HAL
open science

Representing Agda and coinduction in the $\lambda\Pi$-calculus modulo rewriting

Thiago Felicissimo

▶ **To cite this version:**

Thiago Felicissimo. Representing Agda and coinduction in the $\lambda\Pi$-calculus modulo rewriting. Logic in Computer Science [cs.LO]. 2021. hal-03343699

HAL Id: hal-03343699

https://inria.hal.science/hal-03343699v1

Submitted on 14 Sep 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Representing Agda and coinduction in the λΠ-calculus modulo rewriting

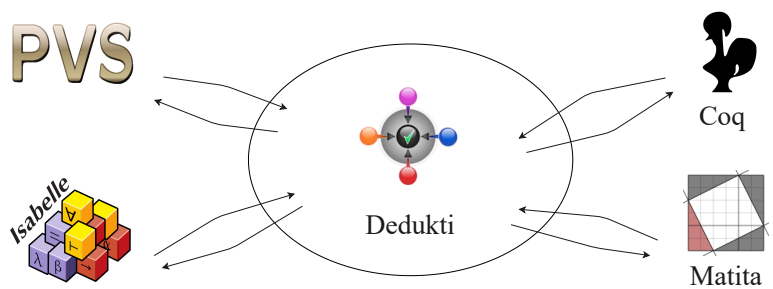
Thiago Felicissimo

MPRI Master 2 Internship from March 2021 to August 2021
Supervised by Frédéric Blanqui and Gilles Dowek
Deducteam/Laboratoire Méthodes Formelles

General Context

One of the main achievements of the research community on proof and type systems is the development of proof assistants, which are put simply programming languages for doing formal proofs. They are very important today both in mathematics, for the development and verification of mathematical proofs, and also in computer science, for proving properties about algorithms and protocols.

However, as each proof assistant implements its own proof system, it is not possible to take a proof developed in one proof assistant and use it in another one, which leads to wasting time redoing a proof in multiple systems. It is thus becoming increasingly important to develop techniques allowing for proof system interoperability, that is, sharing proofs between systems.



Deducteam, an Inria research team located at the ENS Paris-Saclay, addresses this problem by developing a *logical framework* based on the λΠ-calculus modulo rewriting and implemented in Dedukti. Because of its strong expressivity, we can use it to represent the logics implemented in proof assistants in an unified way, which then makes much simpler to perform translations between them. Today, many translators from and into Dedukti are being developed, and the ultimate goal is to be able to translate any proof from a proof assistant to another (whenever possible, according to their logic's expressivity) by using Dedukti as an intermediate system.

Problem Studied

Agda is a proof assistant under active development nowadays, featuring a rich system and a very active user community. Therefore, it is important to understand how we can encode its logic in Dedukti. This problem was first addressed by Guillaume Genestier, who developed a prototype translator from Agda to Dedukti. However, the translator only handles a fragment of Agda, with many features missing, such as sized types, non-prenex universe polymorphism and coinduction. Moreover, until the beginning of this internship its development was halted, and it was not capable of using the newest versions of Agda or Dedukti.

Coinduction is a principle, or a proof technique, dual to induction and which allows to handle possibly infinite objects in a natural way, such as infinite lists, infinite trees, formal languages, non well-founded sets, etc. Because of its usefulness, it is increasingly being added to proof assistants, such as Coq, Isabelle, PVS and, of course, Agda. In order to be able to translate proofs by coinduction coming from multiple proof assistants it is thus important to first understand how to encode coinduction in Dedukti, a problem that had never been addressed before.

Proposed Contributions

During this internship, we studied the representation of Agda and coinduction in Dedukti. Among the techniques of implementing coinduction in proof assistants, Agda features two presentations: *musical coinduction* and *copattern coinduction*. Based on their internal syntax representation in Agda, we proposed an encoding of both presentations in Dedukti. We resumed the development of the Agda2Dedukti translator and extended it with the proposed encoding, allowing it to translate automatically proofs by coinduction into Dedukti.

We also proposed many other improvements to the translator. We updated it to the latest Agda version, and eliminated a dependency with an *ad hoc* branch which made updating the translator almost impractical. Moreover, we extended Agda2Dedukti with a version targeting Lambdapi, a new proof assistant that extends Dedukti with interactive proof development and which should replace it in the future.

Arguments Supporting Their Validity

For the first time, we can represent coinduction in Dedukti, which marks a starting point for sharing proofs by coinduction with other proof assistants. Using the improved translator, we have translated many coinductive definitions from Agda to Dedukti, which in the future can allow for their translation into other systems. For instance, we would be very interested to look at how proofs made with copattern-matching coinduction could be reused in Coq, as its negative coinductive types have a very similar principle.

Moreover, with the new Lambdapi version we make Agda proofs also available in this system, something that is essential given that Dedukti is probably going to be discontinued. This has also the additional interest of allowing us to verify the translated proofs both in Dedukti and in Lambdapi, increasing our confidence in that they are indeed correct.

Summary and Future Work

Coinduction is a very useful proof technique, present in many proof assistants but (until now) missing from Dedukti. We proposed a first representation of coinduction in Dedukti, which opens a new research direction aimed at sharing coinduction proofs between proof assistants. The translation of coinduction from Agda was implemented in Agda2Dedukti, whose development has been resumed, and this allowed us to translate in an automatic way many such proofs. However, our contribution also went further, as we extended Agda2Dedukti to work with Lambdapi and we updated the translator to work with the latest versions of Agda.

Our contributions open many interesting research directions we would like to explore. For instance, it is a natural next question to see how the translated proofs can be imported into other proof assistants. We could proceed as François Thiré, who in [9] exported a library of arithmetical proofs from Matita to other proof assistants, going through Dedukti.

Going in a different direction, there are still many features missing from the translator, such as sized types and non-prenex universe polymorphism. We already have a prototype of an encoding that concerns the later, but we still have to implement it and to prove its correctness.

Finally, our ultimate goal is to develop techniques to share Agda proofs with other proof assistants. This is a very interesting research problem as Agda, differently from most proof assistants, features a predicative type system, and completely mixes propositions with types. Therefore, it is of both theoretical and practical interest to build encodings between predicative and impredicative type theory, which would allow us to share proofs between Agda and the more traditional impredicative proof assistants, such as Coq, Isabelle, etc.

Acknowledgments

I would first like to thank Frédéric Blanqui and Gilles Dowek, who very thoroughly supervised my internship and accepted to be my PhD supervisors. I also need to thank Guillaume Genestier, the previous developer of Agda2Dedukti who introduced me to parts of its code. I would like to thank Jesper Cockx, an Agda developer who very kindly explained to me parts of the Agda codebase and helped me to fix problems with the translator, whose help was essential for my internship. Finally, I would also like to thank all members of Deducteam, who very warmly welcomed me into the team.

1 Background

In this section we present the theory on top of which we build our contribution. We start by presenting the $\lambda\Pi$-calculus modulo rewriting (or $\lambda\Pi/\mathcal{R}$-calculus), a logical framework developed and used at Deducteam for expressing logics and checking their proofs. This is followed by a look at coinduction and coinductive types. We then present the proof assistant Agda and detail some particularities of its type system. Finally, we review Agda2Dedukti, a prototype translator for Agda proofs developed by Guillaume Genestier and we detail the features of the proof assistant it is able to handle.

1.1 The $\lambda\Pi$-calculus modulo rewriting

1.1.1 Starting point: the λ-calculus with dependent types

The lambda-calculus with dependent types, or $\lambda\Pi$-calculus, was proposed in [14] as a logical framework in which many proof and type systems can be expressed. Its syntax is given by

$$A, B, M, N ::= x \in \mathcal{X} \mid c \in \mathcal{C} \mid \mathbf{Type} \mid \mathbf{Kind} \mid MN \mid \lambda x : A.M \mid \Pi x : A.B$$

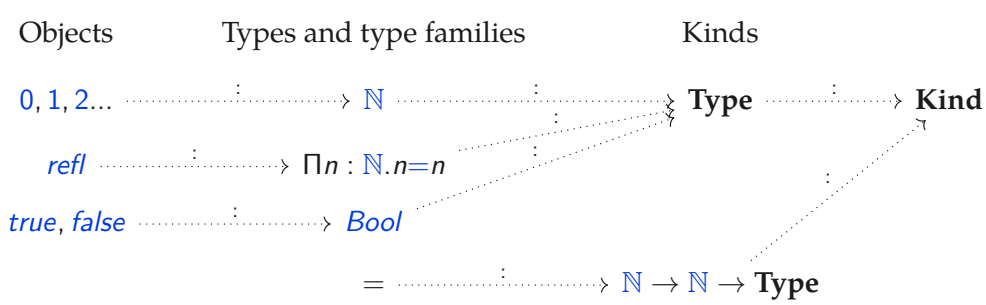
where $\mathcal{C}$ is an infinite set of constants and $\mathcal{X}$ is an infinite set of variables. We denote $\Lambda_{\lambda\Pi}$ the set of terms generated by this grammar. Conversion is defined as usual by β-equivalence, and we write $\Pi x : A.B$ as $A \to B$ when x does not appear in B.

A *context* Γ is a finite sequence of pairs $x : A$, where x is a variable and $A \in \Lambda_{\lambda\Pi}$, such that any variable can only appear once. A *signature* Σ is a finite sequence of pairs $c : A$, where c is a constant, $A \in \Lambda_{\lambda\Pi}$ and every constant can only appear once. As declaring constants in Σ is done all the time when building encodings of theories, we write them in blue to explicit the fact that they are added to the signature Σ. Typing in the $\lambda\Pi$-calculus is defined through judgments of the form $\Sigma; \Gamma \vdash M : A$, for $M, A \in \Lambda_{\lambda\Pi}$. We refer to Appendix B for the typing rules.

Intuitively, most terms can be separated into types (terms typed by **Type**) and objects (terms typed by a type). **Type** is the type of all the regular types, whereas **Kind** is there mostly for "administrative" reasons — its only use is to give a type to **Type** and to terms of the form $A_1 \to A_2 \to \ldots \to \mathbf{Type}$. For instance, if we want to have a symbol $\mathbb{N}$ to represent natural numbers and a constant 0 to represent the number zero, the only way to have $0 : \mathbb{N}$ is by declaring $\mathbb{N} : \mathbf{Type}$. Now suppose we had a type $Set : \mathbf{Type}$ of small types and $\mathbb{N} : Set$. Now we cannot declare $0 : \mathbb{N}$ because $\mathbb{N}$ is an object, and thus cannot type another term.

As the name says, the particularity of the $\lambda\Pi$-calculus when comparing with the λ-calculus is the addition of dependent types[1]. For instance, consider the successor function $S : \mathbb{N} \to \mathbb{N}$. For any element $n : \mathbb{N}$, the application $S\ n$ always gives a term that lives in $\mathbb{N}$. However, if we consider the equality type for natural numbers $= : \mathbb{N} \to \mathbb{N} \to \mathbf{Type}$ (written infix) and we consider a function $refl : \Pi n : \mathbb{N}.n = n$ giving a proof of $n = n$ for every n, then for each element n the application $refl\ n$ lives in a different type. Indeed, $refl\ 0$ is of type $0 = 0$ but not of type $1 = 1$, because it is not a proof of $1 = 1$. This is because the term $refl$ has a type which is dependent: its codomain depends on the argument given.

To resume things, we can give the following characterization of the hierarchy of the types in the $\lambda\Pi$-calculus.



1.1.2 The $\lambda\Pi$-calculus as a logical framework

The $\lambda\Pi$-calculus is well known for being in propositions as types correspondence with intuitionistic predicate logic[2]. Through the Curry-Howard correspondence, a proposition P is seen as a type P and the proofs of P are the inhabitants of this type. For instance, if P is a proposition, we represent the trivial proof of $P \Rightarrow P$ by $\lambda x : P.x$.

However, there is also a different approach to expressing predicate logic in the $\lambda\Pi$-calculus, known as *judgment as types*. Here, instead of representing a proposition directly as an inhabitant of **Type**, we declare a new type $Prop$: **Type** of propositions and a function $Proof : Prop \to$ **Type** associating to each proposition a type of its proofs. We then add other constants to express each connective. For instance, to add implication we add the constant $\Rightarrow : Prop \to Prop \to Prop$ (written infix) and the constants

$$\Rightarrow_{in} : \Pi a\ b : Prop.(Proof\ a \to Proof\ b) \to Proof\ (a \Rightarrow b)$$
$$\Rightarrow_{el} : \Pi a\ b : Prop.Proof\ a \to Proof\ (a \Rightarrow b) \to Proof\ b\,.$$

Therefore, whereas in the proposition as types approach we have that $\lambda x : P.x$ is a proof of $P \Rightarrow P$, in the judgment as types this is expressed by the term $\Rightarrow_{in} P\ P\ (\lambda x : Proof\ P.x)$.

The judgment as types approach was the one originally proposed by [14] to be used with the $\lambda\Pi$-calculus, when seen as a logical framework. Whereas the propositions as types puts this system in a "canonical" correspondence with predicate logic, when using the judgment as types approach we are able to encode many other systems that are not necessarily in any correspondence with the $\lambda\Pi$-calculus. Indeed, it turns out that by using this method we are capable of representing many other type systems with features that are orthogonal to those of the $\lambda\Pi$-calculus, such as System F. This can seem very surprising, as we are capable of expressing a system with polymorphism in a system without it.

If we take another look at the encoding of predicate logic, we can note an important point we did not yet discuss. A proof of $P \vdash P$ with a cut is represented through the Curry-Howard correspondence by $(\lambda x : P.x)\alpha_P$ — where α_P represents the proof of P in the context —, whereas through the judgment as types approach we get the term $\Rightarrow_{el} P\ P\ \alpha_P\ (\Rightarrow_{in} P\ P\ (\lambda x : Proof\ P.x))$. On the first case, we have $(\lambda x : P.x)\alpha_P \hookrightarrow \alpha_P$ and thus the term reduces to the representation of the cut-free proof. However, by using the last approach we lose this computational behavior, as the term $\Rightarrow_{el} P\ P\ \alpha_P\ (\Rightarrow_{in} P\ P\ (\lambda x : Proof\ P.x))$ is stuck and cuts do not reduce anymore.

As pointed out by Assaf[4], encodings such as this one, which lack preservation of computation, fail to be sound for more higher-order systems, such as for the Calculus of Constructions, as they cannot simulate proof reduction, β-reduction or other forms of computation. Thus, even though we are capable of encoding systems such as predicate logic and System F, the rigidity of the computation on the $\lambda\Pi$-calculus prevents us from going further.

1.1.3 Enriching computation in the $\lambda\Pi$-calculus

In 2007, Dowek and Cousineau considered in [8] an extension of the $\lambda\Pi$-calculus in which the notion of computation can be extended by adding rewriting rules. The syntax and the typing rules are kept the same, however they consider a more general notion of equivalence than only $\equiv_\beta$. More precisely, given a set $\mathcal{R}$ of rewriting rules — pairs of the form $cM_1..M_k \hookrightarrow N$, where c is a constant and $M_1, ..., M_k, N \in \Lambda_{\lambda\Pi}$ —, the relation $\equiv$ in the $\lambda\Pi/\mathcal{R}$-calculus is defined as the least equivalence relation containing $\equiv_\beta$ and the context and substitution closure of the rules in $\mathcal{R}$. Given a rewrite rule $cM_1..M_k \hookrightarrow N$, we normally call c its head symbol, $M_1..M_k$ its patterns and N its body. Note that when $\hookrightarrow_{\mathcal{R}\beta}$ is confluent and strongly normalizing, $\equiv$ is decidable, and so is type checking.

By addressing the poorness of computation in the $\lambda\Pi$-calculus and adding the possibility of extending rewriting, the $\lambda\Pi/\mathcal{R}$-calculus becomes capable of expressing much richer systems. In [8], Dowek and Cousineau showed that we can express any functional PTS in a sound and complete way, which was already not possible in the $\lambda\Pi$-calculus. Since then, researchers in Deducteam have built on top of this work and proposed encodings of much richer features in the $\lambda\Pi/\mathcal{R}$-calculus, such as inductive types[6], universe polymorphism[12], cumulativity[4][21], proof-irrelevance[15], etc.

1.1.4 Expressing logics in the $\lambda\Pi$-calculus modulo rewriting

Let's now take a second try at doing a judgment as types encoding of logic, but now using rewrite rules. In the $\lambda\Pi$-calculus, we declared a constant $\Rightarrow$ to represent implication and we had to declare constants $\Rightarrow_{in}$ and $\Rightarrow_{el}$ to represent the introduction and elimination rules for this connective. However, a much nicer approach is possible in the $\lambda\Pi/\mathcal{R}$-calculus: we can just declare a rewrite rule identifying proofs of $a \Rightarrow b$ with functions from $Proof\ a$ to $Proof\ b$.

$$Proof\ (a \Rightarrow b) \hookrightarrow Proof\ a \to Proof\ b$$

Now we do not need to declare constants for the introduction and elimination of implication, because these can be simulated by abstraction and application. For instance, a proof of $P \Rightarrow P$ can be simply given by the term $\lambda x : \mathit{Proof}\ P.x$. We also recover the computational behavior: the representation of the proof of $P \vdash P$ containing a cut is now given by $(\lambda x : \mathit{Proof}\ P.x)\alpha_P$. We thus have $(\lambda x : \mathit{Proof}\ P.x)\alpha_P \hookrightarrow \alpha_P$ and proofs with cuts now reduce to cut-free proofs.

To have a better understanding of how such encodings work, let's have a full look at the representation of predicate logic. However, before starting, we first establish a convention on how we represent encodings. First, declarations in the $\lambda\Pi$-calculus modulo rewriting are either constants, which are added to the signature Σ, or rewrite rules, which are added to $\mathcal{R}$. Therefore, each declaration will be marked either by (c-decl), meaning that the constant c is added to the signature Σ, or by (c-red), meaning that a rewrite rule concerning the constant c is added to $\mathcal{R}$. We also enclose such declarations by two vertical black bars, to explicit that we are making a constant or rule declaration.

We already have declared

$$\begin{array}{ll} \mathit{Prop} : \mathbf{Type} & (\mathit{Prop}\text{-decl}) \\ \mathit{Proof} : \mathit{Prop} \to \mathbf{Type} & (\mathit{Proof}\text{-decl}) \\ \Rightarrow : \mathit{Prop} \to \mathit{Prop} \to \mathit{Prop} & (\Rightarrow\text{-decl}) \\ \mathit{Proof}\ (a \Rightarrow b) \hookrightarrow \mathit{Proof}\ a \to \mathit{Proof}\ b & (\Rightarrow\text{-red}) \end{array}$$

which encodes the implicational fragment of predicate logic. To add first order quantification, we need to add a constant to represent the domain of discourse. If we want however to represent many-sorted predicate logic, in which we can have many sorts (that is, many domains of discourse), we can declare a type $\mathit{Set} : \mathbf{Type}$ which represents the set of sorts[3]. Now we can add multiple constants of type Set to represent different sorts of the language. For this example we only declare $\iota : \mathit{Set}$, which defines an one-sorted fragment of predicate logic. Finally, just like we had to declare a constant $\mathit{Proof} : \mathit{Prop} \to \mathbf{Type}$ which gives to each proposition a type of its proofs, we also need to declare $\mathit{El} : \mathit{Set} \to \mathbf{Type}$, associating to each sort of the language a type of its elements. In this case, sometimes we say that ι is a code in Set for the type $\mathit{El}\ \iota$.

$$\begin{array}{ll} \mathit{Set} : \mathbf{Type} & (\mathit{Set}\text{-decl}) \\ \iota : \mathit{Set} & (\iota\text{-decl}) \\ \mathit{El} : \mathit{Set} \to \mathbf{Type} & (\mathit{El}\text{-decl}) \end{array}$$

Now, given a sort x, we can declare universal quantification as a function which takes a term of type $\mathit{El}\ x \to \mathit{Prop}$ to a term Prop. More formally, we declare by ($\forall$-decl) the constant $\forall$, which allows us to represent $\forall_\iota x.P$ by $\forall\ \iota\ (\lambda x : \mathit{El}\ \iota.P)$. Finally, to have the proper introduction, elimination and computational behavior we add the rule ($\forall$-red), saying that an element of $\forall\ A\ P$ is simply a function taking an element x of type A and returning a proof of $P\ x$.

$$\begin{array}{ll} \forall : \Pi x : \mathit{Set}.(\mathit{El}\ x \to \mathit{Prop}) \to \mathit{Prop} & (\forall\text{-decl}) \\ \mathit{El}\ (\forall\ A\ P) \hookrightarrow \Pi x : \mathit{El}\ A.\mathit{Proof}\ (P\ x) & (\forall\text{-red}) \end{array}$$

It can be show that this set of constants and rewrite rules provides a sound and complete encoding of (minimal intuitionistic) predicate logic. Actually, in [7] researchers from Deducteam proposed a theory containing the one just presented which is capable of expressing in a unified way many systems and logics in the $\lambda\Pi/\mathcal{R}$-calculus, such as (intuitionistic and classic) predicate logic, higher order logic, the Calculus of Constructions, etc. We can thus see that the expressivity of the $\lambda\Pi/\mathcal{R}$-calculus makes it a very good candidate to be used as a logical framework and universal proof checker.

1.1.5 Dedukti and Lambdapi: implementing the $\lambda\Pi$-calculus modulo rewriting

Of course, if we want to use the $\lambda\Pi/\mathcal{R}$-calculus as a practical logical framework, we need to have some real implementation of it. Dedukti and its newer brother Lambdapi are two implementations of this system, and are used in practice to represent and check proofs. Many translators to and from Dedukti have already been developed or are in development, and concerns proof assistants such as Coq[4][10], HOL[20][5], PVS[13][15], Matita[21], etc. Most notably, the encyclopedia of formal proofs expressed in Dedukti Logipedia[9] is also one of the main projects at Deducteam.

1.2 Coinduction

Induction is a technique widely used in mathematics, which allows to define and reason about finitely constructed objects, such as integers, lists, and trees. The well-foundedness of these objects is key in order to have their induction principles. However, by dropping the well-foundedness condition we find new objects which, although less used, are actually very useful when doing mathematics. This new technique, called coinduction, allows us to represent possibly infinite objects, such as infinite lists, infinite trees but also formal languages[1] and non well-founded sets[3]. Because of its usefulness, coinduction is nowadays present in many proof assistants, such as Coq, Agda, and PVS. In order to understand coinduction and its relation to induction, we present its basis in this subsection.

1.2.1 (Co)Inductive Types

Inductive types are well known by most proof assistant users. By defining a type A and a set of constructors for A (satisfying a certain set of constraints, so we have a nice metatheory), the elements of the inductive type A are defined as the smallest set of terms stable by these constructors[4]. For instance, we can declare the type $\mathit{List}\ \mathbb{N}$ of lists of natural numbers, with constructors $[] : \mathit{List}\ \mathbb{N}$ for the empty list and $(_ :: _) : \mathbb{N} \to \mathit{List}\ \mathbb{N} \to \mathit{List}\ \mathbb{N}$ for adding an element to a list. Then we declare the elements of $\mathit{List}\ \mathbb{N}$ as the smallest set of terms closed by these constructors, that is, the least fixed point of the function

$$\phi : X \mapsto \{[]\} \cup \{n :: x \mid x \in X, n : \mathbb{N}\},$$

which can be expressed by $\cup_i \phi^i(\emptyset)$.These are exactly the terms that can be constructed by finitely applying the type's constructors and are exactly the lists of natural numbers.

Like many objects in mathematics, inductive types have a dual, called coinductive types. By defining a type A and a set of constructors for A, the elements of the coinductive type A are defined as the largest set of terms stable by these constructors. If now we interpret the same set of constructors for $\mathit{List}\ \mathbb{N}$ coinductively, we get the coinductive type $\mathit{Stream}\ \mathbb{N}$. Its elements form the largest set of terms closed by these constructors, that is, the greatest fixed point of the function

$$\phi : X \mapsto \{[]\} \cup \{n :: x \mid x \in X, n : \mathbb{N}\}.$$

which can be described by $\cap_i \phi^i(\Lambda)$, where Λ is the set of all terms.

When we consider only finite terms, both inductive and coinductive types collapse to the same object. However, if we allow for infinite terms, the set of elements of $\mathit{List}\ \mathbb{N}$ stays the same, but we now get new elements in the type $\mathit{Stream}\ \mathbb{N}$. For instance, the term $0 :: 0 :: 0...$ is stable by $0 :: _$ and thus it is an element of $\mathit{Stream}\ \mathbb{N}$. Therefore, in this setting the terms of type $\mathit{Stream}\ \mathbb{N}$ are finite and infinite lists — we could also drop the constructor $[]$, yielding another definition of streams in which they are always infinite. Therefore, in the rest of this subsection, we will consider Λ to represent the set of infinitary lambda terms, allowing us to have such infinite terms in the type $\mathit{Stream}\ \mathbb{N}$.

There is a very important point about this duality. If we analyze the equation $\mathit{List}\ \mathbb{N} = \cup_i \phi^i(\emptyset)$, this says that to construct the elements of $\mathit{List}\ \mathbb{N}$ we first start with the empty set and at each step we construct a new set of terms by adding the empty list and by applying $n :: _$ to previous terms. At the end we find exactly the terms which can be finitely (in at most i steps, for some i) built with these constructors.

On the other hand, the equation $\cap_i \phi^i(\Lambda)$ tells another story: we first start with all terms and at each step we build a new set by eliminating terms which are both different of the empty list and cannot be destructed as $n :: x$, for some term x in the previous set. At the end we find exactly the terms which can be destructed arbitrarily many times through the constructors.

The duality here is very clear: whereas elements of inductive types are built by constructing elements with constructors from scratch, elements of coinductive types are built by starting with everything and eliminating those which cannot be observed as constructors. Therefore, whereas induction is about building things, coinduction is about destructing them. We will also see on the next part that when looking at the recursion and corecursion principles this gets inverted: whereas the recursion principle allows us to destruct an element of an inductive type, the corecursion principle allows us to build an element into a coinductive type.

1.2.2 (Co)Recursion Principle

In order to understand how inductive and coinductive types can be used, we need to look at their principles. Although it would be faster to just state them, it is much more nicer to see how we can naturally recover them from a categorical semantics of induction and coinduction. This is a standard presentation and can be found in works such as in [22].

Consider the category **Set** of sets and the endofunctor $F : X \mapsto 1 + \mathbb{N} \times X$ with its obvious action on morphisms (note that F corresponds somewhat to the function ϕ seen previously). We can then build the category $\mathbf{Set}_F$ of F-algebras, whose objects are functions (e.g., morphisms in **Set**) of the form $\alpha_A : 1 + \mathbb{N} \times A \to A$ and morphisms in $\mathbf{Set}_F(\alpha_A, \alpha_B)$ are functions $f : A \to B$ making the following diagram commute.

$$\begin{tikzcd} 1 + \mathbb{N} \times A \arrow[r, "Ff"] \arrow[d, "\alpha_A"] & 1 + \mathbb{N} \times B \arrow[d, "\alpha_B"] \\ A \arrow[r, "f"] & B \end{tikzcd}$$

We can show that $\mathbf{Set}_F$ has as terminal object the set $\mathit{List}\ \mathbb{N}$ equipped with $\alpha_{\mathit{List}\ \mathbb{N}}$, defined by $* \mapsto []$ and $(n, l) \mapsto n :: l$. Then, by initiality, for each $\alpha_A : 1 + \mathbb{N} \times A \to A$ there is a unique function $\mathit{rec}\ \alpha_A$ making the following diagram commute.

$$\begin{tikzcd} 1 + \mathbb{N} \times \mathit{List}\ \mathbb{N} \arrow[r, "F(\mathit{rec}\ \alpha_A))"] \arrow[d, "\alpha_{\mathit{List}\ \mathbb{N}}"] & 1 + \mathbb{N} \times A \arrow[d, "\alpha_A"] \\ \mathit{List}\ \mathbb{N} \arrow[r, "\mathit{rec}\ \alpha_A"] & A \end{tikzcd}$$

We see the recursion principle naturally arise.

Recursion Principle: Each $\alpha_A : 1 + \mathbb{N} \times A \to A$ defines a unique function $\mathit{rec}\ \alpha_A : \mathit{List}\ \mathbb{N} \to A$;

A theorem by Lambek[16] ensures that $\alpha_{\mathit{List}\ \mathbb{N}}$ is actually an isomorphism, so we can actually inverse it and find an expression for $\mathit{rec}\ \alpha_A$ as $\alpha_A \circ F(\mathit{rec}\ \alpha_A) \circ \alpha^{-1}_{\mathit{List}\ \mathbb{N}}$. By separating the cases when the list is empty or not, we find

$$\begin{aligned} &(\mathit{rec}\ \alpha_A)\ [] = \alpha_A\ (*) \\ &(\mathit{rec}\ \alpha_A)\ (n :: l) = \alpha_A\ (n, (\mathit{rec}\ \alpha_A)\ l)\,. \end{aligned}$$

This is quite revealing: we see that defining the function α_A is actually pattern matching with primitive recursion. For instance, if we take $A = \mathbb{N}$ and $\alpha_{\mathbb{N}}$ defined by $* \mapsto 0$ and $(n, \mathit{len}) \mapsto \mathit{len} + 1$, we get

$$\begin{aligned} &(\mathit{rec}\ \alpha_{\mathbb{N}})\ [] = 0 \\ &(\mathit{rec}\ \alpha_{\mathbb{N}})\ (n :: l) = ((\mathit{rec}\ \alpha_{\mathbb{N}})\ l) + 1\,, \end{aligned}$$

the definition of the function *length* on lists.

Likewise, we can build the category $\mathbf{Set}^F$ of F-coalgebras, whose objects are functions of the form $\beta_A : A \to 1 + \mathbb{N} \times A$ and morphisms in $\mathbf{Set}^F(\beta_A, \beta_B)$ are functions $f : A \to B$ making the following diagram commute.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\beta_A"] & B \arrow[d, "\beta_B"] \\ 1 + \mathbb{N} \times A \arrow[r, "Ff"] & 1 + \mathbb{N} \times B \end{tikzcd}$$

We can then show that $\mathbf{Set}^F$ has as terminal object $\mathit{Stream}\ \mathbb{N}$ with $\beta_{\mathit{Stream}\ \mathbb{N}}$ defined by $[] \mapsto *$ and $n :: l \mapsto (n, l)$. Then, by finality, for each $\beta_A : A \to 1 + \mathbb{N} \times A$ there is a unique function $\mathit{corec}\ \alpha_A$ making the following diagram commute, thus yielding the corecursion principle.

$$\begin{tikzcd} A \arrow[r, "\mathit{corec}\ \beta_A"] \arrow[d, "\beta_A"] & \mathit{Stream}\ \mathbb{N} \arrow[d, "\beta_{\mathit{Stream}\ \mathbb{N}}"] \\ 1 + \mathbb{N} \times A \arrow[r, "F(\mathit{corec}\ \beta_A)"] & 1 + \mathbb{N} \times (\mathit{Stream}\ \mathbb{N}) \end{tikzcd}$$

Corecursion Principle: Each $\beta_A : A \to 1 + \mathbb{N} \times A$ defines a unique function $corec\ \beta_A : A \to Stream\ \mathbb{N}$.

We first remark a very important point. Whereas functions defined by recursion eliminates from an inductive type to an arbitrary type, corecursive functions do the opposite, eliminating from an arbitrary type to a coinductive one. Therefore, a function that eliminates from a coinductive type to an arbitrary one cannot be corecursive, just like a function that builds an inductive type from an arbitrary one cannot be recursive neither.

A second theorem by Lambek[16] ensures also that $\beta_{Stream\ \mathbb{N}}$ is an isomorphism, allowing us to write $corec\ \beta_A = \beta^{-1}_{Stream\ \mathbb{N}} \circ F(corec\ \beta_A) \circ \beta_A$. By doing a case analysis on the value of $\beta_A\ x$, we can then find the following expression for $corec\ \beta_A$.

$$(corec\ \beta_A)\ x = \begin{cases} [] & \text{if } \beta_A\ x = * \\ n :: ((corec\ \beta_A)(y)) & \text{if } \beta_A\ x = (n, y) \end{cases}$$

If we take, for instance, $A = \mathbb{N}$ and $\beta_A : n \mapsto (n, n+1)$ we get the equation

$$(corec\ \beta_{\mathbb{N}})\ n = n :: ((corec\ \beta_{\mathbb{N}})\ (n+1))\,,$$

which maps each integer n to the stream $n, n+1, n+2, \ldots$ — we will call this function *natStream*, as we will use it as a recurring example.

We could take this clause as a definition of *natStream*, however as it refers to itself in a non well-founded way, it is clear that it can cause non-termination issues. Even though coinductive types are non well-founded by definition, in practice when dealing with them in proof assistants and programming languages, we need to have a finitary way to represent these objects, as computers can only store finite data. We will discuss in one of the other parts how this problem can be handled.

1.3 The Agda proof assistant

Agda is a dependently-typed programming language developed in Sweden, mainly used as a proof assistant[19]. Its type system extends Martin-Löf Type Theory[17] with many features, such as (co) inductive types, universe polymorphism, sized types, etc. On the following, we take a look at some of its main characteristics. We refer to Appendix C for some more optional details.

1.3.1 Universes and type system

Just like Martin-Löf Type Theory, Agda features an infinite hierarchy of universes $Set_0 : Set_1 : Set_2 \ldots$, such that any type must be typed by a universe — note that universes themselves satisfy this criteria, as each universe Set_i is typed by the universe Set_{i+1}. We call the integers indexing the universes *universe levels*. We also might refer to universes as sorts. Most of the time, we write Set when referring to Set_0. We also note that, unlike Coq and Martin-Löf Type Theory, Agda does not feature comulativity by default, which is the ability of raising a type A living in a universe Set_i to the universe Set_j when $i < j$.[5]

Given two types $A : Set_i, B : Set_j$, with B possibly containing a free variable x of type A, we can form the dependent product type $(x : A) \to B$ (the Agda notation for $\Pi x : A.B$) using the following rule, where $\sqcup$ calculates the maximum between two levels.

$$\frac{\Gamma \vdash A : Set_i \qquad \Gamma, x : A \vdash B : Set_j}{\Gamma \vdash (x : A) \to B : Set_{i \sqcup j}}$$

Finally, one of the main particularities of Agda, when compared with most proof assistants such as Coq, HOL, Lean, etc, is that Agda's type system does not separate propositions from "normal" types. For instance, whereas in Coq the type $\mathbb{N}$ of natural numbers lives in Set and the proposition true $\top$ lives in $Prop$, in Agda both of them live in Set[6]. An important consequence is that, whereas in Coq the lambda term $\lambda x : A.x$ can either be the identity function for A (if $A : Set$) or a proof of $A \Rightarrow A$ (if $A : Prop$), in Agda the term $\lambda x : A.x$ is both the identity and a proof of $A \Rightarrow A$ at the same time. It all depends if we prefer to interpret A as a normal type or a type representing a proposition. Therefore, Agda implements a radical version of Curry-Howard, making absolutely no difference between types and propositions.

1.3.2 Inductive types, recursive functions and records

Like most proof assistants, Agda features inductive types. Though its presentation is mostly standard, its main peculiarity is that elimination principles are not defined explicitly. Rather, elimination from an inductive type is done by defining a recursive function with clauses (in a Haskell-like manner) which then needs to pass the language's termination and totality checkers. For instance, we can declare the inductive type of natural numbers by (Agda code bellow)

```
data Nat : Set where
  zero : Nat
  succ : Nat → Nat
```

and then define the sum of two natural numbers by induction on the first argument using the following definition.

```
_+_ : Nat → Nat → Nat
zero + x = x
(succ y) + x = succ (y + x)
```

Another particularity of Agda is that it also feature records, which are basically inductive types with one constructor and special treatment. For instance, we can define the type of dependent pairs with the following record definition.

```
record Σ (A : Set) (B : A → Set) : Set where
  constructor _,_
  field
    fst : A
    snd : B fst
```

We note that the fields are also called projections, as they can be used as eliminators. For instance, the application fst (a, b) for $(a, b) : \Sigma\ A\ B$ reduces to the value of a.

1.4 Agda2Dedukti: a practical translator into the λΠ-calculus modulo rewriting

The problem of encoding the logic of Agda in the λΠ-calculus modulo rewriting was first treated by Guillaume Genestier, who started the development of Agda2Dedukti, a prototype translator[12][11]. In this subsection we present a review of how the main parts of the encoding works. We also refer to Appendix C for more details.

Before starting, we adapt our convention on how to represent Dedukti encodings and we introduce the color green to represent constants alongside blue. Now we declare in blue constants which encode the underling type theory of a system, so for instance as the hierarchy $Set_0 : Set_1 : \ldots$ is primitive in the Agda type system and cannot be removed, it will be represented by constants in blue. On the other hand, we use green to declare constants which correspond to definitions in an Agda file and which are not primitive in the system, but added by the user, such as the definition of natural numbers $\mathbb{N}$ and the function plus $+$.

Variables and symbols which are primitive to the λΠ-calculus modulo theory, such as $x, A, M, \alpha, \lambda, \Pi, \rightarrow$, **Type** are still represented in black. We remind that, even thought the colors blue and green are also used in the Agda, their meaning is completely different, and thus it is important to not mistake Agda code with Dedukti declarations. Finally, we allow ourselves to write some symbols in infix notation or to write some arguments as subscripts, when this simplifies the notation (see cases of $\sqcup$ and $\rightsquigarrow$ below).

1.4.1 Universes and type system

To represent the infinite hierarchy of universes $Set_0 : Set_1 : Set_2 : \ldots$, we first declare a type of sorts and a function that associates to each sort the type of its terms. Therefore, each Agda type A that lives in a sort or universe α will be represented as a term in the type $U\ \alpha$.

$$Sort : \mathbf{Type} \qquad (Sort\text{-decl})$$
$$U : Sort \rightarrow \mathbf{Type} \qquad (U\text{-decl})$$

Then we define a type L to represent universe levels (it would be more appropriate to call it $\mathbb{N}$, but we keep this name to the representation of natural numbers in the theory). Finally, we can define the sorts Set_i by defining a function associating a sort to each level.

$$L : \textbf{Type} \qquad (L\text{-decl})$$
$$z : L \qquad (z\text{-decl})$$
$$s : L \to L \qquad (s\text{-decl})$$
$$set : L \to Sort \qquad (set\text{-decl})$$

We can already represent some basic types, like is the case with natural numbers with $\mathbb{N} : U\ (set\ z)$. However, to represent the elements that live in $\mathbb{N}$ we need another function, taking a sort α and a type A in $U\ \alpha$ and returning the type of elements of A.

$$El : \Pi\alpha : Sort.U\ \alpha \to \textbf{Type}\ \ (\text{written as } El_\alpha) \qquad (El\text{-decl})$$

Now we can declare 0 as an element of $El_{set\ z}\ \mathbb{N}$. In Agda, we also have $Set_i : Set_{i+1}$ for each i, therefore we need to represent this in the encoding. To do so, we first define a function mapping each sort α into its successor sort $\Box\ \alpha$. Then we can declare a function mapping each sort α to the corresponding object $\diamond\ \alpha$ that lives in $\Box\ \alpha$. To properly identify the object $\diamond\ \alpha$ with the sort α we add a rewrite rule identifying their types.

$$\Box : Sort \to Sort \qquad (\Box\text{-decl})$$
$$\Box\ (set\ i) \hookrightarrow set\ (s\ i) \qquad (\Box\text{-red})$$
$$\diamond : \Pi\alpha : Sort.U\ (\Box\ \alpha) \qquad (\diamond\text{-decl})$$
$$El\ _\ (\diamond\ \alpha) \hookrightarrow U\ \alpha \qquad (\diamond\text{-red})$$

The wildcard _ in the last rule represents a non used variable. As this is constraint by typing as being equal to $\Box\ \alpha$, we do not need to specify it. Finally it is only left to represent Agda dependent products, such as $(n : \mathbb{N}) \to n = n$. To do this, we first declare a constant calculating the max between two sorts. This function uses an auxiliary max function which operates on levels.

$$\sqcup : L \to L \to L\ \ (\text{written infix}) \qquad (\sqcup\text{-decl})$$
$$(s\ x) \sqcup (s\ y) \hookrightarrow s\ (x \sqcup y) \qquad (\sqcup\text{-red})$$
$$z \sqcup x \hookrightarrow x \qquad (\sqcup\text{-red})$$
$$x \sqcup z \hookrightarrow x \qquad (\sqcup\text{-red})$$
$$\vee : Sort \to Sort \to Sort\ \ (\text{written infix}) \qquad (\vee\text{-decl})$$
$$(set\ i) \vee (set\ j) \hookrightarrow set\ (i \sqcup j) \qquad (\vee\text{-red})$$

Now we can define the constant representing products, which takes two sorts α, β, a type A in α and a function mapping each element of A to a type in β.

$$\rightsquigarrow\ : \Pi(\alpha\ \beta : Sort)(A : U\ \alpha).(El_\alpha\ A \to U\ \beta) \to U\ (\alpha \vee \beta)\ \ (\text{written infix as } {}_\alpha\!\rightsquigarrow_\beta) \qquad (\rightsquigarrow\text{-decl})$$
$$El_\ (A\ {}_\alpha\!\rightsquigarrow_\beta\ B) \hookrightarrow \Pi x : El_\alpha\ A.El_\beta\ (B\ x) \qquad (\rightsquigarrow\text{-red})$$

For instance, if we want to represent $refl : (n : \mathbb{N}) \to n = n$ we can declare the constant $refl$ as living in

$$El_{set\ z}\ (\mathbb{N}\ {}_{(set\ z)}\!\rightsquigarrow_{(set\ z)}\ (\lambda n : El_{set\ z}\ \mathbb{N}.n = n)),$$

as the latter reduces to $\Pi n : El_{set\ z}\ \mathbb{N}.El_{set\ z}\ (n = n)$. In this case we could ask ourselves why not define the type of $refl$ directly as being $\Pi n : El_{set\ z}\ \mathbb{N}.El_{set\ z}\ (n = n)$. However, for a type to be in the image of the translation, it must be convertible to a type of the form $El_\alpha\ A$, for some α, A. Therefore, by writing it in this more complicated way, we explicit the fact that $refl$ lives in the translation of an Agda type, and not just in some arbitrary type in Dedukti.

Nevertheless, as this encoding makes the presentation of the work much heavier, we will make a choice to simplify the notation in the next parts. Explicitly, we write a product type such as $El_{\alpha\vee\beta}\ (A\ {}_\alpha\!\rightsquigarrow_\beta\ B)$ directly in its normal form, and we

write $El\ A$ to represent $El_{set\ z}\ A$. Therefore, the type $El_{set\ z}\ (\mathbb{N}\ {}_{(set\ z)}{\rightsquigarrow}_{(set\ z)}\ (\lambda n : El_{set\ z}\ \mathbb{N}.n = n))$ of $refl$ gets represented as $\Pi n : El\ \mathbb{N}.El\ (n = n)$. However, this simplification is only for presentation purposes, and is not used in practice in the real translation.

1.4.2 Inductive types and recursive functions

The representation of Agda's inductive types and recursive functions can be done in a very simple way. For each inductive definition, such as the one of natural numbers, we declare a constant representing the type and one constant to represent each constructor.

$$\mathbb{N} : U\ (set\ z) \qquad (\mathbb{N}\text{-decl})$$
$$zero : El\ \mathbb{N} \qquad (zero\text{-decl})$$
$$succ : El\ \mathbb{N} \to El\ \mathbb{N} \qquad (succ\text{-decl})$$

In order to translate a recursive function, such as the sum, we first declare a constant defining the function and we add a rewrite rule for each clause. Note that, as these rules are only fired when the left term corresponds to an instance of the constructor, when translating a terminating Agda function we obtain automatically a terminating set of rewrite rules.

$$+ : El\ \mathbb{N} \to El\ \mathbb{N} \to El\ \mathbb{N} \qquad (+\text{-decl})$$
$$zero + y \hookrightarrow y \qquad (+\text{-red1})$$
$$(succ\ x) + y \hookrightarrow succ\ (x + y) \qquad (+\text{-red2})$$

On the definition of the translated function $+$, as there was no overlap between clauses, the translation was immediate. However, consider the following definition with overlapping clauses.

```
test1 : Nat → Bool
test1 (succ zero) = true
test1 _ = false
```

If we were to translate this definition naively we would have the following rewrite rules.

$$test1\ (succ\ zero) \hookrightarrow true$$
$$test1\ _ \hookrightarrow false$$

However, because rewrite rules have no priority order, we would have in Dedukti both $test1\ (succ\ zero) \hookrightarrow true$ and $test1\ (succ\ zero) \hookrightarrow false$. In order to solve this problem we must make sure that the reduction respects the semantics of Agda, meaning that we can only move to the next clause when we are sure that there is no possible match with the current one.

Fortunately, Agda's internal coverage check, which is used to check totality of clauses, also compiles them into a non-overlapping set of clauses. For instance, by translating the clauses produced by the coverage check, we obtain the following rewrite rules for the function $test1$. This allows the translation of functions to correctly reflect the semantics of their definitions in Agda.

$$test1\ zero \hookrightarrow false$$
$$test1\ (succ\ zero) \hookrightarrow true$$
$$test1\ (succ\ (succ\ _)) \hookrightarrow false$$

2 Representing Coinduction in the $\lambda\Pi$-calculus modulo rewriting

As seen in the subsection about coinduction, the interesting point of this technique is being able to reason about objects which are possibly infinite. Obviously, this raises a problem when trying to implement coinduction in proof assistants, as terms must always be finite. This question is normally addressed by resorting to lazy representations of elements of

coinductive types. This means that the infinite terms are never represented in their entirety, but can be developed an arbitrary amount of times, when required by the user.

In the $\lambda\Pi$-calculus modulo rewriting, it is clear that trying to define the function *natStream* naively by

$$natStream\ n \hookrightarrow n :: (natStream\ (succ\ n))$$

would not work, as rewriting rules can be fired without any checks if the computation is really necessary. Therefore, we need to find a smarter way to control rewriting in this setting. In this section we will explore how this is handled in the case of Agda and we will see how such ideas can be reused in our setting, allowing to represent coinduction and to translate Agda proofs.

2.1 Coinduction in Agda

Coinduction in Agda features two presentations: musical coinduction[19], which is the old way of using coinduction in Agda, and copattern matching coinduction[2], which is today considered the standard.

2.1.1 Musical Coinduction

Musical coinduction addresses the problem of non-termination by introducing the following control operators, which control explicitly the evaluation of the corecursive calls. The constant ∞ associates to each type A the type $\infty\ A$ of halted computations, whereas the operators $\sharp$ and $\flat$, also known as thunk and force, allow respectively to halt a computation and to resume it. We remark however that the only terms that can be halted with $\sharp$ are corecursive calls.

```
∞ : (A : Set) → Set
♯ : {A : Set} → A → ∞ A
♭ : {A : Set} → ∞ A → A
```

To define the coinductive type of streams using musical coinduction we use the following declaration.

```
data Stream (A : Set) : Set where
  _::_ : (x : A) (xs : ∞ (Stream A)) → Stream A
  [] : Stream A
```

The main particularity here is that the corecursive argument of the constructor _ :: _ now takes a halted computation of type *Stream A*. Therefore, to define for instance the curecursive function *natStream* we need to use the $\sharp$ operator to halt the computation of *natStream* (*succ n*). As terms do not reduce under the $\sharp$, this definition is terminating.

```
natStream : Nat → Stream Nat
natStream n = n :: ♯ (natStream (succ n))
```

A halted calculation can be resumed by the symbol $\flat$, as expressed by the identity $\flat\ (\sharp\ x) = x$. Using this symbol we can define for instance a function which, given a position n, takes the n-th element of the stream, if it exists. In order to do this, we first need to introduce the type constructor *Maybe*, used when defining partial functions. Its constructors tell us that a value of type *Maybe A* is either a value of A or nothing.

```
data Maybe (A : Set) : Set where
  just : A → Maybe A
  nothing : Maybe A
```

We can now proceed to the definition of the function n-th. At each step, if the position we are looking for is zero we simply return the head, otherwise we resume the computation of the tail (using the $\flat$ operator) and we do a recursive call on it. If at any point we reach the end of the stream (as streams here are only possibly infinite, and not always), we return nothing to signal that the searched element does not exist. We note that, in opposition to *natStream*, which is defined by corecursion, *nth* is defined by recursion on its first argument.

```
nth : Nat → Stream Nat → Maybe Nat
nth zero (hd :: tl) = just hd
nth (succ n) (hd :: tl) = nth n (♭ tl)
nth _ [] = nothing
```

2.1.2 Copattern matching coinduction

Even though musical coinduction solves the problem of non-termination, it is clear that it is not very intuitive to use, as the user needs to control explicitly how calculations are halted and resumed, which requires some experience. Abel *et al* introduced in [2] a different presentation of coinduction through copattern matching. The main idea is to express coinductive types as records and define their elements not through constructors but rather through their eliminators, also called *projections*. Of course, the fact that we work with records imposes that the type can only have one constructor, but this restriction can be circumvented in many cases.

For instance, if we consider the coinductive type of streams defined only by the constructor $_ :: _ : A \to \mathit{Stream}\ A \to \mathit{Stream}\ A$ (therefore only containing infinite streams), we can express it by the following definition. Note that coinductive records must be marked with a the coinductive flag, as shown.

```
record Stream (A : Set) : Set where
  coinductive
  field
    hd : A
    tl : Stream A
```

We can then define corecursive functions by copattern matching by defining how the value produced by the function reduces when eliminated through each one of the record's projections. For instance, in order to define $\mathit{natStream} : \mathbb{N} \to \mathit{Stream}\ \mathbb{N}$ we must explain how $\mathit{natStream}\ n$ reduces when we inspect the fields *hd* and *tl*. Note that, as the term $\mathit{natStream}\ (\mathit{succ}\ n)$ does not reduce by itself, but only when eliminated through a projection, this definition is terminating.

```
natStream : Nat → Stream-Nat
hd (natStream n) = n
tl (natStream n) = natStream (succ n)
```

In order to compare the two presentations of coinduction, we can also look at how the *n*-th function can be defined in this setting. Note that as *n*-th is defined by recursion (in its first argument), and not by corecursion, it uses projections in a fundamentally different way from *natStream*. Whereas *natStream* uses them to explain how the value of the function reduces, *n*-th uses projections in order to access the fields of the stream *st*, which is given as second argument. Also note a very important change here, when comparing with the function *n*-th defined for musical coinduction: because with copattern matching coinduction we only have coinductive types with one constructor, which in this case is the constructor $_ :: _$, then all streams are infinite in this case, and thus this function can be total.

```
nth : Nat → Stream Nat → Nat
nth zero st = hd st
nth (succ n) st = nth n (tl st)
```

We remark that whereas both musical and copattern matching coinduction solve the problem of non-termination, when using copattern matching coinduction we do not have to deal with control operators, and thus we have a much more natural and user-friendly way of using coinduction.

A last remark is that, even though in Agda most records enjoy eta-conversion (more details on that in appendix C), this is disabled for coinductive records, as it can lead to non-termination issues. Indeed, if we were to try to eta-expand $\mathit{natStream}\ 0$ we would have the infinite unraveling

$$\mathit{natStream}\ 0 \hookrightarrow \mathit{Record}\{\mathit{hd} = 0; \mathit{tl} = \mathit{natStream}\ 1\} \hookrightarrow \mathit{Record}\{\mathit{hd} = 0; \mathit{tl} = \mathit{Record}\{\mathit{hd} = 1; \mathit{tl} = \mathit{natStream}\ 2\}\} \hookrightarrow \ldots,$$

where *Record* is the generic constructor for records.

2.2 Coinduction in the λΠ-calculus modulo rewriting

Now that we have seen the basis of coinduction in Agda, we look at how we can encode such types and definitions in Dedukti. Very fortunately, Agda's internal representation of terms already provides a representation which was easily adapted to our setting, so we use that as a basis for our encoding in Dedukti.

Even though copattern-matching coinduction is the main one used nowadays, we also chose to cover musical coinduction, as both presentations teach us interesting ideas of how coinduction can be represented, which can be applied in the future to translate coinduction in other proof assistants.

We reuse the same conventions established in X to represent Dedukti definitions. However, we will also use a superscript as in $A^{\text{♪}}$ when translating the musical version of A and as in A^{co} when translating the copattern matching version of A, in order to separate very explicitly both cases.

2.2.1 Musical coinduction

To encode musical coinduction, we first start by declaring constants for the control operators. Note that there is no constant for $\sharp$ in the translation, as we will explain.

$$\infty : U\ (Set\ z) \to U\ (Set\ z) \qquad (\infty\text{-decl})$$
$$\flat : \Pi A : U\ (Set\ z).El\ (\infty\ A) \to El\ A \ \text{(written as } \flat_A) \qquad (\flat\text{-decl})$$

In order to encode a coinductive type declaration, we proceed the same as when encoding an inductive type. We first declare a constant to define the type itself and then we declare constants to define the constructors of the type. For instance, to define the type *Stream* we define the following constants, the first representing the declaration of the type, and the last two the declaration of the constructors.

$$Stream^{\text{♪}} : U\ (Set\ z) \to U\ (Set\ z) \qquad (Stream^{\text{♪}}\text{-decl})$$
$$::\ : \Pi A : U\ (Set\ z).El\ A \to El\ (\infty\ (Stream^{\text{♪}}\ A)) \to El\ (Stream^{\text{♪}}\ A) \ \text{(written infix as } ::_A) \qquad (::\text{-decl})$$
$$[]\ : \Pi A : U\ (Set\ z).El\ (Stream^{\text{♪}}\ A) \ \text{(written as } []_A) \qquad ([]\text{-decl})$$

This generalizes the encoding of inductive types and is fairly straightforward, but the interesting part comes when encoding corecursive functions. If we were to define a constant $\sharp_A$, as done with $\flat_A$, and translate the definitions directly, we would have the following definition for $natStream^{\text{♪}}$.

$$natStream^{\text{♪}} : El\ \mathbb{N} \to El\ (Stream^{\text{♪}}\ \mathbb{N}) \qquad (natStream^{\text{♪}}\text{-decl})$$
$$natStream^{\text{♪}}\ n \hookrightarrow n ::_{\mathbb{N}} (\sharp_{\mathbb{N}}\ (natStream^{\text{♪}}\ (succ\ n))) \qquad (natStream^{\text{♪}}\text{-red})$$

However, in this setting we cannot forbid reductions which happen under a $\sharp_A$ sign, as done in the semantics of Agda. This means that this rule causes non-termination, as we have the infinite reduction sequence

$$natStream^{\text{♪}}\ n \hookrightarrow n ::_{\mathbb{N}} (\sharp_{\mathbb{N}}\ (natStream^{\text{♪}}\ (succ\ n))) \hookrightarrow n ::_{\mathbb{N}} (\sharp_{\mathbb{N}}\ ((succ\ n) ::_{\mathbb{N}} (\sharp_{\mathbb{N}}\ (natStream^{\text{♪}}\ (succ\ (succ\ n)))))) \hookrightarrow \dots .$$

Therefore, we do not proceed like this. Instead, we apply the idea also used in the internal syntax representation of Agda to represent a function using two versions. In the case of *natStream* we have the following declarations.

$$natStream^{\text{♪}} : El\ \mathbb{N} \to El\ (Stream^{\text{♪}}\ \mathbb{N}) \qquad (natStream^{\text{♪}}\text{-decl})$$
$$\sharp\text{-}natStream^{\text{♪}} : El\ \mathbb{N} \to El\ (\infty\ (Stream^{\text{♪}}\ \mathbb{N})) \qquad (\sharp\text{-}natStream^{\text{♪}}\text{-decl})$$

The idea here is that each corecursive function will have its halted version, which we can use in corecursive calls without non-termination problems. In this setting, an application of $\sharp$ to a corecursive call is translated into the halted version of it. For instance, to finish the definition of $natStream^{\text{♪}}$ we declare the following rewrite rules.

$$natStream^{\flat} \; n \hookrightarrow n ::_{\mathbb{N}} (\sharp\text{-}natStream^{\flat} \; (succ \; n)) \qquad (natStream^{\flat}\text{-red})$$
$$\flat_{\mathbb{N}} \; (\sharp\text{-}natStream^{\flat} \; n) \hookrightarrow natStream^{\flat} \; n \qquad (\sharp\text{-}natStream^{\flat}\text{-red})$$

The first rewrite rule corresponds to the definition of the function, whereas the second allows to transform the halted version of the function into a computing one, through the $\flat$ symbol. Note that, as $\sharp\text{-}natStream^{\flat} \; (succ \; n)$ does not reduce by itself, but only when applied as an argument of $\flat_{\mathbb{N}}$, we do not have the infinite reduction sequence presented previously.

2.2.2 Copattern matching coinduction

Whereas the encoding of musical coinduction needs the duplication of function symbols in order to eliminate the $\sharp$ operator, we will see that copattern matching coinduction admits a much simple encoding, as we can obtain terminating corecursive definitions by just orienting the clauses defining corecursive functions.

First, in order to encode a coinductive type declaration, we declare once again a constant to represent the type. However, instead of declaring constants to define the constructors, we now declare constants to define the projections. The type *Stream* can for instance be represented by the following constants.

$$Stream^{co} : U \; (set \; z) \to U \; (set \; z) \qquad (Stream^{co}\text{-decl})$$
$$hd : \Pi A : U \; (set \; z).El \; (Stream^{co} \; A) \to El \; A \;\; (\text{written as } hd_A) \qquad (hd\text{-decl})$$
$$tl : \Pi A : U \; (set \; z).El \; (Stream^{co} \; A) \to El \; (Stream^{co} \; A) \;\; (\text{written as } tl_A) \qquad (tl\text{-decl})$$

Now corecursive functions can be translated by declaring a constant to represent the function and adding rewriting rules corresponding to the clauses. In the case of *natStream* we have the following declarations.

$$natStream^{co} : El \; \mathbb{N} \to El \; (Stream^{co} \; \mathbb{N}) \qquad (natStream^{co}\text{-decl})$$
$$hd_{\mathbb{N}} \; (natStream^{co} \; n) \hookrightarrow n \qquad (natStream^{co}\text{-red1})$$
$$tl_{\mathbb{N}} \; (natStream^{co} \; n) \hookrightarrow natStream^{co} \; (succ \; n) \qquad (natStream^{co}\text{-red2})$$

As no rewrite rule allows reducing $natStream^{co} \; (succ \; n)$ by itself, we do not have the non-termination problem seen before.

2.3 Examples on translating coinduction

In order to understand how the encoding generalizes to other cases, we consider a series of examples.

2.3.1 Taking the *n*-th element of a stream

We start with the function *n*-th, which was already discussed for both presentations of coinduction. To translate the version using musical coinduction we first need to translate the inductive type constructor *Maybe*. We proceed as usual, declaring one constant to encode the type and one constant for each constructor.

$$Maybe : U \; (Set \; z) \to U \; (Set \; z) \qquad (Maybe\text{-decl})$$
$$just : \Pi A : U \; (Set \; z).El \; A \to El \; (Maybe \; A) \;\; (\text{written as } just_A) \qquad (just\text{-decl})$$
$$nothing : \Pi A : U \; (Set \; z).El \; (Maybe \; A) \;\; (\text{written as } nothing_A) \qquad (nothing\text{-decl})$$

In order to encode *n*-th, we declare only one constant to represent the function, and then the expected rewrite rules. Even thought we saw that the translation of corecursive functions written with musical coinduction uses two constant declarations, *n*-th is not corecursive but recursive, and as such admits a straightforward representation with just one constant.

$$n\text{-}th^{\flat} : El \; \mathbb{N} \to El \; (Stream^{\flat} \; \mathbb{N}) \to El \; (Maybe \; \mathbb{N}) \qquad (n\text{-}th^{\flat}\text{-decl})$$
$$n\text{-}th^{\flat} \; zero \; (x ::_{\mathbb{N}} l) \hookrightarrow just_{\mathbb{N}} \; x \qquad (n\text{-}th^{\flat}\text{-red1})$$
$$n\text{-}th^{\flat} \; (succ \; n) \; (x ::_{\mathbb{N}} l) \hookrightarrow n\text{-}th^{\flat} \; n \; (\flat_{\mathbb{N}} \; l) \qquad (n\text{-}th^{\flat}\text{-red2})$$
$$n\text{-}th^{\flat} \; _ \; []_{\mathbb{N}} \hookrightarrow nothing_{\mathbb{N}} \qquad (n\text{-}th^{\flat}\text{-red3})$$

In order to test the definitions of $n\text{-}th^{\flat}$ and $natStream^{\flat}$ we can try to compute the normal form of $n\text{-}th^{\flat}\ 1\ (natStream^{\flat}\ 6)$, where we write numerals in decimal notation to simplify the presentation. This gives the following rewrite sequence, which computes to the value $just_{\mathbb{N}}\ 7$ as expected.

$$
\begin{aligned}
n\text{-}th^{\flat}\ 1\ (natStream^{\flat}\ 6) &\longrightarrow n\text{-}th^{\flat}\ 1\ (6 ::_{\mathbb{N}} (\sharp\text{-}natStream^{\flat}\ 7)) && \text{by } (natStream^{\flat}\text{-red}) \\
&\longrightarrow n\text{-}th^{\flat}\ 0\ (\flat_{\mathbb{N}}\ (\sharp\text{-}natStream^{\flat}\ 7)) && \text{by } (n\text{-}th^{\flat}\text{-red2}) \\
&\longrightarrow n\text{-}th^{\flat}\ 0\ (natStream^{\flat}\ 7) && \text{by } (\flat\text{-red}) \\
&\longrightarrow n\text{-}th^{\flat}\ 0\ (7 ::_{\mathbb{N}} (\sharp\text{-}natStream^{\flat}\ 8)) && \text{by } (natStream^{\flat}\text{-red}) \\
&\longrightarrow just_{\mathbb{N}}\ 7 && \text{by } (n\text{-}th^{\flat}\text{-red1})
\end{aligned}
$$

We can also look at the translation of *n-th* when using copattern-matching coinduction. Once again, as this is a recursive function, and not a corecursive one, this is represented in Dedukti just like other recursive functions.

$$
\begin{aligned}
&n\text{-}th^{co} : El\ \mathbb{N} \to El\ (Stream^{co}\ \mathbb{N}) \to El\ \mathbb{N} && (n\text{-}th^{co}\text{-decl}) \\
&n\text{-}th^{co}\ zero\ x \longrightarrow hd_{\mathbb{N}}\ x && (n\text{-}th^{co}\text{-red1}) \\
&n\text{-}th^{co}\ (succ\ n)\ x \longrightarrow n\text{-}th^{co}\ n\ (tl_{\mathbb{N}}\ x) && (n\text{-}th^{co}\text{-red2})
\end{aligned}
$$

Once again, we can compute the normal form of $n\text{-}th^{co}\ 1\ (natStream^{co}\ 6)$ and see we get the expected value.

$$
\begin{aligned}
n\text{-}th^{co}\ 1\ (natStream^{co}\ 6) &\longrightarrow n\text{-}th^{co}\ 0\ (tl_{\mathbb{N}}\ (natStream^{co}\ 6)) && \text{by } (n\text{-}th^{co}\text{-red2}) \\
&\longrightarrow n\text{-}th^{co}\ 0\ (natStream^{co}\ 7) && \text{by } (natStream^{co}\text{-red2}) \\
&\longrightarrow hd_{\mathbb{N}}\ (natStream^{co}\ 7) && \text{by } (n\text{-}th^{co}\text{-red1}) \\
&\longrightarrow 7 && \text{by } (natStream^{co}\text{-red1})
\end{aligned}
$$

2.3.2 Predicates on streams

We have seen how we can declare corecursive functions in Agda and then translate them into Dedukti. However, as our main objective is doing proof interoperability, we also need to see how we can define coinductive predicates and reason about them by coinduction. However, remember that, by the *Curry-Howard* correspondence, propositions are just types, thus proofs by coinduction are just corecursive functions, and therefore the ideas we have seen up until now apply in the same way. To illustrate this, we look at how we can represent the notion of equality between streams in Agda and then translate them into Dedukti.

As seen in subsection 1.2, corecursive functions must have coinductive types as codomain. Therefore, by the *Curry-Howard* correspondence, proofs by coinduction must prove coinductive predicates. However, the notion of equality that is most common in type theory is not defined with a coinductive type, but with an inductive one, and thus in order to reason about equality on streams we have to define a coinductive notion of equality for them.

In the language of musical coinduction, we can represent this notion using the following coinductive type. In the definition, $\equiv$ is Agda's type for regular equality. Furthermore, some arguments are between brackets to declare them as implicit.

```
data _∼_ {A : Set} : Stream A → Stream A → Set where
  ∼-empty : [] ∼ []
  ∼-cons : {x x′ : A} {l l′ : ∞ (Stream A)} → x ≡ x′ → ∞ (♭ l ∼ ♭ l′) → (x :: l) ∼ (x′ :: l′)
```

Intuitively, two streams are similar (that is, coinductively equal) when they are both empty or when they have equal heads and, when resuming the computation on their tails with $\flat$, we have a "halted" proof that they are similar.

This coinductive type can be translated very straightforwardly into Dedukti, giving the following declarations. On the declaration of $\sim\text{-}cons^{\flat}$ we mark some arguments between brackets to indicate that they will be implicit. Once more, this is not actually done in the translation, but rather a simplification for presentation purposes.

$$\sim^{\natural} : \Pi A : U\ (Set\ z).El\ (Stream\ A) \to El\ (Stream\ A) \to U\ (Set\ z)\ \text{(written infix as } \sim_A) \qquad (Stream^{\natural}\text{-decl})$$

$$\sim\text{-}empty^{\natural} : \Pi A : U\ (Set\ z).[]_A \sim^{\natural}_A []_A \qquad (\sim\text{-}empty^{\natural}\text{-decl})$$

$$\sim\text{-}cons^{\natural} : \Pi(A : U\ (Set\ z))\ \{x\ y : El\ A\}\ \{l\ l' : El\ (Stream^{\natural}\ A)\}.$$
$$El\ (x \equiv y) \to El\ (\infty\ ((\flat_A\ l) \sim^{\natural}_A (\flat_A\ l'))) \to El\ ((x ::_A l) \sim^{\natural}_A (x' ::_A l')) \qquad (\sim\text{-}cons^{\natural}\text{-decl})$$

Using this type, we can prove many interesting properties, for instance that $\sim$ is an equivalence relation, satisfying reflexivity, symmetry and transitivity. We can also use it to prove properties about operations on streams. For instance, if we have a binary operation on the type A we can show that by extending it pointwise on streams we preserve some nice properties. To illustrate this, let us define an operation of sum between two streams of natural numbers. The following definition says that when one of the streams is empty, the result is also empty, but when both have a head and a tail we perform a normal sum on the heads and we make a corecursive call on the tails.

```
_⊕_ : Stream Nat → Stream Nat → Stream Nat
[] ⊕ _       = []
(_ :: _) ⊕ [] = []
(x :: l) ⊕ (x' :: l') = (x + x') :: ♯ (♭ l ⊕ ♭ l')
```

We can express this function in Dedukti by the following declarations. Note that the halted version of $\oplus$ now also takes a halted argument. Therefore, the occurrence of $\sharp\ (\flat\ l \oplus \flat\ l')$ is replaced with $l\ \sharp\text{-}\oplus\ l'$ in ($\oplus^{\natural}$-red3). The $\flat$ is only applied to l, l' when the calculation of $\oplus$ is resumed by applying the $\flat$ to it, using ($\sharp\text{-}\oplus^{\natural}$-red).

$$\oplus^{\natural} : El\ (Stream\ \mathbb{N}) \to El\ (Stream\ \mathbb{N}) \to El\ (Stream\ \mathbb{N})\ \text{(written infix)} \qquad (\oplus^{\natural}\text{-decl})$$

$$\sharp\text{-}\oplus^{\natural} : El\ (\infty\ (Stream\ \mathbb{N})) \to El\ (\infty\ (Stream\ \mathbb{N})) \to El\ (\infty\ (Stream\ \mathbb{N}))\ \text{(written infix)} \qquad (\sharp\text{-}\oplus^{\natural}\text{-decl})$$

$$[]_{\mathbb{N}} \oplus^{\natural} _ \hookrightarrow []_{\mathbb{N}} \qquad (\oplus^{\natural}\text{-red1})$$

$$(_ ::_{\mathbb{N}} _) \oplus^{\natural} []_{\mathbb{N}} \hookrightarrow []_{\mathbb{N}} \qquad (\oplus^{\natural}\text{-red2})$$

$$(x ::_{\mathbb{N}} l) \oplus^{\natural} (x' ::_{\mathbb{N}} l') \hookrightarrow (x + x') ::_{\mathbb{N}} (l\ \sharp\text{-}\oplus^{\natural}\ l') \qquad (\oplus^{\natural}\text{-red3})$$

$$\flat_{\mathbb{N}}\ (l\ \sharp\text{-}\oplus^{\natural}\ l') \hookrightarrow (\flat_{\mathbb{N}}\ l) \oplus^{\natural} (\flat_{\mathbb{N}}\ l)' \qquad (\sharp\text{-}\oplus^{\natural}\text{-red})$$

Now, using a proof $+$-*assoc* that $+$ is associative, we can show associativity of $\oplus$. The cases in which one of the streams is empty are trivial, the interesting case is when we have $l_i = x_i :: s_i$ for $i = 1, 2, 3$. In this setting, note that we have the following reductions (in Agda).

$$((x_1 :: s_1) \oplus (x_2 :: s_2)) \oplus (x_3 :: s_3) \hookrightarrow ((x_1 + x_2) :: \sharp(\flat\ s_1 \oplus \flat\ s_2)) \oplus (x_3 :: s_3) \hookrightarrow ((x_1 + x_2) + x_3) :: \sharp((\flat\ s_1 \oplus \flat\ s_2) \oplus \flat\ s_3)$$

$$(x_1 :: s_1) \oplus ((x_2 :: s_2) \oplus (x_3 :: s_3)) \hookrightarrow (x_1 :: s_1) \oplus ((x_2 + x_3) :: \sharp(\flat\ s_2 \oplus \flat\ s_3)) \hookrightarrow (x_1 + (x_2 + x_3)) :: \sharp(\flat\ s_1 \oplus (\flat\ s_2 \oplus \flat\ s_3))$$

Therefore, in order to show this case we only need to use $\sim$ -*cons* and provide a proof of $(x_1 + x_2) + x_3 \equiv x_1 + (x_2 + x_3)$, which we have by $+$-*assoc*, and a proof of $\flat\ (\sharp\ (\flat\ l1 \oplus (\flat\ l2 \oplus \flat\ l3))) \sim \flat\ (\sharp\ ((\flat\ l1 \oplus \flat\ l2) \oplus \flat\ l3))$. But as we have $\flat\ (\sharp\ x) = x$, then this amounts to show $\flat\ l1 \oplus (\flat\ l2 \oplus \flat\ l3) \sim (\flat\ l1 \oplus \flat\ l2) \oplus \flat\ l3$, which we have by coinduction hypothesis.

```
⊕-assoc : (l1 l2 l3 : Stream Nat) → (l1 ⊕ l2) ⊕ l3 ∼ l1 ⊕ (l2 ⊕ l3)
⊕-assoc [] _ _ = ∼-empty
⊕-assoc (_ :: _) [] _ = ∼-empty
⊕-assoc (_ :: _) (_ :: _) [] = ∼-empty
⊕-assoc (x1 :: s1) (x2 :: s2) (x3 :: s3) = ∼-cons (+-assoc x1 x2 x3) (♯ (⊕-assoc (♭ s1) (♭ s2) (♭ s3)))
```

An interesting point to mention is that if we were to erase all $\flat$, $\sharp$ and ∞ and swap *Stream* for *List* in the definitions of $\sim$, $\oplus$, $\oplus$-*assoc*, then $\oplus$-*assoc* would still be a valid proof. However, because we are dealing with streams, which do not need to be well-founded, our proof is more general because it also holds for infinite streams.

The proof of $\oplus$-*assoc* can be expressed in Dedukti by the following declarations.

$$\oplus\text{-}assoc^{\flat} : \Pi l_1\ l_2\ l_3 : El\ (Stream\ \mathbb{N}).El\ (((l_1 \oplus^{\flat} l_2) \oplus^{\flat} l3) \sim^{\flat}_{\mathbb{N}} (l_1 \oplus^{\flat} (l_2 \oplus^{\flat} l_3))) \qquad (\oplus\text{-}assoc^{\flat}\text{-decl})$$

$$\sharp\text{-}\oplus\text{-}assoc^{\flat} : \Pi l_1\ l_2\ l_3 : El\ (Stream\ \mathbb{N}).El\ (\infty\ (((l_1 \oplus^{\flat} l_2) \oplus^{\flat} l3) \sim^{\flat}_{\mathbb{N}} (l_1 \oplus^{\flat} (l_2 \oplus^{\flat} l_3))) \qquad (\sharp\text{-}\oplus\text{-}assoc^{\flat}\text{-decl})$$

$$\oplus\text{-}assoc^{\flat}\ []_{\mathbb{N}}\ _\ _ \hookrightarrow \sim\text{-}empty^{\flat}_{\mathbb{N}} \qquad (\oplus\text{-}assoc^{\flat}\text{-red1})$$

$$\oplus\text{-}assoc^{\flat}\ (_ ::_{\mathbb{N}} _)\ []_{\mathbb{N}}\ _ \hookrightarrow \sim\text{-}empty^{\flat}_{\mathbb{N}} \qquad (\oplus\text{-}assoc^{\flat}\text{-red2})$$

$$\oplus\text{-}assoc^{\flat}\ (_ ::_{\mathbb{N}} _)\ (_ ::_{\mathbb{N}} _)\ []_{\mathbb{N}} \hookrightarrow \sim\text{-}empty^{\flat}_{\mathbb{N}} \qquad (\oplus\text{-}assoc^{\flat}\text{-red3})$$

$$\oplus\text{-}assoc^{\flat}\ (x_1 ::_{\mathbb{N}} s_1)\ (x_2 ::_{\mathbb{N}} s_2)\ (x_1 ::_{\mathbb{N}} s_3) \hookrightarrow$$
$$\sim\text{-}cons^{\flat}_{\mathbb{N}}\ (+\text{-}assoc\ x_1\ x_2\ x_3)\ (\sharp\text{-}\oplus\text{-}assoc^{\flat}\ s_1\ s_2\ s_3) \qquad (\oplus\text{-}assoc^{\flat}\text{-red4})$$

$$\flat_{\mathbb{N}}\ (\sharp\text{-}\oplus\text{-}assoc^{\flat}\ l_1\ l_2\ l_3) \hookrightarrow \oplus\text{-}assoc^{\flat}\ (\flat_{\mathbb{N}}\ l_1)\ (\flat_{\mathbb{N}}\ l_2)\ (\flat_{\mathbb{N}}\ l_3) \qquad (\sharp\text{-}\oplus\text{-}assoc^{\flat}\text{-red})$$

The same development and translation can also be done with copattern-matching coinduction. However, as the case of musical coinduction is the most complex one we decided to do it here and, for size constraints, we refer to Appendix D where we detail this development with copattern-matching coinduction.

Up until now, the only example of coinductive type we saw was the type of streams. However, coinductive types enable us to represent many more mathematical structures. For size constraints once more, we also refer to Appendix D for a discussion on how to represent formal languages and translate them to Dedukti. However, we believe that the main ideas of the translation have already been exposed, with these additional examples being left as optional to the reader.

3 Practical Implementation

In the previous section, we saw how coinduction can be used in Agda and how such definitions can be translated in the $\lambda\Pi$-calculus modulo rewriting. We now detail the practical details of how this translation is implemented in Agda2Dedukti. A large part of this internship was also dedicated to resuming the development of Agda2Dedukti, which was halted since September of 2020. Therefore, we also detail many other contributions that were made for improving it. The code of the translator can be found here.

3.1 Translation of Coinduction

As already mentioned, the proposed encoding of coinduction in the $\lambda\Pi$-calculus modulo rewriting is based on the representation of the internal syntax of Agda. Therefore, the main challenge here was adapting Agda2Dedukti to correctly translate the internal representations into Dedukti, something that was not done in Genestier's prototype. The main problem the original prototype had and which prevented the translation of coinduction lied on the translation of clauses defining corecursive functions.

A clause defining a normal recursive function f is generally of the form $f\ \vec{x} = y$, and therefore Agda internally represents a clause by a head symbol f, a list of applied patterns $\vec{x}$, and a body y. However, when we were discussing the encoding of coinduction we saw that corecursive clause definitions do not always satisfy this criterion.

In the case of musical coinduction, each function declaration f is duplicated into a halted version $\sharp\text{-}f$. The clauses of f itself are of the form $f\ \vec{x} = y$, however the only clause defining $\sharp\text{-}f$ is

$$\flat\ (\sharp\text{-}f\ \vec{x}) = f\ \vec{x}\,.$$

In order to represent such a clause in the form $f\ \vec{x} = y$, Agda puts projections in *postfix form*. This means that the previous clause is represented internally as $\sharp\text{-}f\ \vec{x}\ .\flat = f\ \vec{x}$, where the dot in $.\flat$ means that this application should be translated in prefix form. Therefore, the symbol $\sharp\text{-}f$ appears as the head symbol of the clause, even though the true head symbol is $\flat$.

This happens even more frequently when translating copattern matching corecursive functions. Indeed, a corecursive function f defined by copattern matching will have its clauses in the form $\pi\ (f\ \vec{x})\ \vec{z} = y$, which is then represented in the form $f\ \vec{x}\ .\pi\ \vec{z} = y$. For example, the first clause defining the function *natStream* was represented internally as $natStream\ n\ .hd = n$. As Genestier's prototype did not take this into account, such functions declarations were being

translated in an incorrect way. For instance, the first clause of *natStream* was being translated as $natStream\ n\ hd \hookrightarrow n$, whose left side is not even well typed, as $natStream\ n$ is of type $Stream\ Nat$ and hd is of type $\{A : Set\} \to Stream\ A \to A$.

Therefore, in order to correctly translate these clauses we had to change the code implementing the translation of clauses in order to properly account for this representation. As the original Agda2Dedukti code was not documented, this turned out to be not so trivial. Moreover, when representing a clause $f\ \vec{x} = y$ Agda does not store internally all the typing information of the left-hand side, but only of the head symbol f. This information needs to be reconstructed while translating patterns, which makes the process a bit tricky.

Finally, we also had to adapt other parts of the translator which did not interact properly with coinduction. Explicitly, the translation of eta-expansion (see details in Appendix C) was previously treating all records in an homogeneous way, meaning that even coinductive records were translated with eta-expansion in Dedukti. However, we have already seen that eta-expansion causes non-termination when added to coinductive records. This did not cause a problem before, as coinduction was not a feature supported by the translator, but as this is now the case we had to adapt the translation in order to only translate with eta-expansion the records which also have it in Agda.

To see an excerpt of the proofs that were automatically translated using this feature, we refer to this repository.

3.2 Agda2Lambdapi

We previously discussed that, in order to use the $\lambda\Pi$-calculus modulo rewriting in practice, researchers at Deducteam have developed two implementations Dedukti and Lambdapi. Whereas Dedukti will probably be discontinued, Lambdapi is under active development and extends it in multiple ways. Lambdapi features most notably interactive proof development, with a proof mode and tactics, but also other features such as efficient rewriting, metavariables and implicit arguments. As the prototype translator Agda2Dedukti was only capable of translating into Dedukti, and not Lambdapi, the extension of the translator with an Agda2Lambdapi mode was a natural goal of the internship, which would allow the translation of files into both Dedukti and Lambdapi.

Most of the development of this new mode consisted of adapting the syntax of the output. Moreover, Lambdapi files must state explicitly in their beginning which other files they use, something which was not needed in Dedukti, and therefore the translation of each file now needed to take this into account. However, the most challenging part of this development was dealing with AC symbols, which are used to implement the translation of universe polymorphism.

3.2.1 Dealing with AC symbols

Associative commutative (or just AC) symbols are symbols which satisfy an associative commutative equational theory. For instance, if we declare $+ : Nat \to Nat \to Nat$ as being AC then we automatically get the conversions $x + (y + z) \equiv (x + y) + z$ and $x + y \equiv y + x$. Note that, even though we could add the conversion $x + (y + z) \equiv (x + y) + z$ by means of the rewriting rule $x + (y + z) \hookrightarrow (x + y) + z$, there is no way to add the conversion relation $x + y \equiv y + x$ with a terminating rewrite system. Therefore, the ability of having AC symbols strictly enriches the capability of handling equational theories.

AC symbols may also enjoy a richer type of matching, called AC matching. In the presence of AC matching, all terms of the form $x + x$, $x + (y_1 + x)$, $x + (y_1 + (y_2 + x))$, etc are matched by the rule $x + x \hookrightarrow x$, whereas with normal matching we would have to declare a rewrite rule

$$x + (y_1 ... (y_k + x) ...) \hookrightarrow x + (y_1 ... (y_{k-1} + y_k) ...)\,.$$

for each k (thus, an infinity of rewrite rules).

We will not enter in all the details here, but the important point is that the implementation of universe levels used AC matching, which is particularly needed when using universe polymorphism. However, whereas Dedukti featured both AC symbols and AC matching, Lambdapi does not feature AC matching, as its implementation is complex and error-prone. Therefore, the challenge here was adapting the representation of universe levels such that AC matching was not required. In order to do so, Frédéric Blanqui introduced in Lambdapi a mechanism to put terms internally in a canonical form, such that given an order on variable names, the canonical form uses the AC identities to order them.

The precise order of the variables is irrelevant, the interesting point is that the term $x+(y_1...(y_k+x)...)$ will be represented either as $x+(x+(...))$ (case I) or $y_{i_1}+(...(x+(x+...))...)$ (case II) or $y_{i_1}+(...(y_{i_k}+(x+x))...)$ (case III), and thus the occurrences of x will be grouped together. This allows us to replace the rule $x+x \hookrightarrow x$, which uses AC matching, by the two syntactic rules

$$x+x \hookrightarrow x$$

matching (III) and

$$x+(x+y) \hookrightarrow x+y$$

matching (I) and (II).

Using this technique, we modified with Frédéric Blanqui the encoding of universe levels in order to get rid of AC matching. This also evolved the testing of the canonical form mechanism and the reporting of multiple bugs to the development of Lambdapi. This encoding allowed us then to correctly translate Agda files using universe polymorphism into Lambdapi.

3.3 Adding support for latest Agda version

The Agda2Dedukti translator is implemented as a backend of Agda, and as such it makes heavy use of its code. As the development of the translator had been halted, it did not support the latest version of Agda, and therefore in order to update the translator we had to adapt the parts of our code that used features from the previous version. Making those changes would not have been such a hard task if the translator used a previous version of Agda.

However, this was not the case, and it actually used an *ad hoc* version which incorporated many changes that were needed for the translation. As this version had already too much diverted, incorporating the changes of the newest standard version would have been impractical, and doing this for each new version was clearly not a good strategy. Therefore, in order to update the translator, we had to get rid of the dependency on the *ad hoc* version, in order to allow us to use the standard version of Agda

Fortunately, to do that we had the help of Jesper Cockx, an Agda developer who also had helped on the development of the translator previously. He kindly incorporated in the standard version most of the changes needed, which allowed us to use it (almost) directly with the translator. The only change not yet incorporated is an active pull request which should be merged soon and which changes less then 10 lines. Therefore, nowadays the translator uses a version of Agda almost identical to the standard one, as the only changes we need to add for the moment are these few lines. With all of these changes, we were able to update the translator, which now uses a slightly modified version (less then 10 lines) of a copy of the standard version dating less than 2 months.

4 Conclusion

We have for the first time successfully proposed a representation of coinduction in Dedukti, by encoding coinductive definitions from Agda. Moreover, we implemented this translation in Agda2Dedukti, which now allows for automatically translating coinduction proofs from Agda to Dedukti. This allowed us to automatically translate multiple proofs by coinduction, and opens a research direction for importing them into other proof assistants. Finally, we have proposed many improvements to Agda2Dedukti, which now supports Lambdapi and works almost directly with the latest versions of the Agda master branch.

This work opens many interesting directions for future work. A natural next problem is to see how we can import the translated coinduction proofs into other proof assistants, such as Coq. Furthermore, we also plan to treat other features still missing from the translator. For instance, sized types are annotations allowing to show termination, and are in particular used in the Agda standard library for having a more general version of coinduction. Moreover, we already have a prototype of an encoding for universe polymorphism that extends the current one to the non-prenex case.

Finally, the ultimate goal is to understand how Agda proofs can be imported in other proof systems, and vice versa. This is a particularly interesting research direction, as Agda is the first proof assistant encoded into Dedukti which feature a predicative type system and which mixes completely propositions with types. Therefore, it is important to better understand the relation between predicative and impredicative type theory and to build encodings between them. This would allow us to share proofs between Agda and other impredicative type systems, such as Coq, Matita, Isabelle, etc.

Appendix A References

[1] A. Abel. Equational reasoning about formal languages in coalgebraic style.

[2] A. Abel, B. Pientka, D. Thibodeau, and A. Setzer. Copatterns: Programming infinite structures by observations. 2013.

[3] P. Aczel. *Non-Well-Founded Sets*. Csli Lecture Notes, 1988.

[4] A. Assaf. *A framework for defining computational higher-order logics*. Theses, École polytechnique, Sept. 2015.

[5] A. Assaf and G. Burel. Translating HOL to Dedukti. In C. Kaliszyk and A. Paskevich, editors, *Fourth Workshop on Proof eXchange for Theorem Proving, PxTP'15*, volume 186 of *EPTCS*, pages 74–88, Berlin, Germany, Aug. 2015.

[6] A. Assaf, G. Burel, R. Cauderlier, D. Delahaye, G. Dowek, C. Dubois, F. Gilbert, P. Halmagrand, O. Hermant, and R. Saillard. Dedukti: a logical framework based on the $\lambda\pi$-calculus modulo theory. Manuscript, 2016.

[7] F. Blanqui, G. Dowek, É. Grienenberger, G. Hondet, and F. Thiré. Some axioms for mathematics. In N. Kobayashi, editor, *6th International Conference on Formal Structures for Computation and Deduction, FSCD 2021, July 17-24, 2021, Buenos Aires, Argentina* (*Virtual Conference*), volume 195 of *LIPIcs*, pages 20:1–20:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

[8] D. Cousineau and G. Dowek. Embedding pure type systems in the lambda-pi-calculus modulo. In S. R. Della Rocca, editor, *Typed Lambda Calculi and Applications*, pages 102–117, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[9] G. Dowek and F. Thiré. Logipedia: a multi-system encyclopedia of formal proofs. Manuscript.

[10] G. Férey. *Higher-Order Confluence and Universe Embedding in the Logical Framework*. PhD thesis, 2021.

[11] G. Genestier. *Dependently-Typed Termination and Embedding of Extensional Universe-Polymorphic Type Theory using Rewriting*. PhD thesis, 2020. Thèse de doctorat dirigée par Blanqui, Frédéric et Hermant, Olivier Informatique université Paris-Saclay 2020.

[12] G. Genestier. Encoding agda programs using rewriting. 2020.

[13] F. Gilbert. Proof certificates in PVS. In *ITP 2017 - 8th International Conference on Interactive Theorem Proving*, volume 10499 of *ITP 2017: Interactive Theorem Proving*, pages 262–268, Brasilia, Brazil, Sept. 2017. Springer.

[14] R. Harper, F. Honsell, and G. Plotkin. A framework for defining logics. *J. ACM*, 40(1):143–184, Jan. 1993.

[15] G. Hondet and F. Blanqui. Encoding of Predicate Subtyping with Proof Irrelevance in the $\lambda\Pi$-Calculus Modulo Theory. In U. de'Liguoro, S. Berardi, and T. Altenkirch, editors, *26th International Conference on Types for Proofs and Programs* (*TYPES 2020*), volume 188 of *Leibniz International Proceedings in Informatics* (*LIPIcs*), pages 6:1–6:18, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[16] J. Lambek. A fixpoint theorem for complete categories. *Mathematische Zeitschrift*, 103:151–161, 1968.

[17] P. Martin-Löf and G. Sambin. *Intuitionistic type theory*, volume 9. Bibliopolis Naples, 1984.

[18] nLab authors. eta-conversion. `http://ncatlab.org/nlab/show/eta-conversion`, July 2021. Revision 12.

[19] The Agda Team. Agda's documentation. `https://agda.readthedocs.io/en/latest/`.

[20] F. Thiré. Sharing a library between proof assistants: Reaching out to the HOL family. In F. Blanqui and G. Reis, editors, *Proceedings of the 13th International Workshop on Logical Frameworks and Meta-Languages: Theory and Practice, LFMTP@FSCD 2018, Oxford, UK, 7th July 2018*, volume 274 of *EPTCS*, pages 57–71, 2018.

[21] F. Thiré. *Interoperability between proof systems using the logical framework Dedukti*. PhD thesis, ENS Paris-Saclay, 2020.

[22] V. Vene. *Categorical programming with inductive and coinductive types*.

Appendix B Typing rules for the λΠ-calculus modulo rewriting

The following describes typing in the λΠ-calculus modulo rewriting for a given set of rewrite rules $\mathcal{R}$. Given a context Γ, a signature Σ and $M, A \in \Lambda_{\lambda\Pi}$, we define the typing judgment $\Sigma; \Gamma \vdash M : A$ inductively by the following deduction rules[7]. The relation $\equiv$ in the rule Conv is the least equivalence relation containing $\equiv_\beta$ and the context and substitution closure of the rules in $\mathcal{R}$. In the rules Decl, Prod, Convs, Abs and Conv, the letter s stands either for **Type** or **Kind**.

Context forming rules

$$\frac{}{\Sigma; \emptyset \text{ well-formed}}\ \text{Empty} \qquad \frac{\Sigma; \Gamma \vdash A : s \qquad x \notin \Gamma}{\Sigma; \Gamma, x : A \text{ well-formed}}\ \text{Decl}$$

Term forming rules

$$\frac{\Sigma; \Gamma \text{ well-formed}}{\Sigma; \Gamma \vdash \textbf{Type} : \textbf{Kind}}\ \text{Sort}$$

$$\frac{\Sigma; \Gamma \vdash A : \textbf{Type} \qquad \Sigma; \Gamma, x : A \vdash B : s}{\Sigma; \Gamma \vdash \Pi x : A.B : s}\ \text{Prod}$$

$$\frac{\Sigma; \Gamma \text{ well-formed} \qquad x : A \in \Gamma}{\Sigma; \Gamma \vdash x : A}\ \text{Var}$$

$$\frac{\Sigma; \Gamma \text{ well-formed} \qquad c : A \in \Sigma \qquad \Sigma; \emptyset \vdash A : s}{\Sigma; \Gamma \vdash c : A}\ \text{Cons}$$

$$\frac{\Sigma; \Gamma \vdash \Pi x : A.B : s \qquad \Sigma; \Gamma, x : A \vdash M : B}{\Sigma; \Gamma \vdash \lambda x : A.M : \Pi x : A.B}\ \text{Abs}$$

$$\frac{\Sigma; \Gamma \vdash M : \Pi x : A.B \qquad \Sigma; \Gamma \vdash N : A}{\Sigma; \Gamma \vdash MN : B(N/x)}\ \text{App}$$

Conversion rule

$$\frac{\Sigma; \Gamma \vdash M : A \qquad \Sigma; \Gamma \vdash B : s \qquad A \equiv B}{\Sigma; \Gamma \vdash M : B}\ \text{Conv}$$

Typing rules for the λΠ-calculus modulo rewriting

Appendix C Universe polymorphism and eta-conversion

Among the many characteristics of Agda, universe polymorphism and eta-conversion are two very important features. In the following, we will look at how they are present in Agda and then we will discuss their encoding in Dedukti proposed by Genestier. As this part is not essential for understanding coinduction and its representation in Dedukti we preferred to leave it out of the main text, however we hope this can be of help to the interested reader wanting to learn more about this subject.

C.1 Universe polymorphism and eta-conversion in Agda

C.1.1 Universe polymorphism

As already said, Agda extends Martin-Löf Type Theory in a number of ways. One of these new features is the addition of *universe polymorphism*, which allows for building terms which can live in multiples universes. In order to understand what this means, suppose we want to define an inductive type for lists, associating to each type A in Set another type in Set of lists of A.

```
data List (A : Set) : Set where
  cons : A → List A → List A
  nil : List A
```

However, Set in Agda is just an alias for Set_0, as we have an infinite hierarchy $Set_0 : Set_1 : \ldots$ of sorts. Thus if we have a type B which lives in Set_1 we need to declare another inductive type $List_1 : Set_1 \to Set_1$ to build lists of elements in B, and so on if we have a type C living in Set_2. Universe polymorphism allows us to build the inductive type

```
data List (i : Level) (A : Set i) : Set i where
  cons : A → List i A → List i A
  nil : List i A
```

which can then be instantiated at each level, avoiding the declaration of an infinite number of versions of *List*. Universe polymorphism also allows us to build functions that can deal with types in multiple universes, such as the universe polymorphic identity function below.

```
id-poly : (i : Level) → (A : Set i) → A → A
id-poly i A x = x
```

In order to give a type to terms like $(i : \mathit{Level}) \to (A : \mathit{Set}\ i) \to A \to A$, Agda introduces a sort $\mathit{Set}\omega$ of universe polymorphic type. Using this sort, we can build types which feature *prenex* universe polymorphism, in which the level quantification occurs in the outer part of the term. This is what ensures us that the polymorphic definitions *List* and *id-poly* are indeed part of Agda's type theory.

However, Agda has also recently added a second sort hierarchy $\mathit{Set}\omega_0 : \mathit{Set}\omega_1 : \ldots$, which then also allows for *non-prenex* universe polymorphism, in which level quantification can appear anywhere in the term. This allows for instance to build the following function, which applies a universe polymorphic function f to a universe polymorphic value x to get another universe polymorphic value. The omega hierarchy also fixes a missing symmetry, as before the sort $\mathit{Set}\omega$ was the only sort not having a type. By adding the omega hierarchy, each $\mathit{Set}\omega_i$ is now typed by $\mathit{Set}\omega_{i+1}$.

```
app-poly : ((i : Level) → Set i → Set i) → ((i : Level) → Set i) → (i : Level) → Set i
app-poly f x i = (f i) (x i)
```

C.1.2 η-equivalence

Like some proof assistants (and unlike the $\lambda\Pi$-calculus modulo rewriting), the Agda conversion system features η-equivalence, a kind of dual to β-equivalence. Whereas β-reduction explains how to reduce an eliminator (application) applied to a constructor (abstraction)

$$(\lambda x : A.M)N \hookrightarrow_\beta M(N/x)\,,$$

η-expansion explains how to expand to a constructor applied to an eliminator[7]

$$f \hookrightarrow_\eta (\lambda x : A.f\ x) \qquad \text{with } f : \Pi x : A.B\,.$$

Of course, starting from a term $f : A \to B$ we could keep η-expanding to infinity, as this is a non-terminating process. However, by expanding $\lambda x : A.f\ x$ we would create a β-redex, thus we don not do this step and we say that $\lambda x : A.f\ x$ is in *eta-long form*.

Note that a major difference between β-reduction and η-expansion is that, whereas β-reduction can be defined in an untyped setting (as in the untyped λ-calculus), η-expansion needs to inspect the type of the term in order to know if it is η-expandable. Therefore, we say that η-expansion is a *type-directed* computation rule.

In the Agda system, this rule is also defined for most record types[8]. For instance, if we consider the previously defined record of dependent pairs, if *pair* is an element of $\Sigma\ \mathsf{Nat}\ (\lambda_.\mathsf{Nat})$ (the type of pairs of natural numbers), then we have

$$\mathit{pair} \equiv (\mathit{fst}\ \mathit{pair}, \mathit{snd}\ \mathit{pair})\,.$$

We then say that the term $(\mathit{fst}\ \mathit{pair}, \mathit{snd}\ \mathit{pair})$ is in eta-long form and we do not expand it anymore.

C.2 Representing universe polymorphism and eta-conversion

C.2.1 Universe polymorphism

Consider once again the universe polymorphic type of lists.

```
data List (i : Level) (A : Set i) : Set i where
  cons : A → List i A → List i A
  nil : List i A
```

In order to represent this inductive type in Dedukti we would have first to declare the following constant to represent this type.

$$List : \Pi i : L.U\ (set\ i) \to U\ (set\ i) \qquad (List\text{-decl})$$

However, remember that in order for this term to live in our representation of Agda, we need to be able to declare it as living in a type of the form $El_\alpha\ A$, such that $El_\alpha\ A$ reduces to the expected type $\Pi i : L.U\ (set\ i) \to U\ (set\ i)$. In our current encoding this would not be possible, as we are not able yet to represent universe polymorphism.

In order to add this feature to our representation we first add a sort $set\omega$ to type universe polymorphic types. Next, we need to add a function taking types depending on a level and producing a universe polymorphic type in $set\omega$. To do this, we add the function $\forall$ taking a sort depending on a level $(\alpha : L \to Sort)$ and a type in $U\ (\alpha\ i)$ depending on a level i $(A : \Pi i : L.U\ (\alpha\ i))$, and producing a universe polymorphic type. Finally, we declare a rule asserting that the elements of $\forall\ \alpha\ A$ are indeed functions giving for each i a type in $El_{(\alpha\ i)}\ (A\ i)$.

$$set\omega : Sort \qquad (set\omega\text{-decl})$$
$$\forall : \Pi\alpha : L \to Sort.(\Pi i : L.U\ (\alpha\ i)) \to U\ set\omega \qquad (\forall\text{-decl})$$
$$El_{_}\ (\forall\ \alpha\ A) \hookrightarrow \Pi i : L.El_{(\alpha\ i)}\ (A\ i) \qquad (\forall\text{-red})$$

Using this new encoding, we can now declare the constant $List$ as having a type of the form $El_\alpha\ A$.

$$List : El_{set\omega}\ (\forall\ (\lambda i : L.set\ (s\ i))\ (\lambda i : L.(\diamond\ (set\ i))\ {}_{set\ (s\ i)}\!\rightsquigarrow_{set\ (s\ i)}\ (\lambda_, \diamond\ (set\ i))))$$

We can also verify that its assigned type reduces to the expected one, as we have the reduction

$$El_{set\omega}\ (\forall\ (\lambda i : L.set\ (s\ i))\ (\lambda i : L.(\diamond\ (set\ i))\ {}_{set\ (s\ i)}\!\rightsquigarrow_{set\ (s\ i)}\ (\lambda_, \diamond\ (set\ i)))) \hookrightarrow \Pi i : L.U\ (set\ i) \to U\ (set\ i)\,.$$

An additional aspect of universe polymorphism which is much harder to represent is level conversion. In Agda, level conversion contains many identities which are semantically valid, such as $i \sqcup j \equiv j \sqcup i$, $(i \sqcup j) \sqcup k \equiv i \sqcup (j \sqcup k)$, $i \sqcup i \equiv i$, etc, and which are needed to be used when checking proofs and definitions. For instance, if we have a function $maxSet = \lambda i\ j : Level.Set_{i \sqcup j}$ taking two levels and yielding the highest instance of Set, then in Agdawe have the conversions $maxSet\ i\ j \equiv maxSet\ j\ i$ and $maxSet\ i\ i \equiv Set_i$. Even thought we also have this in Dedukti when we replace i and j by closed terms, for this to be true with variables we would have to have in Dedukti the conversions $i \sqcup j \equiv j \sqcup i$ and $i \sqcup i \equiv i$, which is not true for the encoding we have looked at until now. In order to take this into account, an extension of the representation of levels was proposed by Genestier, which uses AC conversion and matching. We will not enter into its details here, as this will not be important for us, but we refer to [12] for more details.

C.2.2 Eta-conversion

As we have already seen, computation in Agda features eta-expansion, a rewrite rule which, different from most, is type-directed. This characteristic makes eta-expansion impossible to be directly expressed with our notion of rewrite rule. Indeed, in the $\lambda\Pi$-calculus modulo rewriting a rewrite rule is a pair $l \hookrightarrow r$ in which l is of the form $cl_1 ... l_k$. We call this kind of rewriting untyped because matching is done purely syntactically, and we cannot inspect the types of the terms in order to know if a rewrite rule is applicable. In contrast, η-expansion is defined by

$$f \hookrightarrow \lambda x : A.f\ x \quad \text{if } f : \Pi x : A.B$$

and therefore we need to know the type of f in order to know if we can apply the rule. Moreover, this is not the only problem, as the applicability of this rule is also sensitive to the position on the term. Indeed, even if the term f appears in $\lambda x : A.f\ x$ with a type $\Pi x : A.B$, we cannot further expand it, as this would lead to non-termination issues.

Therefore, in order to solve this problem, we must both simulate a rule which is typed and prevent its non-termination loops. A possible solution is to introduce a symbol η allowing to annotate terms with their types.

$$\eta : \Pi(\alpha : Sort)(A : U\ \alpha).A \to A \ \text{(written as } \eta^{A}_{\alpha}) \qquad (\eta\text{-decl})$$

Using this symbol, we can properly match on a term's type in order to define eta-expansion. For instance, if f has a product type $A\ {}_{\alpha}\!\!\rightsquigarrow_{\beta}\ B$, then it can be eta-expanded using the following rule.

$$\eta^{A\ {}_{\alpha}\!\!\rightsquigarrow_{\beta}\ B}_{_}\ f \hookrightarrow \lambda x : El_{\alpha}\ A.\eta^{B\ x}_{\beta}\ (f\ x) \qquad (\eta \rightsquigarrow\text{-red})$$

Moreover note that, after the reduction, the application $f\ x$ gets annotated by the η symbol, and the outer abstraction is no more annotated. Therefore, unless if $f\ x$ has also a product type then the rewrite rule cannot be reapplied and thus we do not run into non-termination.

We can also add rules to express the eta-expansion of records. For instance, consider the record type of dependent pairs, which admits the following translation into Dedukti.

$$\Sigma : \Pi(A : U\ (set\ z))\ (B : El\ A \to U\ (set\ z)).U\ (set\ z) \qquad (\Sigma\text{-decl})$$

$$pair : \Pi(A : U\ (set\ z))\ (B : El\ A \to U\ (set\ z))\ (a : El\ A).$$
$$El\ (B\ a) \to El\ (\Sigma\ A\ B) \ \text{(written as } pair_{A,B}) \qquad (pair\text{-decl})$$

$$fst : \Pi(A : U\ (set\ z))\ (B : El\ A \to U\ (set\ z)).El\ (\Sigma\ A\ B) \to El\ A \ \text{(written as } fst_{A,B}) \qquad (fst\text{-decl})$$

$$snd : \Pi(A : U\ (set\ z))\ (B : El\ A \to U\ (set\ z))\ (x : El\ (\Sigma\ A\ B)).$$
$$El\ (B\ (fst_{A,B}\ x)) \ \text{(written as } snd_{A,B}) \qquad (snd\text{-decl})$$

$$fst_{_,_}\ (pair_{_,_}\ a\ b) \hookrightarrow a \qquad (fst\text{-red})$$

$$snd_{_,_}\ (pair_{_,_}\ a\ b) \hookrightarrow b \qquad (snd\text{-red})$$

We can add eta-expansion to this record by declaring the following rule.

$$\eta^{\Sigma\ A\ B}_{_}\ M \hookrightarrow pair_{A,B}\ (\eta^{A}_{set\ z}\ (fst_{A,B}\ M))\ (\eta^{B\ (fst_{A,B}\ M)}_{set\ z}\ (snd_{A,B}\ M)) \qquad (\eta\Sigma\text{-red})$$

This presentation gives the general intuition behind this representation. Nevertheless, in order to define precisely how the translation of η-expansion fully works, we would have to deal with many nuances and technical details, which we thus prefer to omit here. We refer to [12] for more details.

Appendix D More examples in translating coinduction

In subsection 2.3 we began to see some examples of how we can use coinduction in Agda and translate it into Dedukti. We continue here with some additional examples.

D.1 Predicates on streams

We have already seen how we can prove properties on streams using the language of musical coinduction. The same can be done with copattern matching coinduction. In this presentation of coinduction, we define the equality between two streams by the following type. Note that, as the streams defined in this setting are always infinite, then we do not have to consider the case in which the streams are both empty. Therefore, two streams are similar iff their heads are equal and their tails are similar.

```
record _∼_ {A} (xs : Stream A) (ys : Stream A) : Set where
  coinductive
  field
    hd-≡ : hd xs ≡ hd ys
    tl-∼ : tl xs ∼ tl ys
```

We represent this definition by the following declarations in Dedukti, in which the arguments x, y are left implicit.

$$\sim^{co} : \Pi(A : U\ (set\ z)).El\ (Stream^{co}\ A) \to El\ (Stream^{co}\ A) \to U\ (set\ z)\ \text{(written infix as } \sim^{co}_A\text{)} \qquad (\sim^{co}\text{-decl})$$

$$hd\text{-}\equiv : \Pi(A : U\ (set\ z))\ \{x\ y : El\ (Stream^{co}\ A)\}.$$
$$El\ (x \sim^{co}_A y) \to El\ ((hd_A\ x) \equiv (hd_A\ y))\ \text{(written as } hd\text{-}\equiv_A\text{)} \qquad (hd\text{-}\equiv\text{-decl})$$

$$tl\text{-}\sim : \Pi(A : U\ (set\ z))\ \{x\ y : El\ (Stream^{co}\ A)\}.$$
$$El\ (x \sim^{co}_A y) \to El\ ((tl_A\ x) \sim^{co}_A (tl_A\ y))\ \text{(written as } tl\text{-}\sim_A\text{)} \qquad (tl\text{-}\sim\text{-decl})$$

Once more, we can extend the operation of sum between natural numbers to streams and show that this extension preserves associativity.

```
_⊕_ : Stream Nat → Stream Nat → Stream Nat
hd (x ⊕ y) = (hd x) + (hd y)
tl (x ⊕ y) = (tl x) ⊕ (tl y)

⊕-assoc : (s1 s2 s3 : Stream Nat) → (s1 ⊕ s2) ⊕ s3 ∼ s1 ⊕ (s2 ⊕ s3)
hd-≡ (⊕-assoc s1 s2 s3) = +-assoc (hd s1) (hd s2) (hd s3)
tl-∼ (⊕-assoc s1 s2 s3) = ⊕-assoc (tl s1) (tl s2) (tl s3)
```

Note that the definition of $\oplus$ and the proof that it is associative is much simpler in the case of copattern matching coinduction then in the case of musical coinduction.

We can justify that by two reasons. First, as the streams here are always finite, we do not have to consider the special cases when one of the streams is empty. Even though considering them is straightforward, it makes the code a lot longer. However, the main reason for copattern matching coinduction being simpler to use is that we do not need to deal with control operators, as everything is automatically terminating, leading to much more natural proofs and definitions.

We can very straightforwardly translate the definition of $\oplus$ and the associativity proof in Dedukti by the following declarations.

$$\oplus^{co} : El\ (Stream^{co}\ \mathbb{N}) \to El\ (Stream^{co}\ \mathbb{N}) \to El\ (Stream^{co}\ \mathbb{N})\ \text{(written infix as } \oplus^{co}\text{)} \qquad (\oplus^{co}\text{-decl})$$
$$hd_{\mathbb{N}}\ (x \oplus^{co} y) \hookrightarrow (hd_{\mathbb{N}}\ x) + (hd_{\mathbb{N}}\ y) \qquad (\oplus^{co}\text{-red1})$$
$$tl_{\mathbb{N}}\ (x \oplus^{co} y) \hookrightarrow (tl_{\mathbb{N}}\ x) \oplus^{co} (tl_{\mathbb{N}}\ y) \qquad (\oplus^{co}\text{-red2})$$
$$\oplus\text{-}assoc^{co} : \Pi l_1\ l_2\ l_3 : El\ (Stream^{co}\ \mathbb{N}).El\ (((l_1 \oplus^{co} l_2) \oplus^{co} l3) \sim^{co}_{\mathbb{N}} (l_1 \oplus^{co} (l_2 \oplus^{co} l_3))) \qquad (\oplus\text{-}assoc^{co}\text{-decl})$$
$$hd\text{-}\equiv_{\mathbb{N}}\ (\oplus\text{-}assoc^{co}\ l_1\ l_2\ l_3) \hookrightarrow +\text{-}assoc\ (hd_{\mathbb{N}}\ l_1)\ (hd_{\mathbb{N}}\ l_2)\ (hd_{\mathbb{N}}\ l_3) \qquad (\oplus\text{-}assoc^{co}\text{-red1})$$
$$tl\text{-}\sim_{\mathbb{N}}\ (\oplus\text{-}assoc^{co}\ l_1\ l_2\ l_3) \hookrightarrow \oplus\text{-}assoc\ (tl_{\mathbb{N}}\ l_1)\ (tl_{\mathbb{N}}\ l_2)\ (tl_{\mathbb{N}}\ l_3) \qquad (\oplus\text{-}assoc^{co}\text{-red2})$$

D.2 Formal languages

Up until now we have only seen the example of streams, however coinduction is a very powerful principle that allows us to deal with many kinds of mathematical objects. One of these objects are formal languages, which can be represented in a very elegant way using coinduction. Following [1], we present in this part the basic ideas of how this can be done in Agda, and then show how this can be translated into Dedukti. We limit our discussion only to the case of copattern matching coinduction, in order to prevent extending ourselves too much over this subject.

Given an alphabet A, a language over A is simply a subset $L \subseteq A^*$, where A^* is the free monoid generated by A, that is, the set of finite lists with elements in A. A language L can be also described by the following data: a Boolean $\nu : Bool$ stating whether ε is in L and a function $\delta : A \to \mathcal{P}(A^*)$ mapping each letter a to the language $a^{-1}L$ defined by $ax \in L \iff x \in a^{-1}L$. This decomposition can then be used to represent formal languages very elegantly as coinductive types.

```
record Lang (A : Set) : Set where
  coinductive
  field
    ν : Bool
    δ : A → Lang A
```

$$
\begin{array}{ll}
\mathit{Lang} : U\ (\mathit{set}\ z) \to U\ (\mathit{set}\ z) & (\mathit{Lang}\text{-decl}) \\
\nu : \Pi A : U\ (\mathit{set}\ z).\mathit{El}\ (\mathit{Lang}\ A) \to \mathit{El}\ \mathit{Bool}\ \ (\text{written as } \nu_A) & (\nu\text{-decl}) \\
\delta : \Pi A : U\ (\mathit{set}\ z).\mathit{El}\ (\mathit{Lang}\ A) \to \mathit{El}\ A \to \mathit{El}\ (\mathit{Lang}\ A)\ \ (\text{written as } \delta_A) & (\delta\text{-decl})
\end{array}
$$

Using this representation, we can define many of the objects and operations that we normally use with formal languages. For instance, we can define the empty language by corecursion by stating that $\nu\ (\emptyset\ A)$ is false ($\varepsilon \notin \emptyset$) and that, for all $a : A$, $\delta\ (\emptyset\ A)\ a$ is defined by making a corecursive call to $\emptyset$.

$$
\begin{array}{l}
\emptyset : (A : \mathsf{Set}) \to \mathsf{Lang}\ A \\
\nu\ (\emptyset\ A) = \mathsf{false} \\
\delta\ (\emptyset\ A)\ _ = \emptyset\ A
\end{array}
$$

$$
\begin{array}{ll}
\emptyset : \Pi A : U\ (\mathit{set}\ z).\mathit{El}\ (\mathit{Lang}\ A)\ \ (\text{written as } \emptyset_A) & (\emptyset\text{-decl}) \\
\nu_\ \emptyset_ \hookrightarrow \mathit{false} & (\emptyset\text{-red1}) \\
\delta_\ \emptyset_A\ _ \hookrightarrow \emptyset_A & (\emptyset\text{-red2})
\end{array}
$$

Given two languages $L_1, L_2 : \mathit{Lang}\ A$ we can also define the sum $L_1 \uplus L_2$ by stating that $\nu\ (L_1 \uplus L_2)$ is true if it is also the case for L_1 or L_2, and for each $x : A$, $\delta\ (L_1 \uplus L_2)\ x$ is defined as the sum of $x^{-1}L_1$ and $x^{-1}L_2$ (thus, by doing a corecursive call).

$$
\begin{array}{l}
\uplus : \{A : \mathsf{Set}\} \to \mathsf{Lang}\ A \to \mathsf{Lang}\ A \to \mathsf{Lang}\ A \\
\nu\ (a \uplus b) = \nu\ a \vee \nu\ b \\
\delta\ (a \uplus b)\ x = \delta\ a\ x \uplus \delta\ b\ x
\end{array}
$$

$$
\begin{array}{ll}
\uplus : \Pi A : U\ (\mathit{set}\ z).\mathit{El}\ (\mathit{Lang}\ A) \to \mathit{El}\ (\mathit{Lang}\ A) \to \mathit{El}\ (\mathit{Lang}\ A)\ \ (\text{written infix as } \uplus_A) & (\uplus\text{-decl}) \\
\nu_\ (a \uplus_A b) \hookrightarrow (\nu_A\ a) \vee (\nu_A\ b) & (\uplus\text{-red1}) \\
\delta_\ (a \uplus_A b)\ x \hookrightarrow (\delta_A\ a\ x) \uplus_A (\delta_A\ b\ x) & (\uplus\text{-red2})
\end{array}
$$

We can also try to do the same with the product of two languages. Given L_1, L_2 we have $\varepsilon \in L_1 \times L_2$ if and only if $\varepsilon \in L_1, L_2$. The definition of δ is a bit trickier: given a letter x we do a case analysis on $\nu\ L_1$. If L_2 does not contain the empty word, then the words in $x^{-1}(L_1 \times L_2)$ are those of the form $w_1 w_2$, where $xw_1 \in L_1$ and $w_2 \in L_2$, that is, in $\delta\ L_1\ x \times L_2$. If we have $\varepsilon \in L_1$ then in additional to the previous words, we also have the w such that $xw_2 \in L_2$, that is, the words in $\delta\ L_2\ x$.

This gives the following definition of $\times$ in Agda.

$$
\begin{array}{l}
\times : \forall\ \{A : \mathsf{Set}\} \to \mathsf{Lang}\ A \to \mathsf{Lang}\ A \to \mathsf{Lang}\ A \\
\nu\ (a \times b) = \nu\ a \wedge \nu\ b \\
\delta\ (a \times b)\ x = \mathsf{if}\ \nu\ a\ \mathsf{then}\ (\delta\ a\ x \times b) \uplus \delta\ b\ x\ \mathsf{else}\ \delta\ a\ x \times b
\end{array}
$$

However, if we try to typecheck this proof in Agda we actually get the error "Termination checking failed for the following functions: _×_". In order to understand why, remember from section 1.2 that in order for a function to be corecursive, any corecursive call must be guarded by a constructor of the coinductive type of the codomain. When dealing with copattern matching coinduction this means that when defining the corecursive value of a coinductive type constructor (δ in this case), its clause needs to start directly with a corecursive call. But in the case of $\times$ this is clearly not true, as we start with an if-then-else statement, and thus Agda is not able to automatically check that the given definition is terminating.

The way proposed in [1] to solve this problem is to use size types, which are size annotations allowing to help Agda to see that a definition is terminating. This enhances the expressivity of coinduction, as one can then code functions and make proofs with less syntactic constraints. Unfortunately, at the present Agda2Dedukti does not support the translation of sized types. Even thought Dedukti does not check the termination by itself, and thus does not need the information that sized types bring, they also cause typechecking problems, and thus we would need to adapt the encoding in order to treat them.

One possibility in to erase all those annotations during the translator phase, and that is what we plan to implement in the future. However, for the time being a temporary solution is to mark as terminating the functions that Agda is not capable of automatically proving to terminate. Of course, this risks compromising the soundness of the proofs, as Agda simply ignores the termination checking phase for the concerned functions. However, if we are able to show with sized types that such functions terminate, we can just manually erase the sized types and mark the functions as terminating, before using the translator Agda2Dedukti.

Using this strategy we can translate functions such as $\times$, and in this case we have the following declarations in Dedukti.

$$\times : \Pi A : U\ (set\ z).El\ (Lang\ A) \to El\ (Lang\ A) \to El\ (Lang\ A)\ \text{(written infix as } \times_A) \qquad (\times\text{-decl})$$
$$\nu_{_}\ (a \times_A b) \hookrightarrow (\nu_A\ a) \wedge (\nu_A\ b) \qquad (\uplus\text{-red1})$$
$$\delta_{_}\ (a \times_A b)\ x \hookrightarrow if\text{-}then\text{-}else_A\ (\nu_A\ a)\ (((\delta_A\ a\ x) \times_A b) \uplus_A (\delta_A\ b\ x))\ ((\delta_A\ a\ x) \times_A b) \qquad (\uplus\text{-red2})$$

Appendix E End-notes

You can click on the number to get back to where the end-note was made.

[1] More precisely, the addition of dependent types only renders the system more expressive because we are also allowed to have types of the form $A_1 \to ... \to A_k \to$ **Type**, otherwise it would be always possible to replace any occurrence of $\Pi x : A.B$ by $A \to B$.

[2] More precisely, with minimal intuitionistic predicate logic, that is, the fragment on intuitionistic predicate logic only featuring implication and universal quantification.

[3] The term *sort* here is a synonym for domain of discourse, and means something else than the sorts in type theory.

[4] This part only concerns closed terms in normal form. For instance, if we consider elements of $\mathbb{N}$ closed but not in normal form we also have $(\lambda x : \mathbb{N}.x)\ 0$ which does not fit this description. Likewise, if we consider elements of $\mathbb{N}$ in normal form but not closed, we can have for instance a variable x of type $\mathbb{N}$. However, by imposing those two constraints at the same time, we are assured (in systems which have the *canonicity* property, which is a desirable metaproperty in most cases) that such elements of inductive types are indeed the least fixed points of the presented function.

[5] However, this feature can be enabled by a flag.

[6] A hierarchy *Prop* of proof irrelevant types was recently added to Agda, however the "standard" way of doing Agda is to do everything with *Set*. For instance, Agda's standard library does not use *Prop*.

[7] We can also define η-equivalence by means of η-reduction, however this is not so well-behaved when dealing with other types, such as the singleton type[18].

[8] See the Agda documentation at [19] for a detailed description of which records are allowed or not to feature η-equivalence.