ freeVars i0
    ++ freeVars u ++ freeVars b ++ freeVars i

```

```

TermV v                                -> [] -- Dummy value (not necessary)

instance SyntacticObject AtomicFormula where
  vars af = case af of
    Eq0 s      -> [s]
    Eq1 s      -> [s]
    Diag s1 s2 -> [s1,s2]
  freeVars = vars

instance SyntacticObject ConjFormula where
  vars (Conj cf) = concatMap vars cf
  freeVars = vars

instance SyntacticObject DisjFormula where
  vars (Disj df) = concatMap vars df
  freeVars = vars

checkTermShadowing :: [Ident] -> Term -> Bool
checkTermShadowing used term = case term of
  Var _      -> True
  Universe   -> True
  TDef (s,t,e) t' ->
    s `notElem` used && checkTermShadowing used t &&
    checkTermShadowing (if s == Ident "" then used else s : used) e &&
    checkTermShadowing (if s == Ident "" then used else s : used) t'
  Abst s t e -> s `notElem` used && checkTermShadowing used t &&
    checkTermShadowing (if s == Ident "" then used else s : used) e
  App fun arg -> checkTermShadowing used fun &&
    checkTermShadowing used arg
  Sigma s t e -> s `notElem` used && checkTermShadowing used t &&
    checkTermShadowing (if s == Ident "" then used else s : used) e
  Pair t1 t2 -> checkTermShadowing used t1 &&
    checkTermShadowing used t2
  Fst t -> checkTermShadowing used t
  Snd t -> checkTermShadowing used t
  Sum ty1 ty2 -> checkTermShadowing used ty1 &&
    checkTermShadowing used ty2
  InL t1 -> checkTermShadowing used t1
  InR t2 -> checkTermShadowing used t2
  Split ty f1 f2 x ->
    checkTermShadowing used ty && checkTermShadowing used f1 &&
    checkTermShadowing used f2 && checkTermShadowing used x
  Nat -> True
  Zero -> True
  Succ n -> checkTermShadowing used n
  Ind ty b s n ->
    checkTermShadowing used ty && checkTermShadowing used b &&
    checkTermShadowing used s && checkTermShadowing used n
  I -> True

```



```

I0          -> True
I1          -> True
Sys sys     -> all (checkTermShadowing used) (elems sys)
Partial _ t -> checkTermShadowing used t
Restr sys t -> all (checkTermShadowing used) (elems sys) &&
  checkTermShadowing used t
Comp fam _ i0 u b i ->
  checkTermShadowing used fam && checkTermShadowing used i0 &&
  checkTermShadowing used u && checkTermShadowing used b &&
  checkTermShadowing used i
otherwise -> error "[checkTermShadowing] got non-term"

{- Printing functions are in 'Eval.hs' -}

type ErrorString = String

{- Generic association lists utilities -}

extend :: Ctx -> Ident -> CtxEntry -> Ctx
extend ctx s e = if s == Ident "" then ctx else (s,e) : ctx

keys :: [(k,a)] -> [k]
keys = map fst

elems :: [(k,a)] -> [a]
elems = map snd

at :: (Eq k) => [(k,a)] -> k -> a
al `at` s = fromJust $ lookup s al

{- Contexts -}

type Ctx = [(Ident,CtxEntry)]

data CtxEntry = Decl Term          -- Type
              | Def Term Term      -- Type and definition
              | Val Value          -- Value binding for `eval`
  deriving (Eq, Ord)

emptyCtx :: Ctx
emptyCtx = []

-- Extract the value bindings from a context
getBindings :: Ctx -> [(Ident,Value)]
getBindings = concatMap $
  \ (s,entry) -> case entry of Val v -> [(s,v)]; _ -> []

-- Add interval value bindings of a conjunction to a context
-- It is used solely in evaluating composition for partial types

```

```

addConjBindings :: Ctx -> ConjFormula -> Ctx
addConjBindings ctx (Conj cf) = map getAtomicBinding cf ++ ctx
  where getAtomicBinding :: AtomicFormula -> (Ident,CtxEntry)
        getAtomicBinding = \case
          Eq0 s      -> (s,Val I0)
          Eq1 s      -> (s,Val I1)
          Diag s1 s2 -> (s2,Val (Neutral (Var s2) I))

-- Shall not be called with values in the context
-- (it is used only in `removeFromCtx`)
instance SyntacticObject CtxEntry where
  vars entry = case entry of
    Decl t      -> vars t
    Def ty def  -> vars ty ++ vars def
  freeVars entry = case entry of
    Decl t      -> freeVars t
    Def ty def  -> freeVars ty ++ freeVars def

-- Remove an identifier from the context and also all the others
-- (recursively) which depend on it
removeFromCtx :: Ctx -> Ident -> Ctx
removeFromCtx ctx s = if s `elem` keys ctx then
  let dep = map fst $ filter (\(_,entry) -> s `elem` freeVars entry) ctx
      ctx' = filter (\(s',_) -> s /= s') ctx
  in foldl removeFromCtx ctx' dep
else
  ctx

{- Systems -}

type System = [(ConjFormula,Term)]

-- Get the disjunction of the (conjunctive) formulas of the system
getSystemFormula :: System -> DisjFormula
getSystemFormula = Disj . map fst

-- Utility `map` function for systems: it applies a function
-- to the values inside the system
mapSys :: (Value -> Value) -> System -> System
mapSys f = map (\(psi,v) -> (psi,f v))

-- Split a type into the form [phi]A, with `phi` eventually trivial
-- It is used in the function `compTypes` of `TypeChecker.hs`
split :: Value -> (DisjFormula,Value)
split v = case v of
  Partial phi ty -> (phi,ty)
  Restr _ ty     -> (fTrue,ty)
  otherwise      -> (fTrue,v)

```

## 3.4 Evaluation

In this file we first define the evaluation function, by recursion on the structure of the terms; we also handle evaluation of formulas. Next we implement a function to handle evaluation for each type eliminator (e.g. `doApp` for function application, `doSplit` for the coproduct types eliminator), which have to handle neutral values with eventually a partial or restriction type (see 1.4). Lastly we implement the read-back function and the printing utilities.

Note that in this file the directions environment is not used, as it is needed only during type-checking and conversion, when checking under a formula on already evaluated terms.

Source file `Eval.hs`.

```
{-# LANGUAGE FlexibleInstances #-}
{-# LANGUAGE LambdaCase #-}
{-# LANGUAGE BlockArguments #-}

module Eval where

import Data.List (intercalate,nub,find)
import Data.Foldable (foldrM)
import Data.Maybe (mapMaybe,fromJust)

import Ident
import Interval
import CoreCTT

import Debug.Trace

-- For debug purposes only
debug :: Bool
debug = False

myTrace :: String -> a -> a
myTrace s x = if debug then trace s x else x

-- Retrieve the evaluated type of a variable from the context
lookupType :: Ident -> Ctx -> Value
lookupType s [] = error $ "[lookupType] got unknown identifier " ++ show s
lookupType s ((s',entry):ctx) = if s == s' then
    case entry of
        Decl ty    -> eval ctx ty
        Def ty _    -> eval ctx ty
        Val _       -> lookupType s ctx
    else
        lookupType s ctx
```

```

-- Evaluate a term in the given context
eval :: Ctx -> Term -> Value
eval ctx term = case term of
  Var s -> case lookup s ctx of
    Nothing -> error $ "[eval] not found var `" ++ show s ++ "` in ctx"
    Just (Val v) -> v
    Just (Decl ty) -> simplNeutralValue $ Neutral (Var s) (eval ctx ty)
    Just (Def _ e) -> eval ctx e
  Universe -> Universe
  TDef (s,t,e) t' -> eval (extend ctx s (Def t e)) t'
  Abst{} -> Closure term ctx
  App e1 e2 -> doApply (eval ctx e1) (eval ctx e2)
  Sigma{} -> Closure term ctx
  Pair t1 t2 -> Pair (eval ctx t1) (eval ctx t2)
  Fst t -> doFst (eval ctx t)
  Snd t -> doSnd (eval ctx t)
  Sum ty1 ty2 -> Sum (eval ctx ty1) (eval ctx ty2)
  InL t1 -> InL (eval ctx t1)
  InR t2 -> InR (eval ctx t2)
  Split ty f1 f2 x ->
    doSplit (eval ctx ty) (eval ctx f1) (eval ctx f2) (eval ctx x)
  Nat -> Nat
  Zero -> Zero
  Succ t -> Succ (eval ctx t)
  Ind ty base step n -> doInd (eval ctx ty) (eval ctx base)
    (eval ctx step) (eval ctx n)
  I -> I
  IO -> IO
  I1 -> I1
  Sys sys -> evalSystem ctx sys
  Partial phi t -> foldPartial (evalDisjFormula ctx phi) (eval ctx t)
  Restr sys t -> foldRestr (evalRestrSystem ctx sys) (eval ctx t)
  Comp fam phi i0 u b i -> doComp ctx fam phi i0 u b i
  -- Already evaluated term (used solely for `doComp`)
  TermV v -> v
  otherwise -> error $ "[eval] got " ++ show term

-- Evaluate a conjunctive formula
evalConjFormula :: Ctx -> ConjFormula -> Maybe ConjFormula
evalConjFormula ctx conj = conj'
  where
    -- Get the bindings which concern the formula's variables
    entries' = filter (\(s,_) -> s `elem` vars conj) (getBindings ctx)
    -- Get only the last one of each binding
    entries = map (\s -> fromJust $ find (\(s',_) -> s' == s) entries')
      (nub $ keys entries')
    -- Get the renamings from the entries (i.e. the ones of the form i -> j)
    renamings = concatMap (\case { (s,Neutral (Var s') I) -> [(s,s')] ;

```

```

    _ -> [])} entries
-- Apply renamings to the conjunction
renamedConj = foldr substConj conj renamings
-- Apply value substitutions to the renamed conjunction
vals      = filter (\(_,v) -> v == I0 || v == I1) entries
conj'     = foldrM evalConj renamedConj vals

-- Evaluate a single conjunction by replacing `s` with 0
-- Returns `Nothing` if the resulting formula is false
evalConj :: (Ident, Value) -> ConjFormula -> Maybe ConjFormula
evalConj (s, I0) conj@(Conj cf) =
  if conjToDirEnv conj `makesTrueAtomic` Eq1 s -- Inconsistent cases
  || inconsistent (conjToDirEnv conj') then
    Nothing
  else
    Just conj' -- Substitute into each atomic formula
  where
    conj' = Conj . nub $ concatMap (\case
      Eq0 s' | s == s' -> [];
      Diag s1 s2 -> if s == s1 && s1 == s2 then []
        else [if s == s1 then Eq0 s2
              else if s == s2 then Eq0 s1 else Diag s1 s2];
      af -> [af]) cf

-- Same as before, now replacing `s` with 1
evalConj (s, I1) conj@(Conj cf) =
  if conjToDirEnv conj `makesTrueAtomic` Eq0 s -- Inconsistent cases
  || inconsistent (conjToDirEnv conj') then
    Nothing
  else
    Just conj' -- Substitute into each atomic formula
  where
    conj' = Conj . nub $ concatMap (\case
      Eq1 s' | s == s' -> [];
      Diag s1 s2 -> if s == s1 && s1 == s2 then []
        else [if s == s1 then Eq1 s2
              else if s == s2 then Eq1 s1 else Diag s1 s2];
      af -> [af]) cf

-- Evaluate a disjunctive formula, by first checking if it contains
-- a true conjunction
evalDisjFormula :: Ctx -> DisjFormula -> DisjFormula
evalDisjFormula ctx (Disj df) = if Conj [] `elem` df then
  fTrue
  else -- Otherwise evaluate each conjunction, disregarding the false ones
    Disj $ mapMaybe (evalConjFormula ctx) df

-- Simplify cascading restriction types into one restriction type
-- E.g. [psi_1 -> t_1]([psi_2 -> t_2]([psi_3 -> t_3]A)) becomes

```

```

-- [psi_1 -> t_1 / psi_2 -> t_2 / psi_3 -> t_3]A
foldRestr :: System -> Value -> Value
foldRestr sys0 v0 = -- If the system is empty, return just the type
  if null sys then v else Restr (nub sys) v
  where
    (sys,v) = foldRestr' sys0 v0
    foldRestr' :: System -> Value -> (System,Value)
    foldRestr' sys v = case v of
      Restr sys' v' -> foldRestr' (sys ++ sys') v'
      otherwise      -> (sys,v)

-- Simplify cascading partial types into one partial type
-- E.g. [phi_1]([phi_2]([phi_3]A)) becomes
-- [phi /\ psi_2 /\ psi_3]A
foldPartial :: DisjFormula -> Value -> Value
foldPartial (Disj df0) v0 = -- If the formula is true, return just the type
  if makesTrueDisj emptyDirEnv (Disj df) then
    v
  else -- `nub` removes duplicate formulas
    Partial (Disj $ nub df) v
  where
    (df,v) = foldPartial' df0 v0
    foldPartial' :: [ConjFormula] -> Value -> ([ConjFormula],Value)
    foldPartial' df v = case v of
      Partial (Disj df') v' -> foldPartial' (dnf df' df) v'
      otherwise              -> (df,v)
    -- Get the conjunction of the two disjunctive formulas,
    -- in disjunctive normal form
    dnf :: [ConjFormula] -> [ConjFormula] -> [ConjFormula]
    dnf df1 df2 = [cf1 `meet` cf2 | cf1 <- df1, cf2 <- df2]

-- Evaluate the system of a restriction type,
-- by dropping false formulas
evalRestrSystem :: Ctx -> System -> System
evalRestrSystem ctx sys =
  concatMap (\(phi,t) -> evalConjFormula' phi (eval ctx t)) sys
  where
    -- Need to handle the case of false formulas
    evalConjFormula' phi v = case evalConjFormula ctx phi of
      Nothing -> []
      Just cf -> [(cf,v)]

-- Evaluate a system and eventually simplify it (recursively)
-- if there is a true formula
evalSystem :: Ctx -> System -> Value
evalSystem ctx sys =
  case foldrM evalConjFormula' [] sys of
    Left val -> val -- System has been simplified
    Right sys' -> Sys sys' -- There were no true formulas

```

```

where
  -- The following function gets the new pair (formula,term) and the
  -- part of the system already evaluated. If the new formula is true,
  -- it returns the given value using `Left`; otherwise, the new evaluated
  -- system is returned inside `Right`
  evalConjFormula' :: (ConjFormula,Term) -> System -> Either Value System
  evalConjFormula' (psi,t) sys' = case evalConjFormula ctx psi of
    Nothing      -> Right sys          -- False formula: nothing to add
    Just (Conj []) -> Left $ eval ctx t -- True formula, return the value
    Just cf       -> Right $ (cf,eval ctx t) : sys' -- Otherwise, append

  -- Simplify a neutral value if the type is a restriction type with a true
  -- formula, otherwise do nothing.
  -- `simplNeutralValue` is used only in evaluation.
  simplNeutralValue :: Value -> Value
  simplNeutralValue neu@(Neutral _ ty) = case ty of
    Restr sys _ | any (isTrueConj . fst) sys ->
      snd . fromJust $ find (isTrueConj . fst) sys
    otherwise -> neu

  -- Split the Abst/Sigma constructor and the arguments from a value
  -- inside a closure
  extract :: Value -> (Ident -> Term -> Term -> Value,Ident,Term,Term)
  extract (Abst s t e) = (Abst ,s,t,e)
  extract (Sigma s t e) = (Sigma,s,t,e)
  extract v              = error $ "[extract] got " ++ show v

  -- Evaluate a closure, extending the context by assigning the variable to
  -- the given value. In case of non-dependent abstractions, i.e. empty
  -- variable, we don't need to extend the context
  evalClosure :: Value -> Value -> Value
  evalClosure (Closure (Abst s _ e) ctx) arg =
    eval (if s == Ident "" then ctx else extend ctx s (Val arg)) e
  evalClosure (Closure (Sigma s _ e) ctx) arg =
    eval (if s == Ident "" then ctx else extend ctx s (Val arg)) e
  evalClosure v arg = error $ "[evalClosure] got non-closure " ++ show v
    ++ " applied to " ++ show arg

  -- Handler of `App` (function application, i.e.  $\Pi$ -type eliminator)
  doApply :: Value -> Value -> Value
  -- Standard case: do  $\beta$ -reduction
  doApply fun@(Closure Abst{} _) arg = evalClosure fun arg
  -- Restricted abstraction case, which requires to apply the function
  -- inside the restriction too
  doApply (Restr sys fun@(Closure{})) arg = foldRestr sys' (doApply fun arg)
    where sys' = mapSys (`doApply` arg) sys
  -- Standard neutral case
  doApply fun@(Neutral _ fty@(Closure{})) arg =
    simplNeutralValue $ Neutral (App fun arg) (doApply fty arg)

```

```

-- Restricted neutral case
doApply fun@(Neutral _ (Restr sys cl@Closure{})) arg =
  simplNeutralValue $ Neutral (App fun arg) (foldRestr sys' (doApply cl arg))
  where sys' = mapSys (`doApply` arg) sys
-- System case
doApply (Sys sys) arg = Sys $ mapSys (`doApply` arg) sys
-- Partial type case
doApply fun@(Neutral _ (Partial phi cl@Closure{})) arg =
  Neutral (App fun arg) (foldPartial phi (doApply cl arg))
doApply v arg = error $ "[doApply] got " ++ show v ++ ", " ++ show arg

-- Handler of `Fst` (i.e.  $\Sigma$ -type first projection)
doFst :: Value -> Value
doFst v = case v of
  -- Standard case: do  $\beta$ -reduction
  Pair v1 _ -> v1
  -- Standard neutral case; need to compute the type
  Neutral _ (Closure (Sigma _ t _) ctx) -> simplNeutralValue $ Neutral (Fst v)
    (eval ctx t)
  -- Restricted neutral case
  Neutral x (Restr sys cl@(Closure (Sigma _ t _) ctx)) ->
    simplNeutralValue $ Neutral (Fst (Neutral x cl)) (foldRestr sys' (eval ctx t))
    where sys' = mapSys doFst sys
  -- System case
  Sys sys -> Sys $ mapSys doFst sys
  -- Partial type case
  Neutral x (Partial phi cl@(Closure (Sigma _ t _) ctx)) ->
    Neutral (Fst (Neutral x cl)) (foldPartial phi (eval ctx t))
  otherwise -> error $ "[doFst] got " ++ show v

-- Handler of `Snd` (i.e.  $\Sigma$ -type second projection)
doSnd :: Value -> Value
doSnd v = case v of
  -- Standard case: do  $\beta$ -reduction
  Pair _ v2 -> v2
  -- Standard neutral case; need to compute the type
  Neutral _ ty@(Closure Sigma{} _) -> simplNeutralValue $ Neutral (Snd v)
    (evalClosure ty (doFst v))
  -- Restricted neutral case
  Neutral x (Restr sys cl@(Closure Sigma{} _)) ->
    simplNeutralValue $ Neutral (Snd (Neutral x cl))
      (foldRestr sys' (evalClosure cl (doFst (Neutral x cl))))
    where sys' = mapSys doSnd sys
  -- System case
  Sys sys -> Sys $ mapSys doSnd sys
  -- Partial type case
  Neutral x (Partial phi cl@(Closure Sigma{} _)) ->
    Neutral (Snd (Neutral x cl))
      (foldPartial phi (evalClosure cl (doFst (Neutral x cl))))

```



```

otherwise -> error $ "[doSnd] got " ++ show v

-- Handler of `Split` (i.e. (+)-type eliminator)
doSplit :: Value -> Value -> Value -> Value -> Value
doSplit fam f1 f2 x = case x of
  -- Standard cases (left/right injection): do  $\beta$ -reduction
  InL x1 -> doApply f1 x1
  InR x2 -> doApply f2 x2
  -- Standard neutral case; need to compute the type
  Neutral _ (Sum _ _) -> simplNeutralValue $
    Neutral (Split fam f1 f2 x) (doApply fam x)
  -- Restricted neutral case
  Neutral _ (Restr sys (Sum ty1 ty2)) -> simplNeutralValue $
    Neutral (Split fam f1 f2 (Neutral x (Sum ty1 ty2)))
      (foldRestr sys' (doApply fam x))
    where sys' = mapSys (doSplit fam f1 f2) sys
  -- System case
  Sys sys -> Sys $ mapSys (doSplit fam f1 f2) sys
  -- Partial type case
  Neutral _ (Partial phi (Sum ty1 ty2)) ->
    Neutral (Split fam f1 f2 (Neutral x (Sum ty1 ty2)))
      (foldPartial phi (doApply fam x))
  otherwise -> error $ "[doSplit] got " ++ show x

-- Handler of `Ind` (i.e. Nat eliminator)
doInd :: Value -> Value -> Value -> Value -> Value
doInd fam base step m = case m of
  -- Standard base and inductive cases: do  $\beta$ -reduction
  Zero -> base
  Succ n' -> doApply fun prev
    where
      fun = doApply step n'
      prev = doInd fam base step n'
  -- Standard neutral case; need to compute the type
  Neutral n Nat -> simplNeutralValue $ Neutral (Ind fam base step n)
    (doApply fam (Neutral n Nat))
  -- Restricted neutral case
  Neutral n (Restr sys Nat) ->
    simplNeutralValue $ Neutral (Ind fam base step n)
      (foldRestr sys' (doApply fam (Neutral n Nat)))
    where sys' = mapSys (doInd fam base step) sys
  -- System case
  Sys sys -> Sys $ mapSys (doInd fam base step) sys
  -- Partial type case
  Neutral n (Partial phi Nat) ->
    Neutral (Ind fam base step n) (foldPartial phi (doApply fam (Neutral n Nat)))
  otherwise -> error $ "[doInd] got " ++ show m

-- Utility function to handle eventually empty strings

```

```

ifEmpty :: Ident -> String -> Ident
ifEmpty (Ident "") s = Ident s
ifEmpty i      _ = i

{- Handler of composition (which is not an eliminator!).
The problem with composition is that we need to pattern-match inside
a closure (`famV`); when calling `doComp` recursively, we must
read-back terms, but we cannot do so for the type family (otherwise
it would then be evaluated under the general context and not in its own).
Therefore, we introduce a wrapper `TermV` which makes it possible to
include values (closures) inside terms, so that when the whole term is
evaluated, the closure is evaluated with the right context. The wrapper
`TermV` is used solely in the evaluation of composition.
-}
doComp :: Ctx -> Term -> DisjFormula -> Term -> Term -> Term -> Term -> Value
doComp ctx fam phi i0 u b i =
  if isTrue phiV then      -- 1° trivial case: `phi` is True
    doApply uV iV
  else if i0V == iV then -- 2° trivial case: i = i_0 (no need for `conv`)
    bV
  else
    -- Fresh variables: `var` to pattern-match the type family
    -- `var2` to handle the partially defined `u`
    let var = newVar (keys ctx) (Ident "_i")
        var2 = case uV of
          Closure (Abst v _ _) _ -> newVar (keys ctx) (ifEmpty v "j")
        emptySys = Abst (Ident "") I (Sys [])
        ctxOf v = case v of Closure _ gctx -> gctx
    -- Evaluate the type-family, pattern-matching inside the closure
    in case doApply famV (Neutral (Var var) I) of
      --  $\Pi$ -type `[x:ty]e`, with `ty` a type
      cl@(Closure (Abst x ty e) ctx') | eval ctx' ty /= I ->
        Closure (Abst yi tyc comp) ctx
      where
        -- Variable of the target type `tyc`, i.e. `ty(i)`
        yi = newVar (var : var2 : keys ctx) (ifEmpty x "u")
        -- Transport of that variable at `i0` and `var`
        yt0 = Comp (TermV fam1) fFalse i emptySys (Var yi) i0
        yt = Comp (TermV fam1) fFalse i emptySys (Var yi) (Var var)
        -- Resulting composition
        comp = Comp (TermV fam2) phi i0 u' (App b yt0) i
        -- Type families
        fam1 = Closure (Abst var I ty) ctx'
        fam2 = Closure (Abst var I (App (Abst x ty e) yt)) ctx'
        -- Target type: `ty(i)`
        tyc = readBack (keys ctx) $ case doApply famV iV of
          Closure (Abst _ ty' _) ctx'' -> eval ctx'' ty'
        -- Apply functions to `yt` inside `u`
        u' = case isFalse phiV of

```

```

    True  -> u
    False -> Abst var2 I (App (App u (Var var2)) yt)

--  $\Pi$ -type  $[x:I]e$ 
cl@(Closure (Abst x ty e) ctx') | eval ctx' ty == I ->
  Closure (Abst x' I comp) ctx
  where
    -- Fresh interval variable
    x'  = newVar (var : var2 : keys ctx) (ifEmpty x "i")
    -- Resulting composition
    comp = Comp (TermV fam') phi i0 u' (App b (Var x')) i
    fam' = Closure (Abst var I e) ctx'
    -- Apply functions to  $x'$  inside  $u$ 
    u'   = case isFalse phiV of
      True  -> u
      False -> Abst var2 I (App (App u (Var var2)) (Var x'))

--  $\Sigma$ -type  $\langle x:ty \rangle e$ 
cl@(Closure (Sigma _ ty _) ctx') -> Pair c1 c2
  where
    -- Composition on each pair
    c1 = doComp ctx (TermV fam1) phi i0 u0 (Fst b) i
    c2 = doComp ctx (TermV fam2) phi i0 u1 (Snd b) i
    -- The type family of  $c2$  needs the comp. on the first component
    fam1 = Closure (Abst var I ty) ctx'
    fam2 = Closure (Abst var I ty2) ctx'
    ty2  = readBack (keys ctx) $ evalClosure c1 c1'
    c1'  = doComp ctx (TermV fam1) phi i0 u0 (Fst b) (Var var)
    -- Apply projections inside  $u$ 
    (u0,u1) = case isFalse phiV of
      True  -> (u,u)
      False -> (Abst var2 I (Fst (App u (Var var2)))),
                Abst var2 I (Snd (App u (Var var2))))

-- Coproduct  $ty1 + ty2$ 
Sum ty1 ty2 ->
  -- If  $b$  is neutral, the result is neutral
  case bV of
    Neutral{} -> doNeutralComp
    otherwise -> inj comp
  where (inj,bV',ty) = case bV of
    -- Extract the injection, the inner value and the type
    InL b1 -> (InL,b1,ty1)
    InR b2 -> (InR,b2,ty2)
    -- Resulting composition
    comp = doComp ctx (TermV fam') phi i0 u' b' i
    b'   = readBack (keys ctx) bV'
    fam' = Closure (Abst var I ty') (ctxOf famV)
    ty'  = readBack (keys (ctxOf famV)) ty

```

```

-- Remove the outer injections from `u`
u' = case isFalse phiV of
  True  -> u
  False -> Abst var2 I (readBack (keys ctx) sys')
where app = App u (Var var2)
  sys' = case eval (extend ctx var2 (Decl I)) app of
    Sys sysV -> Sys $ map (\case {(psi, InL q) -> (psi, q);
    (psi, InR q) -> (psi, q)}) sysV
    InL q    -> q
    InR q    -> q

-- Naturals
Nat -> case bV of
  Zero    -> Zero
  Succ b' -> Succ $ doComp ctx fam phi i0 u' b' i
  -- Remove the outer `S` from `u`
  where u' = case isFalse phiV of
    True  -> u
    False -> Abst var2 I (readBack (keys ctx) sys')
    where app = App u (Var var2)
      sys' = case eval (extend ctx var2 (Decl I)) app of
        Sys sysV -> Sys $
          map (\case {(psi, Succ m) -> (psi, m)}) sysV
        Succ m    -> m
  Neutral{} -> doNeutralComp

-- Partial type `[phi]ty`
Partial (Disj df) tyV ->
  if var `elem` vars (Disj df) then
    error $ "Type family '" ++ show (readBack (keys ctx) famV)
    ++ "' is not fibrant"
  else
    sysComp
where
  -- Type family (without the formula)
  fam' = Closure (Abst var I ty') (ctxOf famV)
  ty' = readBack (keys (ctxOf famV)) tyV
  -- Obtain a system with a composition for each conjunction
  -- If the system has just one value, return it
  sysCompVals = map helperComp df
  sysComp = if length df == 1 then
    head sysCompVals
  else
    Sys $ zip df sysCompVals
  -- Do composition on each conjunction
  helperComp :: ConjFormula -> Value
  helperComp conj = doComp (addConjBindings ctx conj)
    (TermV fam') phi i0 u (b' conj) i
  -- Eventually simplify `b` (as it may have already been evaluated)

```

```

b' :: ConjFormula -> Value
b' conj = readBack (keys ctx) $ case bV of
  -- A formula is true
  Sys sysU | any ((conjToDirEnv conj `makesTrueConj`) . fst) sysU
    -> snd . fromJust $
      find ((conjToDirEnv conj `makesTrueConj`) . fst) sysU
  _ -> bV

-- Restriction type  $[\phi]ty$ 
Restr sysR tyV ->
  if var `elem` concatMap vars (keys sys) then
    error $ "Type family '" ++ show (readBack (keys ctx) famV)
      ++ "' is not fibrant"
  else
    doComp ctx (TermV fam') formula i0 u' b i
  where
    -- Get the new formula (without the restriction)
    formula = Disj $ phi' ++ psis
    phi' = case phi of Disj ff -> ff
    psis = keys sysR
    -- Type family
    fam' = Closure (Abst var I ty') (ctxOf famV)
    ty' = readBack (keys (ctxOf famV)) tyV
    --ty' = readBack (keys ctx) tyV
    u' = Abst var2 I (Sys sys')
    -- Concatenate the two systems
    sys' = map (\conj -> (conj, App u (Var var2))) phi'
      ++ case doApply famV (Neutral (Var var2) I) of
        Restr sys'' _ ->
          mapSys (TermV . readBack (keys ctx)) sys''

    -- Neutral type family; the result of the composition is neutral too
    otherwise -> doNeutralComp

  where
    -- Values computed for each argument (remember that Haskell is lazy!)
    famV = eval ctx fam
    phiV = evalDisjFormula ctx phi
    i0V = eval ctx i0
    uV = eval ctx u
    bV = eval ctx b
    iV = eval ctx i
    -- Compute the type of the composition, and prepare the neutral value
    doNeutralComp = simplNeutralValue $
      Neutral (Comp famV phiV i0V uV bV iV) (eval ctx compTy)
    sys = getCompSys phi i0 u b i
    compTy = Restr sys (App fam i)

-- Get the system of the restriction type of a composition
getCompSys :: DisjFormula -> Term -> Term -> Term -> Term -> System

```

```

getCompSys (Disj df) i0 u b i = eq ++ map (\conj -> (conj, App u i)) df
  where
    -- Extract the variables from eventual values
    i' = case i of { Neutral (Var x) _ -> Var x ; _ -> i }
    i0' = case i0 of { Neutral (Var x) _ -> Var x ; _ -> i0 }
    -- Translate `i = i0` into a real formula
    eq = case (i0', i') of
      (I0, I0)      -> [(Conj [], b)]
      (I0, I1)      -> []
      (I0, Var s)    -> [(Conj [Eq0 s], b)]
      (Var s, I0)    -> [(Conj [Eq0 s], b)]
      (Var s, I1)    -> [(Conj [Eq1 s], b)]
      (Var s, Var s') -> [(Conj [Diag s s'], b)]
      (I1, I0)      -> []
      (I1, I1)      -> [(Conj [], b)]
      (I1, Var s)    -> [(Conj [Eq1 s], b)]
      _              -> error $ "[getCompSys] got " ++ show (i, i0)

-- Read-back function which converts values back into terms
-- The first argument is the list of already used names
-- The only non-trivial case is that of closures
readBack :: [Ident] -> Value -> Term
readBack used val = case val of
  App fun arg -> App (readBack used fun) (readBack used arg)
  Succ v -> Succ (readBack used v)
  Fst v -> Fst (readBack used v)
  Snd v -> Snd (readBack used v)
  Pair v1 v2 -> Pair (readBack used v1) (readBack used v2)
  Sum v1 v2 -> Sum (readBack used v1) (readBack used v2)
  InL v -> InL (readBack used v)
  InR v -> InR (readBack used v)
  Split ty f1 f2 x -> Split (readBack used ty) (readBack used f1)
    (readBack used f2) (readBack used x)
  Sys sys -> Sys $ mapSys (readBack used) sys
  Partial phi ty -> foldPartial phi (readBack used ty)
  Restr sys ty -> foldRestr (mapSys (readBack used) sys) (readBack used ty)
  Ind ty b e n -> Ind (readBack used ty) (readBack used b) (readBack used e)
    (readBack used n)
  Comp fam phi i0 u b i -> Comp (readBack used fam) phi (readBack used i0)
    (readBack used u) (readBack used b) (readBack used i)
  -- Closure case: first evaluate the body with a fresh name, then read-back
  cl@(Closure f ctx) -> let
    -- `constr` is `Abst` or `Sigma`
    (constr, s, t, e) = extract f
    s' = newVar used s
    eVal = evalClosure cl (Neutral (Var s') (eval ctx t))
    e' = readBack (s' : used) eVal
    t' = readBack used (eval ctx t)
  in constr s' t' e'

```

```

-- For neutrals, read-back the value, ignoring the type
Neutral v _ -> readBack used v
otherwise -> val

-- Normalization means first evaluating and then reading-back
normalize :: Ctx -> Term -> Term
normalize ctx e = readBack (keys ctx) (eval ctx e)

{- Printing utilities (should be in AbsCTT but these need 'readBack') -}

-- Print function for a term or value (which is read-back into
-- a term, except when debugging)
instance Show Term where
  show t = printTerm' 0 (if debug then t else readBack [] t)

-- Helper function; the first argument `i` measures the depth
-- of the term (but is reset in some cases), which is used to
-- avoid unnecessary parentheses
printTerm' :: Int -> Term -> String
printTerm' i = \case
  Var s      -> show s
  Universe   -> "U"
  TDef (s,t,e) t' ->
    "[" ++ show s ++ ":" ++ printTerm' 0 t ++ " = "
    ++ printTerm' 0 e ++ "]" ++ printTerm' 0 t'
  Abst s t e -> par1 ++ abstS ++ par2
    where abstS = if s == Ident "" || not (containsVar s e)
      then -- A -> B (no dependency)
        printTerm' (i+1) t ++ " -> " ++ printTerm' 0 e
      else
        "[" ++ show s ++ ":" ++ printTerm' 0 t ++ "]" ++ printTerm' 0 e
  Sigma s t e -> par1 ++ abstS ++ par2
    where abstS = if s == Ident "" || not (containsVar s e)
      then -- A * B (no dependency)
        printTerm' (i+1) t ++ " * " ++ printTerm' 0 e
      else
        "<" ++ show s ++ ":" ++ printTerm' 0 t ++ ">"
        ++ printTerm' 0 e
  Pair t1 t2 -> par1 ++ printTerm' i t1 ++ "," ++ printTerm' i t2 ++ par2
  Fst t -> par1 ++ printTerm' (i + 1) t ++ ".1" ++ par2
  Snd t -> par1 ++ printTerm' (i + 1) t ++ ".2" ++ par2
  Sum ty1 ty2 -> par1 ++ printTerm' (i + 1) ty1 ++ " + "
    ++ printTerm' (i + 1) ty2 ++ par2
  InL t1 -> par1 ++ "inl " ++ printTerm' (i + 1) t1 ++ par2
  InR t2 -> par1 ++ "inr " ++ printTerm' (i + 1) t2 ++ par2
  Split ty f1 f2 x -> par1 ++ "split " ++ printTerm' (i+1) ty ++ " "
    ++ printTerm' (i+1) f1 ++ " " ++ printTerm' (i+1) f2 ++ " "
    ++ printTerm' (i+1) x ++ par2
  App fun arg -> par1 ++ printTerm' (i+1) inner

```

```

    ++ " " ++ unwords printedArgs ++ par2
    where (inner,args) = collectApps (App fun arg) []
          printedArgs = map (printTerm' (i+1)) args
Nat      -> "N"
Zero     -> "Z"
Succ t   -> par1 ++ "S " ++ printTerm' (i+1) t ++ par2
Ind ty b s n -> par1 ++ "ind " ++ printTerm' (i+1) ty ++ " "
    ++ printTerm' (i+1) b ++ " " ++ printTerm' (i+1) s ++ " "
    ++ printTerm' (i+1) n ++ par2
I        -> "I"
IO       -> "O"
I1       -> "1"
Sys sys  -> showSystem sys
Partial phi t -> "[" ++ show phi ++ "]" ++ printTerm' (i+1) t
-- If the restriction is empty, don't print it, otherwise it
-- could be mistaken for a partial type with false formula
Restr sys t -> (if null sys then "" else showSystem sys) ++ printTerm' (i+1) t
Comp fam phi i0 u b i' -> par1 ++ "comp " ++ printTerm' (i+1) fam
    ++ " (" ++ show phi ++ ") " ++ printTerm' (i+1) i0 ++ " "
    ++ printTerm' (i+1) u ++ " " ++ printTerm' (i+1) b
    ++ " " ++ printTerm' (i+1) i' ++ par2
----- Used only when debugging, to print proper values
Closure cl _ -> "Cl(" ++ show cl ++ ")"
Neutral v t -> "N{" ++ printTerm' i v ++ "}:" ++ printTerm' (i+1) t
TermV v -> show v
-- Parentheses are not needed if `i` is zero
where (par1,par2) = if i == 0 then ("","") else ("(",")")

-- Print a context (in one line)
showCtx :: Ctx -> String
showCtx ctx = "[" ++ intercalate ", " (map showEntry (reverse ctx)) ++ "]"

-- Print a single context entry
showEntry :: (Ident,CtxEntry) -> String
showEntry (s,Decl ty) = show s ++ " : " ++ show ty
showEntry (s,Def ty val) = show s ++ " : " ++ show ty ++ " = " ++ show val
showEntry (s,Val val) = show s ++ " => " ++ show val

-- Print a system
showSystem :: System -> String
showSystem sys = "[" ++ sysS ++ "]"
    where sysS = intercalate " | " $
        map (\(ff,t) -> show ff ++ " -> " ++ show t) sys

```



## 3.5 Conversion

In this file we implement the  $\alpha\eta$ -conversion predicate between two values, which are assumed to have the same type. This predicate is used only during type-checking, and not in evaluation.

The convertibility predicate uses the directions environment `dirs` given by the type-checker; we must then handle the case of systems  $[\psi_1 \mapsto \mathbf{v}_1, \dots, \psi_n \mapsto \mathbf{v}_n]$  and neutral values of the form  $\mathbf{k}^{\mathbf{A}[\psi_1 \mapsto \mathbf{v}_1, \dots, \psi_n \mapsto \mathbf{v}_n]}$ , where one of the formulas  $\psi_i$  becomes true under `dirs`, reducing them to  $\mathbf{v}_i$ . For this purpose, we have implemented a function called `simpl`.

Source file `Conv.hs`.

```
{-# LANGUAGE FlexibleInstances #-}
module Conv where

import Data.List (find)
import Data.Maybe (fromJust)

import Ident
import Interval
import CoreCTT
import Eval

-- Generic class for objects that allow a notion of  $\alpha$ -conversion
class Convertible a where
  conv :: [Ident] -> DirEnv -> a -> a -> Bool

-- Check convertibility under a conjunctive formula
-- If the formula is false, the values are trivially convertible
convPartialConj :: [Ident] -> ConjFormula -> DirEnv -> Value -> Value -> Bool
convPartialConj used conj dirs v1 v2 =
  let dirs' = addConj dirs conj
  in inconsistent dirs' || conv used dirs' v1 v2

-- Two values are convertible under a disjunctive formula iff
-- they are so under each conjunction
convPartialDisj :: [Ident] -> DisjFormula -> DirEnv -> Value -> Value -> Bool
convPartialDisj used (Disj df) dirs v1 v2 =
  all (\conj -> convPartialConj used conj dirs v1 v2) df

-- Check if two  $\Pi/\Sigma$ -abstractions are of the same kind
sameKind :: Term -> Term -> Bool
sameKind Abst{} Abst{} = True
sameKind Sigma{} Sigma{} = True
sameKind _ _ = False
```

```

{- The following functions are used to simplify neutral values
that may become non-neutral under the added constraints in `dirs`.
They are used only during `conv`, and NOT during `eval`. -}

-- Check if a restriction type contains a true formula
-- under the directions environment `dirs`
isSimplRestr :: DirEnv -> Value -> Bool
isSimplRestr dirs ty = case ty of
  Restr sys _ -> isSimplSys dirs sys
  otherwise    -> False

-- Simplify a restriction type if it contains a true formula
-- under the directions environment `dirs`
simplRestr :: DirEnv -> Value -> Value
simplRestr dirs (Restr sys _) = simplSys dirs sys

-- Check if a system contains a true formula
-- under the directions environment `dirs`
isSimplSys :: DirEnv -> System -> Bool
isSimplSys dirs = any ((dirs `makesTrueConj`) . fst)

-- Simplify a system if it contains a true formula
-- under the directions environment `dirs`
simplSys :: DirEnv -> System -> Value
simplSys dirs sys = snd . fromJust $
  find ((dirs `makesTrueConj`) . fst) sys

-- Simplify a system or neutral value if possible, otherwise do nothing
simpl :: DirEnv -> Value -> Value
simpl dirs (Sys sys)      | isSimplSys dirs sys = simplSys dirs sys
simpl dirs (Neutral _ ty) | isSimplRestr dirs ty = simplRestr dirs ty
simpl _ v = v

-- Check if the type can be simplified; in that case two values
-- of that type are automatically convertible, because they
-- shall reduce to the same value. That is, we don't need
-- to look inside the terms, i.e. we can ignore the proof
proofIrrelevant :: DirEnv -> Value -> Bool
proofIrrelevant dirs ty = case ty of
  Restr sys ty' -> isSimplRestr dirs ty
  || proofIrrelevant dirs ty'
  Closure cl ctx -> let
    -- Fresh variable to evaluate closures
    varV :: Ident -> Value -> CtxEntry
    varV s t = Val $ Neutral (Var $ newVar (keys ctx) s) (eval ctx t)
  in case cl of
    --  $\Pi$ -types: codomain proof irrelevant
    Abst s t e -> proofIrrelevant dirs
      (eval (extend ctx s (varV s t)) e)

```

```

--  $\Sigma$ -types: both components proof irrelevant
Sigma s t e -> proofIrrelevant dirs (eval ctx t) &&
  proofIrrelevant dirs (eval (extend ctx s (varV s t)) e)
otherwise -> False

--  $\alpha\eta$  convertibility for values, which are supposed to have the
-- same type. For efficiency, we first test exact syntactical equality
instance Convertible Value where
conv used dirs v1 v2 =
  v1 == v2 || let cnv = conv used dirs in case (v1,v2) of
    (Universe,Universe) -> True
  --  $\Pi/\Sigma$  closures
  (Closure cl1 ctx1,Closure cl2 ctx2) | sameKind cl1 cl2 -> let
    (_,s1,t1,_) = extract cl1
    (_,_,t2,_) = extract cl2
    var = newVar used s1
    t1V = eval ctx1 t1
    t2V = eval ctx2 t2
    e1' = evalClosure v1 (Neutral (Var var) t1V)
    e2' = evalClosure v2 (Neutral (Var var) t2V)
    in cnv t1V t2V && conv (var : used) dirs e1' e2'
  --  $\eta$ -rule for  $\Pi$  (first case)
  (Closure (Abst s1 t1 _) ctx1,Neutral _ (Closure Abst{} _)) -> let
    var = newVar used s1
    t1V = eval ctx1 t1
    e1' = evalClosure v1 (Neutral (Var var) t1V)
    e2' = doApply v2 (Neutral (Var var) t1V)
    in conv (var : used) dirs e1' e2'
  --  $\eta$ -rule for  $\Pi$  (second case)
  (Neutral _ (Closure Abst{} _),Closure (Abst s2 t2 _) ctx2) -> let
    var = newVar used s2
    t2V = eval ctx2 t2
    e1' = doApply v1 (Neutral (Var var) t2V)
    e2' = evalClosure v2 (Neutral (Var var) t2V)
    in conv (var : used) dirs e1' e2'
  {- Sigma types -}
  (Fst v,Fst v') -> cnv v v'
  (Snd v,Snd v') -> cnv v v'
  (Pair vp1 vp1',Pair vp2 vp2') -> cnv vp1 vp2 &&
    cnv vp1' vp2'
  --  $\eta$ -rule for  $\Sigma$  (first case)
  (vp,Pair v v') -> cnv (doFst vp) v &&
    cnv (doSnd p) v'
  --  $\eta$ -rule for  $\Sigma$  (second case)
  (Pair v v',vp) -> cnv v (doFst vp) &&
    cnv v' (doSnd vp)
  {- Coproduct types -}
  (Sum ty1 ty2,Sum ty1' ty2') -> cnv ty1 ty1' && cnv ty2 ty2'
  (InL v,InL v') -> cnv v v'

```

```

(InR v, InR v') -> cnv v v'
{- Naturals -}
(Nat, Nat)      -> True
(Zero, Zero)    -> True
(Succ n1, Succ n2) -> cnv n1 n2
{- Cubical -}
(I, I)          -> True
(I0, I0)        -> True
(I1, I1)        -> True
-- Systems. We have to check is the system is simplifiable
-- to avoid an infinite loop
(Sys sys, _) | isSimplSys dirs sys ->
  cnv (simpl dirs v1) v2
(_, Sys sys) | isSimplSys dirs sys ->
  cnv v1 (simpl dirs v2)
(Sys sys, Sys sys') -> conv used dirs sys sys'
(Partial phi v, Partial phi' v') -> eqFormulas dirs phi phi' &&
  cnv v v'
(Restr sys t, Restr sys' t') -> conv used dirs sys sys' && cnv t t'
{- Values inside the `Neutral` wrapper -}
(Var s1, Var s2) -> s1 == s2
(App f1 a1, App f2 a2) -> cnv f1 f2 && cnv a1 a2
(Ind ty1 b1 s1 n1, Ind ty2 b2 s2 n2) ->
  cnv ty1 ty2 && cnv b1 b2 &&
  cnv s1 s2 && cnv n1 n2
(Split ty1 f1 g1 x1, Split ty2 f2 g2 x2) -> cnv ty1 ty2
  && cnv f1 f2 && cnv g1 g2 && cnv x1 x2
(Comp fam1 phi1 i01 u1 b1 i1, Comp fam2 phi2 i02 u2 b2 i2) ->
  cnv fam1 fam2 && eqFormulas dirs phi1 phi2 &&
  cnv i01 i02 && cnv u1 u2 && cnv b1 b2 && cnv i1 i2
-- Interval names
(Neutral (Var x1) I, Neutral (Var x2) I) ->
  dirs `makesTrueAtomic` Diag x1 x2
(Neutral (Var x1) I, I0) ->
  dirs `makesTrueAtomic` Eq0 x1
(Neutral (Var x1) I, I1) ->
  dirs `makesTrueAtomic` Eq1 x1
(I0, Neutral (Var x2) I) ->
  dirs `makesTrueAtomic` Eq0 x2
(I1, Neutral (Var x2) I) ->
  dirs `makesTrueAtomic` Eq1 x2
{- Neutrals -}
-- Simplest case: both neutral, with proof irrelevant type
(Neutral v ty, Neutral v' _) | proofIrrelevant dirs ty -> True
-- One value neutral with simplifiable restriction type,
-- the other value not neutral
(Neutral _ ty1, _) | isSimplRestr dirs ty1 ->
  cnv (simpl dirs v1) v2
(_, Neutral _ ty2) | isSimplRestr dirs ty2 ->

```

```

    cnv v1 (simpl dirs v2)
  -- Type is not a simplifiable restriction type,
  -- we must look inside the term (or proof)
  (Neutral v _, Neutral v' _) -> cnv v v'
  -- No other cases
  otherwise -> False

-- Convertibility between two systems
instance Convertible System where
  conv used dirs sys1 sys2 =
    eqFormulas dirs (getSystemFormula sys1) (getSystemFormula sys2)
    && all (\(conj,t1,t2) -> convPartialConj used conj dirs t1 t2) meets
  where meets = [(conj1 `meet` conj2, sys1 `at` conj1, sys2 `at` conj2) |
    conj1 <- keys sys1, conj2 <- keys sys2]

```

## 3.6 Type-checking

In this file we implement the bidirectional type checker, made up of the two functions `inferType` and `checkType`; the former gets a term as input and returns the evaluated type as output, whereas the latter gets as input a term and the evaluated type, and returns a boolean. To be more precise, the two functions use the `Either` monad to handle errors, using `Left err` to report an error and quit, and `Right v` to successfully return a value of the specified type.

Source file `TypeChecker.hs`.

```

module TypeChecker where

import Control.Monad

import Ident
import Interval
import CoreCTT
import Eval
import Conv

-- Infer the type of a term, in the given context and directions environment
inferType :: Ctx -> DirEnv -> Term -> Either ErrorString Value
inferType ctx dirs term = case term of
  -- Variables: look up the type in the context
  Var s -> Right $ lookupType s ctx
  -- Universe
  Universe -> Right Universe
  -- Function application: the type of the function is inferred
  App fun arg -> do
    funTy <- inferType ctx dirs fun
    -- Handle restriction and partial types: `box` is used

```

```

-- to put the resulting type in the eventual restriction
-- or partial type
let (funTy',box) = case funTy of
  Restr sys v    -> (v,makeRestr sys)
  Partial phi v  -> (v,makePartial phi)
  otherwise      -> (funTy,curry snd)
makeRestr :: System -> Value -> Value -> Value
makeRestr sys val = foldRestr $ mapSys (`doApply` val) sys
makePartial :: DisjFormula -> Value -> Value -> Value
makePartial phi _ = foldPartial phi
-- The type must be a  $\Pi$ -type
case funTy' of
  c@(Closure (Abst _ t _) ctx1) -> do
    checkType ctx dirs arg (eval ctx1 t)
    let argVal = eval ctx arg
    return $ box argVal (doApply c argVal)
  otherwise -> Left $
    "term '" ++ show fun ++ "' has type '" ++ show funTy
    ++ "' , which is not a product"

-- First projection: the type of the argument is inferred
Fst p -> do
  ty <- inferType ctx dirs p
  -- Handle restriction and partial types
  let (ty',box) = case ty of
    Restr sys t    -> (t,makeRestr sys)
    Partial phi v  -> (v,foldPartial phi)
    otherwise      -> (ty,id)
  makeRestr :: System -> Value -> Value
  makeRestr = foldRestr . mapSys doFst
  -- The type must be a  $\Sigma$ -type
  case ty' of
    Closure (Sigma _ t _) ctx1 -> do
      return $ box (eval ctx1 t)
    otherwise -> Left $
      "term '" ++ show term ++ "' has type '" ++ show ty
      ++ "' , which is not a sum"

-- Second projection: the type of the argument is inferred
Snd p -> do
  ty <- inferType ctx dirs p
  -- Handle restriction and partial types
  let (ty',box) = case ty of
    Restr sys t    -> (t,makeRestr sys)
    Partial phi v  -> (v,foldPartial phi)
    otherwise      -> (ty,id)
  makeRestr :: System -> Value -> Value
  makeRestr = foldRestr . mapSys doSnd
  -- The type must be a  $\Sigma$ -type

```

```

case ty' of
  c@(Closure Sigma{} ctx1) -> do
    return . box $ evalClosure c (doFst $ eval ctx p)
  otherwise -> Left $
    "term '" ++ show term ++ "' has type '" ++ show ty
    ++ "' , which is not a sum"

-- Coproduct eliminator: the type of the argument is inferred
Split fam f1 f2 x -> do
  ty <- inferType ctx dirs x

--Handle restriction and partial types
let (ty',box) = case ty of
  Restr sys t    -> (t,makeRestr sys)
  Partial phi v  -> (v,foldPartial phi)
  otherwise      -> (ty,id)
famV = eval ctx fam
makeRestr :: System -> Value -> Value
makeRestr = foldRestr . mapSys (famV `doApply`)
-- The type must be a coproduct
case ty' of
  Sum{} -> do
    let sty@(Sum sty1 sty2) = readBack (keys ctx) ty'
        var = newVar (keys ctx) (Ident "a")
    checkType ctx dirs fam
      (Closure (Abst (Ident "_") sty Universe) ctx)
    checkType ctx dirs f1
      (eval ctx $ Abst var sty1 (App fam (InL (Var var))))
    checkType ctx dirs f2
      (eval ctx $ Abst var sty2 (App fam (InR (Var var))))
    return . box $ eval ctx (App fam x)
  otherwise -> Left $ "expected a sum type, got term '" ++ show x
    ++ "' of type '" ++ show ty ++ "' instead"

-- Naturals
Nat -> Right Universe
Zero -> Right Nat
Succ n -> do
  checkType ctx dirs n Nat
  Right Nat
-- Induction for naturals
Ind fam base step n -> do
  -- Check that `n` is a natural (eventually partial/restricted)
  nTyVal <- inferType ctx dirs n
  isNat n nTyVal
  -- Check that `fam` has type N -> U
  checkType ctx dirs fam (makeFunTypeVal Nat Universe)

-- Handle restriction and partial types

```

```

let box = case nTyVal of
  Restr sys Nat -> makeRestr sys
  Partial phi _ -> foldPartial phi
  Nat          -> id
famV = eval ctx fam
makeRestr :: System -> Value -> Value
makeRestr = foldRestr . mapSys (famV `doApply`)

-- Evaluate the type-family `fam`, checking that `base` has
-- type `fam Z`
let tyVal = eval ctx fam
    tyVal0 = doApply tyVal Zero
checkType ctx dirs base tyVal0

-- Checking that the "inductive step" `step` has type
-- [n : nat] fam n -> fam (suc n)
let varname = newVar (keys ctx) (Ident "n")
    var      = Var varname
    ctx'     = extend ctx varname (Decl Nat)
checkType ctx dirs step (eval ctx'
  (Abst varname Nat
    (Abst (Ident "") (App fam var)
      (App fam (Succ var))))
)) -- [n : nat] fam n -> fam (suc n)

return . box $ doApply tyVal (eval ctx n)

-- Interval endpoints
I0 -> Right I
I1 -> Right I

-- Composition
Comp fam phi@(Disj df) i0 u b i -> do
  -- Checking the type-family `fam`, point `i0` and formula `phi`
  checkType ctx dirs fam (makeFunTypeVal I Universe) -- I -> U
  checkType ctx dirs i0 I
  checkDisjFormula ctx phi
  -- Checking that `u` has the correct type
  let var = newVar (keys ctx) (Ident "_i")
  checkType ctx dirs u (eval (extend ctx var (Decl I))
    (Abst var I (Partial phi (App fam (Var var)))))
  -- Checking that `b` has type `[phi -> u i0](fam i0)`
  checkType ctx dirs b $
    eval ctx (Restr (map (\psi -> (psi, App u i0)) df) (App fam i0))
  -- Return the evaluated type, without the restriction if it's empty
  let sys = getCompSys phi i0 u b i
  return $ eval ctx $ (if null sys then id else Restr sys) (App fam i)

-- Failed type inference

```



```

_ -> Left $ "don't know how to infer type of '" ++ show term ++ "'"

-- Check if a term has Nat type
isNat :: Term -> Value -> Either ErrorString ()
isNat _ Nat = Right ()
isNat _ (Restr _ Nat) = Right ()
isNat _ (Partial _ Nat) = Right ()
isNat t v = Left $ "expected type nat, got term '" ++ show t ++
  "' of type '" ++ show v ++ "' instead"

-- Utility function to get type values of the form A -> B
makeFunTypeVal :: Term -> Term -> Value
makeFunTypeVal ty e = eval emptyCtx (Abst (Ident "") ty e)

-- Check the type of a term under a conjunction
-- If the conjunction is false, type-check is trivially true
checkTypePartialConj :: ConjFormula -> Ctx -> DirEnv -> Term
  -> Value -> Either ErrorString ()
checkTypePartialConj conj ctx dirs e v = do
  let dirs' = addConj dirs conj
  unless (inconsistent dirs') $
    checkType ctx dirs' e v

-- Check the type of a term under a disjunction, that is
-- under each conjunction
checkTypePartialDisj :: DisjFormula -> Ctx -> DirEnv -> Term
  -> Value -> Either ErrorString ()
checkTypePartialDisj (Disj df) ctx dirs e v =
  mapM_ (\conj -> checkTypePartialConj conj ctx dirs e v) df

-- Check the type of a term against a given type
-- The type must be a value (i.e. in  $\beta$ -normal form)
checkType :: Ctx -> DirEnv -> Term -> Value -> Either ErrorString ()
checkType ctx dirs term v = case (term,v) of
  -- Let-definition
  (TDef (s,t,e) t',_) -> do
    checkType ctx dirs t Universe
    checkType (extend ctx s (Decl t)) dirs e (eval ctx t)
    checkType (extend ctx s (Def t e)) dirs t' v

  --  $\Pi$ -type former
  (Abst s t e,Universe) -> do
    -- Handle also path types
    unless (t == I) $ checkType ctx dirs t Universe
    checkType (extend ctx s (Decl t)) dirs e Universe

  --  $\Sigma$ -type former
  (Sigma s t e,Universe) -> do
    checkType ctx dirs t Universe

```

```

checkType (extend ctx s (Decl t)) dirs e Universe

--  $\lambda$ - or  $\Pi$ - abstraction
(Abst s t e, Closure (Abst _ t1 _) ctx1) -> do
  -- Handle also  $I$ -abstractions
  unless (t == I) $ checkType ctx dirs t Universe
  let tVal = eval ctx t
      t1Val = eval ctx1 t1
  unless (conv (keys ctx) dirs tVal t1Val) $
    Left $ "type '" ++ show tVal ++ "' is not convertible to type '"
      ++ show t1Val ++ "' (while checking term '" ++ show (Abst s t e)
      ++ "' against type '" ++ show v ++ "')"
  -- Introduce a fresh variable and check the body
  let var = newVar (keys ctx1) s
      e1Val = doApply v (Neutral (Var var) t1Val)
      ctx' = if s == var then
        extend ctx s (Decl t)
      else
        extend (extend ctx s (Decl t)) s (Val (Neutral (Var var) tVal))
  checkType ctx' dirs e e1Val

--  $\Sigma$ -type constructor (pair)
(Pair p1 p2, Closure (Sigma _ t1 _) ctx1) -> do
  let t1Val = eval ctx1 t1
      e1Val = evalClosure v (eval ctx p1)
  -- Check each component
  checkType ctx dirs p1 t1Val
  checkType ctx dirs p2 e1Val

-- Coproduct type former
(Sum ty1 ty2, Universe) -> do
  checkType ctx dirs ty1 Universe
  checkType ctx dirs ty2 Universe

--  $\Sigma$ -type left injection
(InL t1, Sum ty1 _) -> do
  checkType ctx dirs t1 ty1

--  $\Sigma$ -type right injection
(InR t2, Sum _ ty2) -> do
  checkType ctx dirs t2 ty2

-- Restriction type
(e, Restr sys ty) -> do
  let eVal = eval ctx e
      phi = getSystemFormula sys
  checkType ctx dirs e ty
  -- Check for conversion under the formulas
  unless (convPartialDisj (keys ctx) phi dirs eVal (Sys sys)) $

```

```

    Left $ "term '" ++ show e ++ "' does not agree with '" ++
      show (Sys sys) ++ "' on " ++ show phi

-- System
(Sys sys,Partial phi ty) -> do
  -- Check that the formulas match
  let psis = keys sys
  mapM_ (checkConjFormula ctx) psis
  unless (eqFormulas dirs phi (Disj psis)) $
    Left $ show phi ++ " is not logically equivalent to "
      ++ show (Disj psis)
  -- Check conversion the partial elements in the system
  mapM_ (\(psi,t) -> checkTypePartialConj psi ctx dirs t ty) sys
  -- Check conversion at the intersections
  let eq_check = all (\((psi1,t1),(psi2,t2)) ->
    convPartialConj (keys ctx) (psi1 `meet` psi2) dirs
      (eval ctx t1) (eval ctx t2)
    ) [(x1,x2) | x1 <- sys, x2 <- sys, x1 /= x2]
  unless eq_check $
    Left "values are not adjacent"

-- Partial type former
(Partial phi ty,Universe) -> do
  checkDisjFormula ctx phi
  checkType ctx dirs ty Universe

-- Restriction type former
(Restr sys ty,Universe) -> do
  checkType ctx dirs ty Universe
  let tyVal = eval ctx ty
      phi    = getSystemFormula sys
  checkDisjFormula ctx phi
  -- Check the elements in the system
  mapM_ (\(conj,t) -> checkTypePartialConj conj ctx dirs t tyVal) sys

-- If no other rule match, try inferring the type and
-- check if it's compatible
otherwise -> do
  ty <- inferType ctx dirs term
  -- Check for sub-typing: `v` more general than `ty`
  unless (compTypes (keys ctx) dirs ty v) $
    Left $ "type '" ++ show v ++ "' expected, got term '" ++ show term
      ++ "' of type '" ++ show ty ++ "' instead"

-- Check compatibility (subtyping) between two partial or restriction types,
-- as specified by the typing rules: `v1` more general than `v2`
compTypes :: [Ident] -> DirEnv -> Value -> Value -> Bool
compTypes used dirs v1 v2 =
  -- Split the type and get eventual partial type formulas

```

```

-- (by default `True` in the other cases)
let (iphi,ity) = split v1
    (vphi,vty) = split v2
    syscheck   = case (v1,v2) of
        (Restr isys _,Restr vsys _) -> convPartialDisj used
            (getSystemFormula vsys) dirs (Sys isys) (Sys vsys)
        otherwise -> True
    -- Check sub-typing compatibility for restrictions, for the base
    -- types and for formulas in the case of partial types
in syscheck && conv used dirs ity vty && impDisj dirs vphi iphi

-- Check that the variables of the conjunctive formula are in the context
checkConjFormula :: Ctx -> ConjFormula -> Either ErrorString ()
checkConjFormula ctx cf = do
    let dom      = keys ctx
        support = vars cf
    unless (all (`elem` dom) support) $
        Left $ "formula '" ++ show cf ++ "' contains undeclared names"

-- Check that the variables of the disjunctive formula are in the context
checkDisjFormula :: Ctx -> DisjFormula -> Either ErrorString ()
checkDisjFormula ctx (Disj df) = mapM_ (checkConjFormula ctx) df

```

### 3.7 Main program

This last file is the one that handles input-output, using all the previous files to produce a full working interpreter of the type theory. We use the **State** monad to store some information across the iterations of the REPL loop, that is the current context, the last checked term and the list of locked names.<sup>100</sup> For each declaration or definition given in input (typed from the user or from a file), first the parser is called to produce the abstract syntax, then `checkSingleToplevel` checks name shadowing and lastly `checkSingleToplevel'` calls the type-checker to ascertain that the input is correct, finally adding the declaration or definition to the context. When an example is given, that is simply a term, after the syntactical checks the type-checker is called to infer its type. The program supports some commands, starting with ‘:’, such as .

- `:help` (print help)
- `:q` (quit the program)
- `:ans` (print the last term checked)

<sup>100</sup>If a name is locked, then its definition in the context is temporarily erased, keeping only the type declaration. By unlocking the name, the definition is added again.

- :ctx (print the current context)
- :clear  $id_1 \dots id_n$  (remove the given identifiers from the context, recursively)
- :lock  $id_1 \dots id_n$  (lock the given names)
- :unlock  $id_1 \dots id_n$  (unlock the given names)
- :unlockall (unlock every currently locked name)
- :printlock (show all locked names)

Source file MainCTT.hs.

```

module Main where

import System.IO ( hFlush, stdout )
import System.Environment ( getArgs )
import System.Exit      ( exitSuccess )
import Control.Monad.State
import Data.List ( intercalate )
import Data.Maybe ( isJust )

import ParCTT      ( pTerm, pToplevel, pProgram, myLexer )

import Ident
import Interval
import CoreCTT
import Eval
import TypeChecker

type Err = Either String

-- Current context, last term checked, list of locked names
type ReplState = (Ctx,Term,[Ident])

-- Initial state
initReplState :: ReplState
initReplState = ([],Zero,[])

-- Read from a file and call `run`
runFile :: FilePath -> StateT ReplState IO Bool
runFile f = do
  putStrLnIO $ "Reading file " ++ f
  contents <- liftIO . readFile $ f
  res <- run contents
  liftIO . when res . putStrLn $ "\nFile " ++ f ++ " loaded successfully"
  return res

```

```

-- Parse and call `checkProgram`
run :: String -> StateT ReplState IO Bool
run s = case pProgram ts of
  Left err -> do
    liftIO $ putStrLn "\nParse failed!"
    liftIO $ showErr err
    return False
  Right program -> do
    checkProgram program
  where
    ts = myLexer s

-- Check a whole program, by type-checking every top-level
-- declaration
checkProgram :: Program -> StateT ReplState IO Bool
checkProgram (Program []) = return True
checkProgram (Program (toplevel : decls)) = do
  res <- checkSingleToplevel topLevel
  if res then
    checkProgram (Program decls)
  else
    return False

-- Check if a term contains undeclared variables (True = OK)
checkVars :: Ctx -> Term -> Bool
checkVars ctx term = case term of
  Var s          -> isJust $ lookup s ctx
  Universe       -> True
  Abst s t e     -> checkVars ctx t &&
    checkVars (extend ctx s (Decl {-dummy-} Universe)) e
  TDef (s,t,e) t' -> checkVars ctx t &&
    checkVars (extend ctx s (Decl {-dummy-} Universe)) e &&
    checkVars (extend ctx s (Def t e)) t'
  App fun arg     -> checkVars ctx fun && checkVars ctx arg
  Sigma s t e     -> checkVars ctx t &&
    checkVars (extend ctx s (Decl {-dummy-} Universe)) e
  Pair t1 t2      -> checkVars ctx t1 && checkVars ctx t2
  Fst t           -> checkVars ctx t
  Snd t           -> checkVars ctx t
  Sum ty1 ty2     -> checkVars ctx ty1 && checkVars ctx ty2
  InL t1          -> checkVars ctx t1
  InR t2          -> checkVars ctx t2
  Split ty f1 f2 x -> checkVars ctx ty && checkVars ctx f1 &&
    checkVars ctx f2 && checkVars ctx x
  Nat             -> True
  Zero            -> True
  Succ t          -> checkVars ctx t
  Ind ty b s n    -> checkVars ctx ty && checkVars ctx b &&
    checkVars ctx s && checkVars ctx n

```

```

I          -> True
IO         -> True
I1         -> True
Sys sys    -> all (\phi -> all (`elem` keys ctx) (vars phi))
           (keys sys) && all (checkVars ctx) (elems sys)
Partial phi t    -> all (`elem` keys ctx) (vars phi) &&
           checkVars ctx t
Restr sys t      -> checkVars ctx (Sys sys) && checkVars ctx t
Comp fam phi i0 u b i -> checkVars ctx fam &&
           all (`elem` keys ctx) (vars phi) && checkVars ctx i0 &&
           checkVars ctx u && checkVars ctx b && checkVars ctx i

-- Check a single top-level declaration, calling `checkSingleToplevel`
-- Here we mostly check variables
checkSingleToplevel :: Toplevel -> StateT ReplState IO Bool
-- Example: infer its type
checkSingleToplevel (Example t) = do
  (ctx,_,_) <- get
  if not (checkTermShadowing (keys ctx) t) then do
    liftIO . showErr $ "term '" ++ show t ++ "' contains shadowed variables"
    return False
  else if not (checkVars ctx t) then do
    liftIO . showErr $ "term '" ++ show t ++ "' contains undeclared variables"
    return False
  else
    checkSingleToplevel' (Example t)
-- Add a declaration to the context
checkSingleToplevel decl@(Declaration s t) = do
  (ctx,_,_) <- get
  if not (checkTermShadowing (keys ctx) t) then do
    liftIO . showErr $ "term '" ++ show t ++ "' contains shadowed variables"
    return False
  else if not (checkVars ctx t) then do
    liftIO . showErr $ "term '" ++ show t ++ "' contains undeclared variables"
    return False
  else case lookup s ctx of
    Nothing -> checkSingleToplevel' decl
    Just _ -> do
      liftIO . showErr $ "context already contains name '" ++ show s ++ "'"
      return False
-- Add a definition to the context
checkSingleToplevel def@(Definition s t e) = do
  (ctx,_,_) <- get
  if not (checkTermShadowing (s : keys ctx) t &&
    checkTermShadowing (s : keys ctx) e) then do
    liftIO . showErr $ "definition of '" ++ show s
      ++ "' contains shadowed variables"
    return False
  else if not (checkVars ctx t && checkVars ctx e) then do

```

```

liftIO . showErr $ "definition of '" ++ show s
++ "' contains undeclared variables"
return False
else case lookup s ctx of
  Nothing -> checkSingleToplevel' def
  Just _ -> do
    liftIO . showErr $ "context already contains name '"
    ++ show s ++ "'"
    return False

checkSingleToplevel' :: Toplevel -> StateT ReplState IO Bool
checkSingleToplevel' (Example t) = do
  -- Get the context with the locked names (i.e. erasing definitions
  -- of locked names)
  (unlockedCtx,_,lockedNames) <- get
  let ctx = getLockedCtx lockedNames unlockedCtx
      ty = inferType ctx emptyDirEnv t
  case ty of
    Left err -> do
      liftIO $ showErr err
      return False
    Right tyVal -> do
      printLnIO $ "\n'" ++ show t ++ "' has (inferred) type '"
      ++ show (readBack (keys ctx) tyVal) ++ "'"
      -- Since `t` typechecks, `t` must have a normal form
      let norm = normalize ctx t
      printLnIO $ "'" ++ show t ++ "' reduces to '" ++ show norm ++ "'"
      -- Update `ans`
      put (ctx,t,lockedNames)
      return True

checkSingleToplevel' (Declaration s t) = do
  -- Get the context with the locked names (i.e. erasing definitions
  -- of locked names)
  (unlockedCtx,_,lockedNames) <- get
  let ctx = getLockedCtx lockedNames unlockedCtx
  printLnIO $ "\nType-checking term '" ++ show s ++ "' of type '"
  ++ show t ++ "'"
  case addDecl ctx (s,t) of
    Left err -> do
      liftIO . showErr $ err
      return False
    Right ctx' -> do
      printLnIO "Declaration check OK!"
      -- Update `ans`
      put (ctx',t,lockedNames)
      return True

checkSingleToplevel' (Definition s t e) = do

```



```

-- Get the context with the locked names (i.e. erasing definitions
-- of locked names)
(unlockedCtx,_,lockedNames) <- get
let ctx = getLockedCtx lockedNames unlockedCtx
printlnIO $ "\nType-checking term '" ++ show s ++ "' of type '"
  ++ show t ++ "' and body '" ++ show e ++ "'"
case addDef ctx (s,t,e) of
  Left err -> do
    liftIO . showErr $ err
    return False
  Right ctx' -> do
    printlnIO "Type check OK!"
    -- Update `ans`
    put (ctx',e,lockedNames)
    return True

-- Main REPL (infinite) loop
doRepl :: StateT ReplState IO ()
doRepl = do
  (ctx,ans,lockedNames) <- get
  printIO "\n> "
  s <- liftIO getLine
  let w = words s
  case w of
    -- Quit
    [":q"] -> do
      liftIO exitSuccess
    -- Print last type-checked term
    [":ans"] -> do
      printlnIO $ show ans
    -- Show context (with locked names)
    [":ctx"] -> do
      liftIO . printCtxLn $ getLockedCtx lockedNames ctx
    -- Delete from context the given names (and also the ones
    -- that depend on them)
    ":clear" : ids -> do
      let ctx' = foldl removeFromCtx ctx (map Ident ids)
      put (ctx',ans,lockedNames)
    -- Lock a list of identifiers
    ":lock" : ids -> do
      let ids' = map Ident ids
          isInCtx = (`elem` (keys ctx))
          idsToAdd = filter isInCtx ids'
          idsWrong = filter (not . isInCtx) ids'
      when (length idsWrong > 0) $
        printlnIO $ "identifier(s) " ++ intercalate ", " (map show idsWrong)
          ++ " not found in the current context"
      let lockedNames' = idsToAdd ++ lockedNames
      put (ctx,ans,lockedNames')

```

```

-- Unlock a list of identifiers
":unlock" : Idents -> do
  let lockedNames' = filter (`notElem` map Ident idents) lockedNames
  put (ctx,ans,lockedNames')
-- Clear the list of locked identifiers
":unlockall" ->
  put (ctx,ans,[])
-- Show the locked identifiers
":printlock" ->
  putStrLnIO $ "Locked names are: " ++ intercalate ", " (map show lockedNames)
-- Show help menu
":help" -> do
  liftIO printUsage
-- Unknown command
(':' : _ ) : _ ->
  putStrLnIO "Command not found. Type :help"
-- Otherwise, check a new declaration
otherwise -> do
  let ts = myLexer s
  case pToplevel ts of
    Left err -> do
      putStrLnIO "\nParse failed!"
      liftIO . showErr $ err
    Right toplevel -> do
      _ <- checkSingleToplevel toplevel
      return ()
doRepl -- Repeat

-- Add a definition to the current context
addDef :: Ctx -> (Ident,Term,Term) -> Either ErrorString Ctx
addDef ctx (s,t,e) = do
  checkType ctx emptyDirEnv t Universe -- Check that `t` is a type
  let tVal = eval ctx t
  checkType ctx emptyDirEnv e tVal -- Check that `e` has type `t`
  Right $ extend ctx s (Def t e)

-- Add a definition to the current context
addDecl :: Ctx -> (Ident,Term) -> Either ErrorString Ctx
addDecl ctx (s,t) = do
  -- Check that `t` is a type or the interval
  unless (t == I) $ checkType ctx emptyDirEnv t Universe
  Right $ extend ctx s (Decl t)

-- Lock each given identifier in the context,
-- i.e. erase its eventual definition from the context
getLockedCtx :: [Ident] -> Ctx -> Ctx
getLockedCtx idents ctx0 = foldr getLockedCtx' ctx0 idents
  where
    getLockedCtx' :: Ident -> Ctx -> Ctx

```

```

getLockedCtx' s ((s',Def ty def) : ctx) =
  if s == s' then (s',Decl ty) : ctx
    else (s',Def ty def) : getLockedCtx' s ctx
getLockedCtx' s ((s',Decl ty) : ctx) =
  (s',Decl ty) : getLockedCtx' s ctx
getLockedCtx' _ ctx = ctx

-- Print the context, line by line
printCtxLn :: Ctx -> IO ()
printCtxLn ctx = mapM_ (putStrLn . showEntry) (reverse ctx)

-- Print an error
showErr :: String -> IO ()
showErr err = putStrLn $ "\nError: " ++ err

main :: IO ()
main = do
  printUsage
  args <- getArgs
  case args of
    -- No files given: start the REPL loop
    [] -> do
      evalStateT doRepl initReplState
      exitSuccess
    -- Some files given: parse each file, then start the REPL loop
    fs -> evalStateT (
      do
        -- `b` is the result of the type-check of each file
        res <- foldM (\b fp -> (b &&) <$> runFile fp) True fs
        liftIO $ unless res exitSuccess
        (ctx,_,_) <- get
        printLnIO "\nCurrent context is:"
        liftIO . printCtxLn $ ctx
        doRepl
      ) initReplState

-- Print help menu
printUsage :: IO ()
printUsage = do
  putStr $ unlines
    [ " ----- "
    , "| Usage: ./CTT <file> .. <file>    load and type-check files          |"
    , "\item                               then start a REPL                  |"
    , "| Commands:                          |"
    , "\item x : <term>                      add declaration of 'x' to the context |"
    , "\item x : <term> = <term>              add definition of 'x' to the context |"
    , "\item <term>                          infer type of t and normalize it    |"
    , "\item :help                          print help                          |"
    , "\item :q                             quit                                |"
    ]

```

```

\item :ans                print the last term used                | "
\item :ctx                print current context                  | "
\item :clear <id> .. <id>  remove <id>'s from context (recursively) | "
\item :lock <id> .. <id>   lock <id>'s definition                | "
\item :unlock <id> .. <id> unlock <id>'s definition              | "
\item :unlockall          unlock every currently locked definition | "
\item :printlock          print locked definitions               | "
    , " ----- "
    ]
    hFlush stdout

-- Auxiliary printing functions
printIO :: String -> StateT ReplState IO ()
printIO s = liftIO $ do
    putStr s
    hFlush stdout

printlnIO :: String -> StateT ReplState IO ()
printlnIO s = printIO $ s ++ "\n"

```

# Appendix A

## Yoneda lemma

In this section we briefly state and prove a basic version of the (contravariant) Yoneda lemma, which is used in chapter 2. With  $\hat{\mathcal{C}}$  we denote the presheaf category on  $\mathcal{C}$ , i.e. the functor category  $[\mathcal{C}^{\text{op}}, \mathbf{Set}]$ , which has presheaves on  $\mathcal{C}$  as objects and natural transformations between them as arrows.

**Definition A.1** (Yoneda embedding). *Let  $\mathcal{C}$  be a locally small category, i.e. such that  $\text{Hom}_{\mathcal{C}}(I, J)$  is a set for all  $I, J \in \mathcal{C}$ . The Yoneda embedding is the functor  $y : \mathcal{C} \rightarrow \hat{\mathcal{C}}$  given by*

- $(yI)(J) = \text{Hom}_{\mathcal{C}}(J, I)$  for each object  $J \in \mathcal{C}$ ;
- $(yI)_f : \text{Hom}_{\mathcal{C}}(K, I) \rightarrow \text{Hom}_{\mathcal{C}}(J, I)$  which is defined by  $h \mapsto fh$ ,<sup>101</sup> for each morphism  $f : J \rightarrow K$  of  $\mathcal{C}$ .

**Theorem A.2** (Yoneda lemma). *Let  $\mathcal{C}$  be a locally small category and  $\Gamma$  a presheaf on  $\mathcal{C}$ , i.e. a functor  $\Gamma : \mathcal{C}^{\text{op}} \rightarrow \mathbf{Set}$ . Then for each  $I \in \mathcal{C}$  there is a bijection*

$$\Gamma(I) \cong \text{Hom}_{\hat{\mathcal{C}}}(yI, \Gamma).$$

*Proof.* If  $\alpha : yI \rightarrow \Gamma$  is a natural transformation, with components  $\alpha_J : \text{Hom}_{\mathcal{C}}(J, I) \rightarrow \Gamma(J)$  for each  $J \in \mathcal{C}$ , then the naturality condition holds for each  $f : J \rightarrow K$ , i.e.

$$\alpha_J \circ (yI)_f = \Gamma_f \circ \alpha_K \tag{*}$$

which means that for each  $h : K \rightarrow I$ ,

$$\alpha_J(fh) = \Gamma_f(\alpha_K h).$$

Exploiting this, we now show how every element of  $\Gamma(I)$  determines a natural

---

<sup>101</sup>Remember that we use the applicative order, i.e.  $fh = h \circ f$ .

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{C}}(K, I) & \xrightarrow{(\mathbf{y}I)_f} & \mathrm{Hom}_{\mathcal{C}}(J, I) \\
\alpha_K \downarrow & & \downarrow \alpha_J \\
\Gamma(K) & \xrightarrow{\Gamma_f} & \Gamma(J)
\end{array}$$

Figure A.1: Naturality diagram.

transformation between  $\mathbf{y}I$  and  $\Gamma$ , and vice versa; furthermore, we show that these correspondences are each the inverse of the other.

- Given  $\alpha : \mathbf{y}I \rightarrow \Gamma$ , we get  $\hat{\alpha} = \alpha_I(\mathbf{1}_I) \in \Gamma(I)$  since  $\alpha_I : \mathrm{Hom}_{\mathcal{C}}(I, I) \rightarrow \Gamma(I)$ .
- Given  $x \in \Gamma(I)$  and  $f : J \rightarrow I$ , we get  $\Gamma_f : \Gamma(I) \rightarrow \Gamma(J)$  so that  $\Gamma_f(x) \in \Gamma(J)$ . Therefore we set  $\tilde{x}_J(f) = \Gamma_f(x)$ . We now prove that  $\tilde{x} = (\tilde{x}_J)_{J \in \mathcal{C}}$  is a natural transformation  $\mathbf{y}I \rightarrow \Gamma$ . Indeed, given  $g : K \rightarrow J$ , we shall prove that  $\Gamma_g \circ \tilde{x}_J = \tilde{x}_K \circ (\mathbf{y}I)_g$ , which means that for all  $h : J \rightarrow I$ ,

$$\Gamma_g(\tilde{x}_J(h)) = \tilde{x}_K((\mathbf{y}I)_g h)$$

must be proved; the left side is  $\Gamma_g(\tilde{x}_J(h)) = \Gamma_g(\Gamma_h(x)) = \Gamma_{gh}(x)$ ; the right side is  $\tilde{x}_K((\mathbf{y}I)_g h) = \tilde{x}_K(gh) = \Gamma_{gh}(x)$ .

- (Second applied to first) If  $x \in \Gamma(I)$ , then

$$\hat{\tilde{x}} = \tilde{x}_I(\mathbf{1}_I) = \Gamma_{\mathbf{1}_I}(x) = \mathbf{1}_{\Gamma(I)}(x) = x.$$

- (First applied to second) If  $\alpha : \mathbf{y}I \rightarrow \Gamma$  and  $f : J \rightarrow I$ , then

$$(\hat{\tilde{\alpha}})_J(f) = \Gamma_f(\hat{\alpha}) = \Gamma_f(\alpha_I(\mathbf{1}_I)) = \alpha_J(f(\mathbf{1}_I)) = \alpha_J(f).$$

where the second-last equality is witnessed by  $(*)$  (with  $K = I$ ).

□

**Remark A.3.** *Actually we could say more about the Yoneda embedding  $\mathbf{y}$ , as it can be shown that:*

1.  $\Gamma(I) \cong \mathrm{Hom}_{\hat{\mathcal{C}}}(\mathbf{y}I, \Gamma)$  is a natural isomorphism both in  $I \in \mathcal{C}$  and  $\Gamma \in \hat{\mathcal{C}}$ .
2.  $\mathbf{y}$  is a fully faithful functor.

We refer to [Lei14] for further details, since these additional properties are not used in this thesis.

# Appendix B

## The subobject classifier

Here we introduce a categorical construction, called *subobject classifier*, that generalizes the set of truth values  $\{0, 1\}$  in the category of sets to arbitrary categories, allowing to describe ‘subobjects’ of any object  $X$  as morphisms from  $X$  to the subobject classifier, in the same manner as subsets of a set  $X$  can be described by their characteristic function, i.e. functions  $X \rightarrow \{0, 1\}$ .

Although the subobject classifier is not necessary for the development of partial and restriction types (section 2.4.2), it provides some useful insights. We follow the description given in [MLM92].

**Definition B.1** (Subobject). *If  $X$  is an object in a category  $\mathcal{C}$ , a subobject of  $\mathcal{C}$  is an equivalence class of monomorphisms  $m : U \rightarrowtail X$ .<sup>102</sup> The set of subobjects of  $X$  is denoted with  $\text{Sub}_{\mathcal{C}}(X)$ .*

**Definition B.2** (Subobject classifier). *Let  $\mathcal{C}$  be a category with a terminal object  $1$ . An object  $\Omega \in \mathcal{C}$  is said to be a subobject classifier for  $\mathcal{C}$  if there exists a morphism  $\text{true} : 1 \rightarrow \Omega$  such that for each monomorphism  $j : U \rightarrowtail X$  there exists a unique  $\phi : X \rightarrow \Omega$  such that the commutative diagram*

$$\begin{array}{ccc} U & \xrightarrow{!} & 1 \\ j \downarrow & & \downarrow \text{true} \\ X & \xrightarrow{\phi} & \Omega \end{array}$$

*is a pullback.*<sup>103</sup>

---

<sup>102</sup>With a common abuse of language, we also say that  $m$  is a subobject when we really mean the equivalence class of  $m$ .

<sup>103</sup>We denote with ‘!’ the unique morphism from an object to the terminal object  $1$ .

The subobject classifier, if it exists, is unique up to isomorphism (see [Gol79]) and it holds that

$$\text{Sub}_{\mathcal{C}}(X) \cong \text{Hom}_{\mathcal{C}}(X, \Omega).$$

**Example B.3.** *In the category of sets, the subobject classifier is the set of truth values, i.e.  $\Omega = \{0, 1\}$ . The function **true** ‘chooses’ the true value, that is  $\text{true}(\star) = 1$ . If  $j : U \rightarrowtail X$ , then  $j(U) \subseteq X$  and we can identify  $j(U)$  with  $U$ ; the morphism  $X \rightarrow \Omega$  is obviously the characteristic function of  $U$ , which makes the inner diagram commute. It is easy to see that the diagram is a pullback.*

$$\begin{array}{ccc} U & \xrightarrow{\quad ! \quad} & \{\star\} \\ \downarrow j & & \downarrow \text{true} \\ X & \xrightarrow{\quad \chi_U \quad} & \{0, 1\} \end{array}$$

We now start to investigate the existence of the subobject classifier in presheaf categories; first we introduce a useful concept which is the particular case of subobjects in functor categories.

**Definition B.4** (Subfunctor). *Let  $\mathcal{C}$  be a small category, with presheaves  $Q, P \in \hat{\mathcal{C}}$ . Then  $Q$  is said to be a subfunctor of  $P$  if:*

1. *For each  $I \in \mathcal{C}$ ,  $Q(I) \subseteq P(I)$ ;*
2. *For each  $f : J \rightarrow I$ ,  $Q_f = P_f \upharpoonright_{Q(I)}$ .*

**Remark B.5.** *If  $Q$  is a subfunctor of  $P$ , then it is clear that the inclusion  $i : Q \hookrightarrow P$  is a monomorphism. Vice versa, if  $\theta : Q \rightarrowtail P$  is a natural transformation which is a monomorphism, then  $\theta(I) : Q(I) \rightarrow P(I)$  is injective. Let  $Q'$  be the functor defined by  $Q'(I) = \text{Im } \theta(I)$  on objects and by the induced maps on morphisms;  $Q'$  is equivalent as a subobject to  $Q$  and is a subfunctor of  $P$ .*

Suppose that there exists a subobject classifier  $\Omega$  in the presheaf category  $\hat{\mathcal{C}}$ ; then it must hold that

$$\text{Sub}_{\hat{\mathcal{C}}}(\text{Hom}_{\mathcal{C}}(-, I)) \cong \text{Hom}_{\hat{\mathcal{C}}}(\text{Hom}_{\mathcal{C}}(-, I), \Omega) \cong \Omega(I)$$

where the last step is justified by the Yoneda lemma (see appendix A). Therefore,

$$\Omega(I) \cong \{Q \mid Q \text{ is a subfunctor of } \text{Hom}_{\mathcal{C}}(-, I)\}.$$



To best understand this definition, let us introduce an alternative presentation of subfunctors, called *sieves*.

**Definition B.6** (Sieve). *A sieve on  $I \in \mathcal{C}$  is a set of morphisms with codomain  $I$  such that for all  $h : K \rightarrow J$ ,  $f \in S \implies hf \in S$ .*

$$K \xrightarrow{h} J \xrightarrow{f} I$$

We now show that every sieve on  $I$  corresponds to a subfunctor of  $\mathbf{Hom}_{\mathcal{C}}(-, I)$ , and vice versa.

- If  $Q$  is a subfunctor of  $\mathbf{Hom}_{\mathcal{C}}(-, I)$ , then  $S = \{f \mid \exists J \in \mathcal{C} \ f : J \rightarrow I, f \in Q(J)\}$  is a sieve; to see this, let  $f \in S$ , with  $f : J \rightarrow I$ ,  $f \in Q(J)$ ; if  $h : K \rightarrow J$ , then  $Q_h : Q(J) \rightarrow Q(K)$ , so that  $Q_h(f) = hf \in Q(K)$  and  $hf \in S$ .
- If  $S$  is a sieve on  $I$ , let  $Q$  be the functor defined by  $Q(J) = \{f \in S \mid f : J \rightarrow I\} \subseteq \mathbf{Hom}_{\mathcal{C}}(J, I)$  on objects and by the induced composition map on morphisms. Then  $Q$  is obviously a subfunctor of  $\mathbf{Hom}_{\mathcal{C}}(-, I)$ .

Therefore it makes sense to assert that

$$\begin{aligned} \Omega(I) &\cong \{Q \mid Q \text{ is a subfunctor of } \mathbf{Hom}_{\mathcal{C}}(-, I)\} \\ &\cong \{S \mid S \text{ is a sieve on } I\}. \end{aligned}$$

**Remark B.7.** *If  $g : J \rightarrow I$ , then a subobject of  $\mathbf{Hom}_{\mathcal{C}}(-, I)$  induces a subobject of  $\mathbf{Hom}_{\mathcal{C}}(-, J)$ , or in other words, a sieve  $S$  on  $I$  induces a sieve on  $J$  defined by*

$$S \cdot g = \{h \mid hg \in S\}.$$

Having already established  $\Omega(I) \cong \{S \mid S \text{ is a sieve on } I\}$ , using this last remark we finally define the subobject classifier  $\Omega$  on the presheaf category  $\hat{\mathcal{C}}$ .

**Definition B.8** (Subobject classifier on  $\hat{\mathcal{C}}$ ).

*Let  $\Omega \in \hat{\mathcal{C}}$  be defined by*

$$\Omega(I) = \{S \mid S \text{ is a sieve on } I\}$$

*on objects  $I \in \mathcal{C}$  and by*

$$\Omega_g : \Omega(I) \rightarrow \Omega(J), \quad S \mapsto S \cdot g$$

*on morphisms  $g : J \rightarrow I$ .*

The object  $\Omega$  comes along with the natural transformation  $\mathbf{true} : 1 \rightarrow \Omega$  defined by

$$\mathbf{true}_I : \{\star\} \rightarrow \Omega(I), \quad \star \mapsto \mathbf{Hom}_{\mathcal{C}}(-, I),$$

which associates to each object its *maximal sieve*. It is easy to see that  $\mathbf{true}$  is a natural transformation, since

$$\begin{array}{ccc} 1 & \xrightarrow{\mathbf{true}_I} & \Omega(I) \\ \downarrow 1 & & \downarrow \Omega_g \\ 1 & \xrightarrow{\mathbf{true}_J} & \Omega(J) \end{array} \quad \begin{array}{c} I \\ \uparrow g \\ J \end{array}$$

$$\Omega_g(\mathbf{true}_I(\star)) = \mathbf{true}_I(\star) \cdot g = \mathbf{true}_J(\star) \text{ holds.}$$

We now prove that  $\Omega$  really is the subobject classifier of  $\hat{\mathcal{C}}$ .

**Theorem B.9.** *The object  $\Omega$  just defined is a subobject classifier of  $\hat{\mathcal{C}}$ .*

*Proof.* Let  $j : Q \rightarrowtail P$  be a monomorphism, so that  $Q$  is a subfunctor of  $P$ . If  $f : J \rightarrow I$ , then  $P_f : P(I) \rightarrow P(J)$  is a function, so we put

$$\phi_I(x) = \{f : J \rightarrow I \mid P_f(x) \in Q(J)\}.$$

$$\begin{array}{ccc} Q & \xrightarrow{!} & 1 \\ \downarrow j & & \downarrow \mathbf{true} \\ P & \xrightarrow{\phi} & \Omega \end{array}$$

It is easily seen that:

- $\phi_I(x)$  is a sieve: let  $f \in \phi_I(x)$ , with  $f : J \rightarrow I$  and  $P_f(x) \in Q(J)$ . Let  $h : K \rightarrow J$  so that  $P_{hf} : P(I) \rightarrow P(K)$ ; then

$$P_{hf}(x) = P_h(\underbrace{P_f(x)}_{\in Q(J)}) \in Q(I)$$

since  $Q_h$  is the restriction of  $P_h$  to  $Q(J)$ . It follows that  $hf \in \phi_I(x)$ .

- $\phi$  is a natural transformation, as

$$\begin{array}{ccc}
 P(I) & \xrightarrow{\phi_I} & \Omega(I) \\
 P_g \downarrow & & \downarrow \Omega_g \\
 P(J) & \xrightarrow{\phi_J} & \Omega(J)
 \end{array}
 \qquad
 \begin{array}{c}
 I \\
 \uparrow g \\
 J
 \end{array}$$

$$\begin{aligned}
 \Omega_g(\phi_I(x)) &= \phi_I(x) \cdot g = \{h : K \rightarrow J \mid hg \in \phi_I(x)\} \\
 &= \{h : K \rightarrow J \mid P_{hg} \in Q(K)\}, \\
 \phi_J(P_g(x)) &= \{h : K \rightarrow J \mid P_h(P_g(x)) \in Q(K)\} \\
 &= \{h : K \rightarrow J \mid P_{hg} \in Q(K)\}.
 \end{aligned}$$

- The diagram is a pullback: if  $i : R \rightarrowtail P$  is a monomorphism, then  $R$  is a subfunctor of  $Q$  and so for any  $x \in R(I) \subseteq P(I)$ , we have (since the outer diagram commutes)

$$\text{true}_I(\star) = \phi_I(x),$$

that is  $P_f(x) \in Q(J)$  for all  $J \in \mathcal{C}$  and  $f : J \rightarrow I$ . Then  $x \in Q(I)$ , as  $P_{1_I}(x) = x \in Q(I)$ , so that  $R$  is a subfunctor of  $Q$  and  $m : R \rightarrowtail Q$  is the inclusion map. Indeed for the maps it holds that

$$Q_f \upharpoonright_{R(I)} = (P_f \upharpoonright_{Q(I)}) \upharpoonright_{R(I)} = P_f \upharpoonright_{(Q(I) \cap R(I))} = P_f \upharpoonright_{R(I)} = R_f.$$

$$\begin{array}{ccccc}
 R & & & & \\
 \swarrow m & & & & \searrow ! \\
 & Q & \xrightarrow{!} & 1 & \\
 \downarrow j & & & \downarrow \text{true} & \\
 & P & \xrightarrow{\phi} & \Omega & 
 \end{array}$$

- $\phi$  is the unique natural transformation  $\theta : P \rightarrow \Omega$  making the diagram a pullback: if  $x \in P(I)$  and  $f : J \rightarrow I$ , then commutativity means that  $P_f(x) \in Q(J)$  iff  $\theta_J(P_f(x)) = \text{true}_J(\star)$ , i.e.  $\theta_I(x) \cdot f = \text{true}_J(\star)$  by the naturality of  $\theta$ , which is equivalent to  $f \in \theta_I(x)$ . Therefore,

$$\theta_I(x) = \{f : J \rightarrow I \mid P_f(x) \in Q(J)\} = \phi_I(x)$$

and  $\theta = \phi$ .

□



# Appendix C

## Disjointness of coproduct injections

Here we prove, using the type theory of chapter 1, that `false` is not (propositionally) equal to `true`; actually, we prove a more general result stating that the injections of coproduct types are disjoint. We follow exactly the argument given in [Uni13] 2.12, to which we refer to further explanations. We have also proved the whole equivalence stated in [Uni13] 2.12.5, mimicking the given proof; this requires proving some auxiliary lemmas and the code can be found of the GitHub page of the thesis.<sup>104</sup>

First we define path types and transport.

$$\begin{aligned} \text{Path} &: [A : \mathbb{U}] \ A \rightarrow A \rightarrow \mathbb{U} \\ &= [A : \mathbb{U}][a, b : A][i : \mathbb{I}][i = 0 \mapsto a, i = 1 \mapsto b]A \end{aligned}$$

$$\text{refl} : [A : \mathbb{U}][a : A] \ \text{Path} \ A \ a \ a = [A : \mathbb{U}][a : A][i : \mathbb{I}] \ a$$

$$\begin{aligned} \text{transp} &: [F : \mathbb{I} \rightarrow \mathbb{U}] \ F \ 0 \rightarrow F \ 1 \\ &= [F : \mathbb{I} \rightarrow \mathbb{U}][a : F \ 0] \ \text{comp} \ F \ () \ 0 \ (\mathbb{I} \rightarrow []) \ a \ 1 \end{aligned}$$

$$\text{transport} : [B : \mathbb{U}][P : B \rightarrow \mathbb{U}][x, y : B] \ \text{Path} \ B \ x \ y \rightarrow P \ x \rightarrow P \ y$$

---

<sup>104</sup>There are some differences, since path types of CTT are not the same as path types of HOTT (since the computational rule for the induction principle holds only propositionally in CTT); for example, the transport along a reflexivity path is judgmentally equal to the identity function in HOTT, whereas in CTT it has to be proven as a proposition.

$$= [B : \mathbb{U}][P : B \rightarrow \mathbb{U}][x, y : B][pB : \text{Path } B \ x \ y] \\ \text{transp } ([i : \mathbb{I}] \ P \ (pB \ i))$$

Then we define the empty type,

$$\text{empty} : \mathbb{U} = [X : \mathbb{U}] \ X$$

the unit type,

$$\_i : \mathbb{I} \\ \text{unit} : \mathbb{U} = [_i = \_i \rightarrow \mathbb{Z}] \mathbb{N} \\ \text{tt} : \text{unit} = \mathbb{Z}$$

and the booleans.

$$\text{bool} : \mathbb{U} = \text{unit} + \text{unit} \\ \text{false} : \text{bool} = \text{inl } \text{tt} \\ \text{true} : \text{bool} = \text{inr } \text{tt}$$

Fixing an  $a_0 : A$ , we define the function  $\begin{cases} \text{code}_{A,B;a_0}(\text{inl } a) & \equiv \text{Path}_A(a_0, a) \\ \text{code}_{A,B;a_0}(\text{inr } b) & \equiv \text{empty} \end{cases}$ .

$$\text{code} : [A, B : \mathbb{U}][a_0 : A] \ A + B \rightarrow \mathbb{U} \\ = [A, B : \mathbb{U}][a_0 : A][x : A + B] \\ \text{split } (A + B \rightarrow \mathbb{U}) \ ([a : A] \ \text{Path } A \ a_0 \ a) \ (B \rightarrow \text{empty}) \ x$$

Then we give the encoding function.

$$\text{encode} : [A, B : \mathbb{U}][a_0 : A][x : A + B][p : \text{Path } (A + B) \ (\text{inl } a_0) \ x] \\ \text{code } A \ B \ a_0 \ x \\ = [A, B : \mathbb{U}][a_0 : A][x : A + B][p : \text{Path } (A + B) \ (\text{inl } a_0) \ x] \\ \text{transport } (A + B) \ ([x' : A + B] \ \text{code } A \ B \ a_0 \ x') \\ (\text{inl } a_0) \ x \ p \ (\text{refl } A \ a_0)$$

Finally, by specializing the encoding function, we get the injectivity and the disjointness of the constructors.

$$\text{injectivity} : [A, B : \mathbb{U}][a_0, a_1 : A] \\ \text{Path } (A + B) \ (\text{inl } a_0) \ (\text{inl } a_1) \rightarrow \text{Path } A \ a_0 \ a_1 \\ = [A, B : \mathbb{U}][a_0, a_1 : A] \ \text{encode } A \ B \ a_0 \ (\text{inl } a_1)$$

```
disjointness : [A, B : U][a0 : A][b : B]  
  Path (A + B) (inl a0) (inr b) → empty  
= [A, B : U][a0 : A][b : B] encode A B a0 (inr b)
```

```
true_neq_false : Path bool false true → empty  
= disjointness unit unit tt tt
```





# Bibliography

- [ABC<sup>+</sup>21] Carlo Angiuli, Guillaume Brunerie, Thierry Coquand, Robert Harper, Kuen-Bang Hou (Favonia), and Daniel R. Licata. Syntax and models of cartesian cubical type theory. *Mathematical Structures in Computer Science*, 31(4):424–468, 2021.
- [AW09] S. Awodey and M. A. Warren. Homotopy theoretic models of identity types. *Mathematical Proceedings of the Cambridge Philosophical Society*, 146(1):45–55, 2009.
- [Awo10] Steve Awodey. *Category Theory*. Oxford University Press, Inc., USA, 2nd edition, 2010.
- [Ben21] Bruno Bentzen. Naive cubical type theory. *Mathematical Structures in Computer Science*, 31(10):1205–1231, 2021.
- [CCHM15] Cyril Cohen, Thierry Coquand, Simon Huber, and Anders Mörtberg. Cubical Type Theory: a constructive interpretation of the univalence axiom. In *21st International Conference on Types for Proofs and Programs*, number 69 in 21st International Conference on Types for Proofs and Programs, page 262, Tallinn, Estonia, May 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
- [Coq96] Thierry Coquand. An algorithm for type-checking dependent types. *Science of Computer Programming*, 26(1):167–177, 1996.
- [Gol79] Robert Goldblatt. *Topoi, the categorical analysis of logic*. Elsevier North-Holland Amsterdam, 1979.
- [GSA<sup>+</sup>22] Daniel Gratzer, Jonathan Sterling, Carlo Angiuli, Thierry Coquand, and Lars Birkedal. Controlling unfolding in type theory, 2022.
- [GTL89] Jean-Yves Girard, Paul Taylor, and Yves Lafont. *Proofs and Types*. Cambridge University Press, USA, 1989.

- [Hof97] Martin Hofmann. Syntax and semantics of dependent types. In *Semantics and Logics of Computation*, pages 79–130. Cambridge University Press, 1997.
- [How80] William Alvin Howard. The formulae-as-types notion of construction. In Haskell Curry, Hindley B., Seldin J. Roger, and P. Jonathan, editors, *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus, and Formalism*. Academic Press, 1980.
- [HS96] Martin Hofmann and Thomas Streicher. The groupoid interpretation of type theory. In *In Venice Festschrift*, pages 83–111. Oxford University Press, 1996.
- [Hub16] Simon Huber. *Cubical Interpretations of Type Theory*. PhD thesis, University of Gothenburg, 2016.
- [KL21] Krzysztof Kapulkin and Peter LeFanu Lumsdaine. The Simplicial Model of Univalent Foundations (after Voevodsky). *J. Eur. Math. Soc.*, page 2071–2126, 2021.
- [Lan64] P. J. Landin. The Mechanical Evaluation of Expressions. *The Computer Journal*, 6(4):308–320, 01 1964.
- [Lei14] T. Leinster. *Basic Category Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2014.
- [Mil78] Robin Milner. A theory of type polymorphism in programming. *Journal of Computer and System Sciences*, 17(3):348–375, 1978.
- [ML75] Per Martin-Löf. An intuitionistic theory of types: predicative part. In H.E. Rose and J.C. Shepherdson, editors, *Logic Colloquium '73, Proceedings of the Logic Colloquium*, volume 80 of *Studies in Logic and the Foundations of Mathematics*, pages 73–118. North-Holland, 1975.
- [MLM92] Saunders Mac Lane and Ieke Moerdijk. *Sheaves in Geometry and Logic a First Introduction to Topos Theory*. Springer New York, 1992.
- [OP18] Ian Orton and Andrew M. Pitts. Axioms for modelling cubical type theory in a topos. *Log. Methods Comput. Sci.*, 14(4), 2018.
- [Str91] T. Streicher. *Semantics of Type Theory: Correctness, Completeness, and Independence Results*. Progress in Computer Science and Applied Logic Series. Springer, 1991.

- [SU06] Morten Heine Sørensen and Paweł Urzyczyn. *Lectures on the Curry-Howard Isomorphism*, volume 149 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, 2006.
- [Uni13] The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. <https://homotopytypetheory.org/book>, Institute for Advanced Study, 2013.
- [vBJ77] L. van Benthem Jutting. *Checking Landau’s “Grundlagen” in the Automath system*. PhD thesis, StichtingMathematisch Centrum, 1977.
- [Voe06] Vladimir Voevodsky. A very short note on homotopy  $\lambda$ -calculus, 2006.
- [Wan21] Qufei Wang. A Haskell Implementation for a Dependent Type Theory with Definitions. Master’s thesis, Department of Computer Science and Engineering, 2021.