A Programming Logic Based on Type Theory

Proefschrift

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de Rector Magnificus, prof.dr. J.H. van Lint, voor een commissie aangewezen door het College van Dekanen in het openbaar te verdedigen op woensdag 5 oktober 1994 om 16.00 uur

door

Erik Poll

geboren te Haarlemmermeer
Dit proefschrift is goedgekeurd door de promotoren

prof dr. F. E. J. Kruseman Aretz
prof dr. H P Barendregt

en de co-promotor

dr.ir. C Hemerik
Acknowledgements

The research on which this thesis is based was carried out while I was employed by the Dutch organisation for scientific research NWO, on the SION-project "Typed Lambda Calculi".

I would like to thank Kees Hemerik for his guidance and stimulation over the past four years, and for always insisting on more text between the formulas.

Thanks also go to the other members of the manuscript committee – Henk Barendregt, Marc Bezem, Frans Kruseman Aretz and Rob Nederpelt – for their valuable suggestions and comments on draft versions of this thesis.

Finally, I want to thank all the people I've enjoyed working with over the past four years, in particular Bert van Benthem Jutting, Tijn Borghuis, Huub ten Eikelder, Herman Geuvers, and Paula Severi.

NWO
Contents

Summary iii

Samenvatting v

1 Introduction 1
   1.1 Background 1
   1.2 Aims and Motivations 2
   1.3 Overview of this thesis 5

2 Pure Type Systems 9
   2.1 PTSs 10
   2.2 DPTSs 16
   2.3 Relation between PTSs and DPTSs 21

I Syntax 25

3 The Basic System : $\lambda\omega_L$ 27
   3.1 $\lambda\omega$ as a programming language : $\lambda\omega_p$ 28
   3.2 $\lambda\omega$ as a logic : $\lambda\omega_p$ 33
   3.3 The programming logic $\lambda\omega_L$ 37
   3.4 Program and Proof Development 44
      3.4.1 Coupled derivation rules for function types 45
      3.4.2 Coupled derivation rules for polymorphic types 46
      3.4.3 Other datatype-constructors 51
   3.5 Comparison with Program Extraction in $\lambda C$ 54

4 Simple Extensions 57
   4.1 Extending PTSs with $+, \times$ and $\Sigma$ 58
      4.1.1 Cartesian Products 59
      4.1.2 Disjoint Sums 60
      4.1.3 Dependent Sums 62
      4.1.4 Labeled Products 65
      4.1.5 Labeled Sums 67
      4.1.6 Properties of (D)PTSs extended with $+, \times$ and $\Sigma$ 69
   4.2 Extension of the Programming Language 71
   4.3 Extension of the Programming Logic 76
Summary

Typed lambda calculi can be seen as functional programming languages or – by the Curry-Howard-de Bruijn isomorphism – as logics. The first view provides a solid basis for richly typed programming languages. The second view is the basis of several systems for the machine-assisted construction and verification of proofs. Together, the two points of view offer the possibility of using type theory as the basis for programming logics, i.e., logics in which we can reason about programs and datatypes, and in which we can prove that a program satisfies a certain specification.

One approach, made possible by the expressive power of type systems, is to identify the notions of datatype and specification, and obtain programs from constructive proofs. This approach is, for instance, taken in the system Coq, where programs are obtained from constructive proofs in the Calculus of Constructions, via some extraction operation [PM89a]. From a theoretical point of view, this approach seems very elegant, but from a practical point of view it has the disadvantage that a program under construction can only be manipulated indirectly via its proof. Ways to avoid the need for an extraction operation have been considered in Martin-Löf's type theory [NPS90] and in Nuprl [Con86], using so-called subset types, but these have the very serious disadvantage of making type checking undecidable.

From a practical point of view, it seems preferable to have a programming logic in which programs and correctness proofs are separate objects, and which allows the simultaneous development of programs and their correctness proofs, somewhat similar to the method advocated by Hoare and Dijkstra. Such a programming logic is the subject of this thesis.

Starting point of this thesis are the Pure Type Systems (PTSs) [Bai92], a large class of type systems which can be described in a uniform way. Apart from PTSs we also use DPTSs, which are extensions of PTSs with a definition mechanism. The extension with definitions does not increase the overall expressive power of a PTS, but it is indispensable for practical use.

We design a PTS $\lambda \omega_L$, which consists of a typed functional programming language and an associated logic in which properties of programs can be stated and proved. This programming language is the system $\lambda \omega$, which is the PTS corresponding to Girard's system $F^{=\omega}$. The system $\lambda \omega_L$ provides a single language for programs, datatypes, proofs, propositions and specifications, and integrates a strong type system for programs with a specification system for programs. Verification of proofs is a special case of type checking, and is easy to implement.

Programs and correctness proof are separate, but related, objects in $\lambda \omega_L$. They can be constructed hand in hand, in a compositional manner, by stepwise refinement. It is also possible to prove the correctness of program transformation rules in the system, and use such rules to develop programs and their correctness proofs.

An implementation of the system would offer a programming environment combining a
syntax-directed editor for well-typed programs and a goal-directed proof assistant.

The basic system \( \lambda \omega_L \) is extended with different language constructs that are useful for programs and datatypes. First, it is extended with labelled products and sums -- i.e. records and variants -- and with abstract datatypes. The second extension is the inclusion of recursion, i.e. of recursive programs and recursive datatypes. This extension with recursion changes the nature of the programming language. The programs are no longer all terminating, which results in partial objects. To reason about recursive programs, the logic is extended in the style of LCF, with axioms stating that recursive programs are least fixed points.

The syntax of \( \lambda \omega_L \) and its extensions is discussed in the first part of this thesis, along with the underlying design considerations, and some simple examples to illustrate the intended use of the systems. The main syntactical properties of the systems are given. These establish the soundness of the type systems, and some of them, notably strong normalisation, are important for the decidability of typechecking.

The semantics of \( \lambda \omega_L \) and its extensions is treated in the second part of this thesis. Of all the systems that have been introduced we give models, which provide the justification (and the inspiration) of the different extensions.

These models provide denotational semantics for the parts of the systems used as programming languages. First, the general structure of models for these programming languages is described, by extending the Bruce-Meyer-Mitchell models [BMM90]. Then we give instantiations of these general model definitions. For the languages without recursion, these instantiations are the standard PER-models. For the language with recursion, this instantiation is a CPO-model, in which datatypes are interpreted as cpos and recursive programs as least fixpoints. This domain-theoretic model provides the basis for reasoning about recursive programs and partial objects.

For the parts of the systems used as logics, proof-irrelevance models are given, in which propositions are interpreted as truth values. These simple interpretations are all that is needed to prove consistency of the logics, and consistency of any axioms that we may want to include.
Samenvatting

Getypeerde lambda-calculi kunnen enerzijds beschouwd worden als functionele programmeetalen, en anderzijds - dankzij het Curry-Howard-de Bruijn isomorfisme - als logica's. Het eerste gezichtspunt biedt een solide basis voor programmeer- talen, en anderzijds - dankzij het Curry-Howard-de Bruijn isomorfisme - als logica's. Het eerste gezichtspunt is overtuigend als basis voor programmalogica's d.w.z. logica's voor het redeneren over programma's en datatypen, waarin bewezen kan worden dat een programma aan een bepaalde specificatie voldoet.

Een aanpak, die mogelijk gemaakt door de expressiviteit van typesystemen, is om de begrippen datatype en specificatie te identificeren, en programma's te verkrijgen uit constructieve bewijzen. Deze benadering wordt bijvoorbeeld gebruikt in het systeem Coq, waar programma's worden verkregen uit constructieve bewijzen in de Calculus Van Constructions, via een extractie-operatie [PM89a]. Vanuit theoretisch oogpunt is deze aanpak erg elegant, maar praktisch gezien heeft het als nadeel dat een programma tijdens constructie alleen indirect gemanipuleerd kan worden via het bewijs ervan.

In Martin-Löf's type theorie [NPS90] en in Nuprl [Con86], is gekeken naar de mogelijkheid om zo'n extractie-operatie overbodig te maken, door zgn. subset typen te gebruiken. Deze hebben echter het grote nadeel dat typeering onbeslisbaar wordt.

Voor praktische programmaconstructie lijkt het beter om een programmalogica te hebben waarin programma's en een correctheidsbewijzen aparte objecten zijn, die echter wel tegelijkertijd kunnen worden geconstrueerd, op een vergelijkbare manier als voorgesteld door Hoare en Dijkstra. Zo'n programmalogica is het onderwerp van dit proefschrift.

Uitgangspunt van dit proefschrift zijn de Pure Type Systems (PTSen) [Bar92], een grote klasse van typesystemen die op uniforme manier beschreven kunnen worden. Behalve PTSen worden ook DPTSen gebruikt, uitbreidingen van PTSen met een definitiemechanisme. The uitbreiding van een PTS met definities verhoogt de totale expressieve kracht van een PTS niet, maar is onmisbaar in praktisch gebruik.

We ontwerpen een PTS $\lambda W L$, dat bestaat uit een getypeerde functionele programmeertaal, en een bijbehorende logica voor uitspraken over programma's en datatypen. De programmeertaal is het systeem $\lambda W$, het PTS dat overeenkomt met Girard's systeem $F^\omega$. Het systeem $\lambda W L$ biedt een taal taal voor programma's, datatypen, bewijzen, proposities en specificaties, en integreert een krachtig typesysteem voor programma's met een specificatietaal voor programma's. Bewijsverificatie is een bijzonder geval van typecontrole, en eenvoudig te implementeren.

Programma's en correctheidsbewijzen zijn aparte, maar verwante, objecten in $\lambda W L$. Ze kunnen hand in hand geconstrueerd worden, op een compositionele manier, door stapsgewijze verfijning. Ook is het mogelijk om de correctheid van programmatransformaties aan te tonen.
in \( \lambda \omega_L \), en zulke transformaties te gebruiken bij het ontwikkelen van programma’s en hun correctheidsbewijzen.

Een implementatie van het systeem zou een programmeeromgeving bieden, waarin een syntax-gestuurde editor voor goedgetypeerde programma’s wordt gekombineerd met een doelgestuurde bewijs-assistent.

Het kalkule systeem \( \lambda \omega_L \) wordt uitgebreid met verschillende taakconstructies die nuttig zijn voor programma’s en datatypen. Eerst wordt het uitgebreid met gelabelde product- en somtypen – d.w.z. records en variants – en met abstracte datatypen. Daarna wordt het systeem uitgebreid met recursieve programma’s en recursieve datatypen. De programmeertaal verandert nogal met de de uitbreiding met recursie. Het is niet langer het geval dat alle programma’s niet-termineren. Om over recursieve programma’s en mogelijk niet-terminerende berekeningen te redeneren wordt de logica uitgebreid op de stijl van LCF, met axioma’s die uitdrukken dat recursieve programma’s kleinste dekpunten zijn.

The syntax van \( \lambda \omega_L \) en haar uitbreidingen wordt behandeld in het eerste deel van dit proefschrift met de overwegingen die hiervan ten grondslag liggen, en enkele eenvoudige voorbeelden om het beoogde gebruik te verduidelijken. De belangrijkste syntactische eigenschappen van de systemen komen aan de orde. Deze tonen de gezondheid van de type-systemen aan, en sommige, in het bijzonder sterke normalisatie, zijn belangrijk voor beslisbaarheid van typen.\n
The semantiek van \( \lambda \omega_L \) en de uitbreidingen ervan komt aan de orde in het tweede deel van dit proefschrift. Van alle systemen die gedefinieerd zijn worden modellen gegeven, die de rechtvaardiging (en soms ook de inspiratie) van de verschillende uitbreidingen geven.

Voor die delen van de systemen die als programmesysteem dienen, bestaan deze modellen uit de notatiede semantiek. Eerst wordt de algemene structuur van modellen voor deze programmeertalen beschreven, door de Bruce-Meyer-Mitchell models [BMM90] uit te breiden. Daarna worden instantiaties van deze algemene model definities gegeven. Deze instantiaties zijn de gebruikelijke PER-modellen voor de talen zonder recursie. Voor de programmeertaal met recursie wordt een CPO-model als instantiatie gegeven, waarin datatypen als cpo’s en recursieve programma’s als kleinste dekpunten worden geïnterpreteerd. Dit model biedt de basis het redeneren over recursieve programma’s en non-terminatie.

Voor die delen van de systemen die als logica’s dienen, worden proof-irrelevance modellen gegeven, waarin proposities als waarheidswaarden geïnterpreteerd worden. Deze eenvoudige interpretaties volstaan om consistentie van logica’s aan te tonen, en consistentie van axioma’s die we zouden willen toevoegen.
Chapter 1

Introduction

1.1 Background

There has been a steady evolution in the type systems used in programming languages. The first programming languages, such as assembly languages and LISP, were untyped. The first higher-order languages provided a few base types, such as integers and reals. Later, programming languages offered increasingly powerful constructions with which programmers could build their own types. To meet the need for more flexible type systems, features such as subtyping and polymorphism were included, and, more recently, object-oriented languages were introduced.

Typed lambda calculi can be viewed as rudimentary, but very pure and expressive programming languages. This view provides a solid basis for richly typed (functional) programming languages. It offers a framework for the description and classification of type systems of programming languages, and often suggests improvements and generalisations (see for example [Rey85], [Car89], and [BH90]).

Typed lambda calculi can also be viewed as (constructive) logics, by the so-called Curry-Howard-de Bruijn isomorphism. Types are then regarded as propositions, and terms as their proofs. This is the view taken in AUTOMATH [dB80], Martin-Löf's Type Theory [ML79], Edinburgh Logical Framework (LF) [HHP93], and the Calculus of Constructions [CH88]. Implementations of AUTOMATH provided mechanical verification of mathematical proofs. The other systems have also been implemented, namely in Nuprl [Con86], LEGO [LP92], and Coq [Dow91]. These implementations not only verify proofs, but also provide some computer-assistance for the construction of proofs.

The two possible interpretations of typed lambda calculi – as typed programming languages and as logics – make type theory a suitable basis for programming logics, i.e. logics in which specifications can be expressed and in which it can be proved (or disproved) that a program meets a certain specification.

The best-known example of a programming logic is Hoare's logic. However, Hoare's logic suffers from the mismatch between the object language for programs and the logical language, in particular where it concerns the status of variables, and from the very rigid format of the judgement (see [Apt81]). Also, the scopes of variables and assumption are not always clear. These problems makes it difficult to reason about functions and procedures.
CHAPTER 1. INTRODUCTION

The advantage of a single formalism that provides both the notions of program and datatype and the notions of proof and propositions, is that the programming language and the logic are more in tune. This means we can hope to avoid problems like the ones mentioned above.

1.2 Aims and Motivations

Our aim is the design of a programming logic, that is based on type theory, but whose language constructs and deduction rules are geared towards practical program construction. The system should offer the possibility for the mechanical verification of proofs. The ultimate goal is an implementation of the system that provides a programming environment for constructing programs and their correctness proofs.

There are several reasons for integrating the programming language and logic in one formalism.

One is that it may help to obtain a compact and homogeneous system that is as elegant and general as possible. Programs, datatypes, proofs, propositions, and specifications can all be handled in a uniform way.

Also, certain primitives in the programming language will require matching primitives in the logic. For instance, to reason about programs of the form (\( \lambda x. \text{nat} \ldots \)), we probably need universal quantifications of the form (\( \forall x. \text{nat} \ldots \)). By working in one formalism, we can hope that the primitives in programming language and logic are well-matched.

An added bonus is that proof checking is the same as type checking, so that the same algorithms can be used for type checking and proof checking.

The most important design consideration is the expressivity of the type system for programs. The remainder of this section is dedicated to the motivation of our choice. We compare some of the alternatives, and consider the different kinds of programming logics they result in.

There is a whole spectrum of type systems for programming languages. At one end of the spectrum are the untyped programming languages. Here we effectively have just one type, which is the type of all programs. At the other end of the spectrum are very expressive type systems, such as Martin-Löf's Type Theory and the Calculus of Constructions. Here types are complete specifications, and the type of a program provides all the relevant information about its (functional) behaviour. Most of the conventional programming languages lie somewhere between these two extremes. The type of a program gives some information about the program, but not all of it.

In all but the most expressive type systems, a type alone does not suffice as the specification of a program. Apart from the type, some additional information is needed to tell which programs of that type have all the required properties. This information can be regarded as a predicate with that type as domain, which characterises a subset of that type.

Regardless of how expressive the type system of the programming language is, we can say that a specification is a pair that consists of

- a type, and
- a predicate on that type,
1.2. AIMS AND MOTIVATIONS

A solution of a specification is a pair that consists of

- a program of the right type, and
- a proof that this program satisfies the predicate.

It depends on the strength of the type system how much of a specification is expressed by the type, and how much this leaves to be expressed by the predicate. In very strong type theories all information we may want to express in a specification can be expressed in the type, so no predicate is needed. In untyped languages no information can be expressed in the type, and the whole specification is given by the predicate. And in most conventional programming languages, some information can be expressed by the type, but the larger part of a specification is expressed by the predicate. In fact, there may be some overlap between the information given by the type and the predicate.

So we can make a (rough) distinction between three kinds of programming logics:

(i) An untyped programming language with all information about programs expressed in predicates.

(ii) A typed programming language, with some information about programs expressed in types, and the rest in predicates.

(iii) A typed programming language with a very expressive type system, where all information about programs is expressed in their types.

In [Gir86] the first two are called external programming logics and the last kind is called an integrated programming logic. We use the term internal instead of integrated. In external programming logics, specifications and correctness proofs live outside of the programming language. In internal programming logics, these notions are internal to the programming language; the type of a program is its specification, and type checking amounts to verification. A comparison of these different kinds of programming logics is given in [Dyb90].

Regardless of how the specification is divided over type and predicate, the total amount of work it takes to establish correctness of an algorithm is roughly the same. From a pragmatic point of view, however, there are big differences between the different approaches. The programming logics in this thesis are all of the kind (ii). Basically, in types as much information is expressed as can be mechanically verified. Below we motivate our preference for (ii) over (i) and (iii).

Why types?

To explain why we do not favour approach (i), we briefly review the reasons for having types in a programming language.

The essential property of types is that they impose restrictions on the interaction between objects. The type of an object controls the access to that object and the ways it can be used. As a result, some of its properties can be hidden from the outside world. For this it is vital that all type constraints can be verified mechanically by a type checking algorithm.

One advantage of types concerns the implementation of programming languages. In a typed language, we can take advantage of efficient machine representations for certain base
types, such as integers or reals, or for certain type-constructions, such as arrays. The restrictions enforced by the type system keep these representations hidden from the programmer and prevent illegal operations on them.

The other advantages of types concern the use of the programming language. The type system impose restrictions on the combinatorial freedom. These restrictions can prevent simple mistakes, e.g. multiplying a boolean with a natural number.

More important for the construction of programs is the way in which data-structuring helps to organise programs. The classification of programs and data that is provided and enforced by the type system helps to structure programs, and makes programs easier to read.

Finally, there is the possibility of data-abstraction. In a typed programming language abstract datatypes can be used to hide information about one part of a program form the rest of the program.

The type of a program can be seen as an incomplete specification of a program. For example, if \( f : \text{int} \rightarrow \text{int} \), then \( f \) is a function that maps integers to integers. This is of course a very incomplete specification - we still have no clue as to what \( f \) is , but such incomplete specifications have the advantage of being very easy to write and to read. Moreover, they can easily be verified, and a type-checker can guarantee that these incomplete specifications are met.

Why not specifications as types?

Most research on programming logics based on type theory concerns systems of kind (iii). Here the notions of type and specification are identified, as are the notions of program and correctness proof.

This idea dates back to Heyting’s semantics of constructive proofs: a constructive proof \( f \) of \( \forall x \in A. \text{pre}(x) \Rightarrow \exists y \in B. \text{post}(x,y) \) contains an algorithm which, given a term \( x \) and a proof of \( \text{pre}(x) \), returns a term \( y \) and a proof of \( \text{post}(x,y) \). The proposition gives all the relevant information about this algorithm. It is its specification.

This approach to program construction is attractive at first sight. However, the problem is that constructive proofs have taken the place of programs, and it is difficult to separate the algorithmic part of these constructive proofs from the correctness part. Typically, the larger part of the constructive proof \( f \) above will be devoted not to the construction of the witness \( y \), but to the proof of \( \text{post}(x,y) \). This proof is important for the correctness, but not for the algorithm.

It is possible to obtain programs from proofs by an ”extraction” operation. In [PM89a] such an extraction procedure is defined for the Calculus of Constructions. However, this leaves the problem that the program that will eventually be extracted from a proof is not visible during the construction of that proof. Consequently, design choices can only be made on the basis of the specification, and not on the basis of an operational understanding of the algorithm or efficiency considerations.

In Martin-Löf’s Type Theory there is an alternative to program extraction. So-called subset-types can be used to discard the correctness parts of a proof (see [NPS90]). However, this has the – very high – price of making typing undecidable. This should not come as a surprise: we cannot expect that it is decidable whether a program satisfies a specification. The undecidability of type-checking means that there is little practical difference between this approach and approach (i). In fact, it can be argued that these systems are no longer
1.3 OVERVIEW OF THIS THESIS

internal programming logics, because, although specifications live inside the system, proofs that programs have certain types, - correctness proofs - live outside it.

There are an important differences between (ii) and (iii). When types are complete specifications, some of the advantages of having types that were mentioned earlier are lost. Types are no longer easy to read and write, and type constraints are no longer easy to verify.

One practical difference occurs in situations where we do not have a complete specification for a program. In practice, such situations occur frequently, because for large programs complete correctness proofs are not feasible, and not even all that interesting. Typically, our only concern is the correctness of relatively small "algorithmic" parts of the program. Approach (ii) is then much more convenient than (iii). It gives us the freedom to choose for which parts of a program we give complete specifications and correctness proofs. For the rest of the program we use the incomplete specifications provided by the type system.

During the construction of a program the specification may change. An advantage of the distinction between type information and the logical information - given by the predicate - in approach (ii) is that any changes in the specification are more likely to be in the predicate than in the type. This also affects the re-usability of programs and types. The same type can be used in different situations, with different predicates. For example, a type of trees can be used with different predicates, for instance predicates expressing that the trees are sorted or balanced.

1.3 Overview of this thesis

As starting point we use Pure Type Systems (PTSs), as described for instance in [Bar92]. In particular, we use the PTSs in Barendregt's $\lambda$-cube, which give the fine-structure of the Calculus of Constructions. The nice thing about PTSs is that many type systems can be defined as PTSs, and that these definitions are very compact. This makes it easy to compare systems, and is also useful to design a type system for a particular purpose. Another advantage of using PTSs is that their syntactic theory is well-developed.

Apart from PTSs, we also use DPTSs. A DPTS is the extension of a PTS with a definition-mechanism. This extension does not increase the overall expressive power of a PTS, but it is indispensable for practical use.

We design a PTS $\lambda \omega_L$ that can be used as a programming logic. In this PTS both programs and their correctness proofs can be handled as related but distinguishable objects. There is a strict separation between the programming language and the logic: expressions in the programming language cannot depend on logical expressions. Of course, logical expressions can depend on expressions from the programming language.

Two extensions of this basic system are given. The reason for these extensions is pragmatic: we want to include more language constructs that are useful for programs and datatypes in the programming language. First the system is extended with more type-constructors (namely $+, \times$ and $\Sigma$), and then it is extended with recursion. For the logic associated extensions are needed for reasoning about these new language constructs.

Three aspects of the basic system and its extensions can be distinguished: syntax, pragmatics and semantics.
Syntax

Of all the systems the most important syntactic properties are given, such as subject reduction and uniqueness of types. These properties are the basic "soundness" criteria for any type system. For PTSs most of these properties are well-known, and for the different extensions they can be proved in the same way. Of vital importance for the decidability of typechecking is the property of strong normalisation of type expressions.

Pragmatics

Although programs and correctness proof are separate objects, we want to be able to construct programs and their correctness proofs together. For this, syntax-directed (or compositional) rules can be used. The programming language provides typing rules that deduce the type of a program from the types of its component parts. In the logic matching proof rules can be derived, that deduce a property of that program from properties of its component parts. With these coupled derivation rules, programs and their correctness proofs can be constructed hand in hand.

Instead of using these compositional rules, properties of programs can also be proved using equalities between programs, i.e. using correctness-preserving transformations. The powerful quantifications that are available make it possible to express and prove such transformation rules inside the formal systems.

Semantics

The semantics of the systems is treated in the second part of the thesis, in the chapters 6, 7 and 8. It is always done using the following three steps:

For each of the programming languages we first give a general model definition, which describes the general structure of a model for the programming language. These general model definitions are extensions of the BMM-environment models given in [BMM90].

Then an instantiation of this general model definition is given. For this, two kinds of models will be used, PER-models and CPO-models. For the programming languages without recursion the more or less standard PER-models are used. For the programming language with recursion a CPO-model is used, in which all datatypes are interpreted as cpos and recursive programs are interpreted as least fixed-points.

Based on the general model definitions for the programming languages, simple models for the associated logics are given. These are so-called proof-irrelevance models, in which propositions are simply interpreted as truth values. These simple models for the logics suffice to prove the consistency of the logics, and of any axioms that are added.

Short description of the chapters

We conclude this introduction with a short description of the individual chapters.

In chapter 2 we give a short introduction to Pure Type Systems (PTSs) and their most important properties. We also define DPTSs, PTSs extended with a definition-mechanism, and give their main properties.

The rest of the thesis is divided in two parts. The first part concerns the syntax and pragmatics of the different systems, the second part the semantics.
In chapter 3 the basic system, the PTS $\lambda\omega_L$, is defined. It is a PTS that comprises a programming language and an associated logic in which properties of programs and datatypes can be expressed and proved. The programming language is $\lambda\omega$, which is the PTS that correspond to Girard's system $F^\omega$ [Gir72]. It is a higher-order extension of the Girard-Reynolds second-order (or polymorphic) lambda calculus. The whole system $\lambda\omega_L$ can be regarded a refinement of the Calculus of Constructions.

In the next two chapters, extensions of the programming language and associated extensions of the programming logic are given.

The first extension, given in chapter 4, is the inclusion of so-called $+$-, $\times$- and $\Sigma$-types. In the programming language these can be used as labelled products and sums - i.e. records and variants - and abstract datatypes. In the logic they can be used for conjunction, disjunction and existential quantification.

The second extension, given in chapter 5, is the extension of the programming language with recursive datatypes and recursive programs. Programs are then no longer guaranteed to terminate. Domain theory is used as the basis for reasoning about recursive programs and non-termination. So, axioms are introduced in the logic to reason about recursive programs in the style of LCF [GMW79]

In the next three chapters, we consider the semantics of the different systems that have been introduced.

Chapter 6 treats the semantics of the basic system introduced in chapter 3. A general model definition for the programming language is given, which describes the general structure of a $\lambda\omega$-model. It is shown that the standard PER-model is indeed an instantiation of this general model definition. For any instantiation of the general model definition, a simple proof irrelevance model suffices for the logic. This means that propositions are interpreted as truth values, and all proofs are identified. This interpretation of the logic can be used to show consistency of the logic and of axioms that are added to the logic, e.g. the axiom for classical logic.

In chapter 7 the general model definition is extended to incorporate the extensions of the programming language given in chapter 4, i.e. the type constructors $+$, $\times$ and $\Sigma$. Again, it is shown that the standard PER-model provides an instantiation of the general model definition, and a proof-irrelevance semantics of the logic is used to prove consistency of the logic and of axioms that have been added

In chapter 8 the general model definition is extended to incorporate the extensions of the programming language given in chapter 5, i.e. recursion. We now give a completely different instantiation of the general model definition, namely a CPO-model, in which datatypes are interpreted as cpos, and the fixed-point operator as the least fixed-point operator on cpos. As before, a proof-irrelevance semantics of the logic is used to prove consistency of the logic and of axioms that are added.

Finally, in chapter 9, we give a comparison with related work, and suggest some directions for further research.
Chapter 2

Pure Type Systems

Pure Type Systems (PTSs) provide a way of describing a large class of type systems in a uniform way. They were introduced by S. Berardi [Ber88] and J. Terlouw [Ter89] as a generalisation of the systems in Barendregt's lambda cube [Bar92]. The notion of PTS is useful for two reasons. Firstly, some meta-theoretical properties can be proved for all PTSs or for large classes of PTSs at the same time. Secondly, many type systems can be described as PTSs, and these compact and very precise descriptions make it possible to compare and classify them. They also make it easy to design a type system for a particular purpose, as will be done in chapter 3.

The "purity" of PTSs lies in the fact that there is only one type constructor, namely the dependent product π (which generalises the function space ->), and one reduction rule, namely β-reduction. As a result, PTSs are very bare type systems. In the course of this thesis we will extend PTSs with more type constructors and associated reduction rules, but the essence of these systems will already be contained in their underlying PTS.

One shortcoming of PTSs is that they do not provide a way to introduce definitions, i.e. abbreviations for terms. Such a facility does not increase the overall expressive power, but it is essential for practical use. Indeed, all implementations of PTSs, such as Coq [Dow91], LEGO [LP92], and CONSTRUCTOR [Hel91], do provide a definition mechanism, even though the formal definitions of the type systems they implement do not. This is in contrast to the AUTOMATH systems [DB80], where the definition mechanism is explicitly considered as part of the formal system.

For this reason DPTSs - extensions of PTSs with a definition mechanism - were introduced in [SP93] [SP94]. For every PTS there is a corresponding DPTS. In some respects, these are the same type system, and depending on the situation it may be preferable to look at one or the other. The PTS provides a more abstract view, which is useful for talking about a system. But for working in a system the definition mechanism provided by the DPTS is needed.

The extension of a PTS with definitions is not as harmless as it may appear at first sight. In particular, it is an open problem whether the extension always preserves the property of strong normalisation. For the PTSs used in this thesis, we do prove that the extension with definition preserves strong normalisation.

In section 2.1, the definition of PTSs and their most important properties are given. In section 2.2, the definition of DPTSs and their most important properties are given. Finally, in section 2.3, the relation between PTSs and DPTSs is discussed.
2.1 PTSs

In this section we define Pure Type Systems and list their most important properties. For a more comprehensive discussion of PTSs we refer to [BH90], [Bar91] or [Bar92].

A PTS is a typed lambda calculus. It can be defined as a 4-tuple consisting of a set of pseudoterminals, a set of pseudontexts, a reduction relation on pseudoterminals, and - most importantly - a typing relation. This typing relation is defined by a set of inference rules for deriving judgements of the form

\[ \Gamma \vdash a : A \]

which is read as "\( a \) has type \( A \) in context \( \Gamma \)" or "\( a \) is an inhabitant of \( A \) in context \( \Gamma \)"

2.1 Definition. A specification of a PTS is a triple \( (S, A, R) \) with

- \( S \) is a set of symbols called the sorts,
- \( A \subseteq S \times S \), a set of axioms of the form \( s : s' \),
- \( R \subseteq S \times S \times S \), a set of rules of the form \( (s_1, s_2, s_3) \).

We write \( \langle s_1, s_2 \rangle \) for a rule \( (s_1, s_2, s_3) \in R \) if \( s_2 = s_3 \). All PTSs mentioned in this thesis will only have rules of the form \( \langle s_1, s_2 \rangle \).

The sorts in \( S \) are the universes of the type system. In specifications given later these may include a sort * for the universe of all types, a sort *s for the universe of all datatypes, or a sort *p for the universe of all propositions. The axioms in \( A \) establish a hierarchy between the universes. The rules in \( R \) control the dependencies between inhabitants of the different universes, by controlling the abstractions and quantifications that are allowed.

The PTS specified by \( S = (S, A, R) \) is denoted by \( \lambda S \). The pseudoterminals of a PTS are defined below. There is just one collection of pseudoterminals, so there is no a priori distinction between terms and types (or other "levels" of expressions). This is an important difference between the definition of a type system as a PTS and a more ad-hoc definition. When a particular PTS is defined, we will generally distinguish different sets of pseudoterminals for the different levels of expressions.

2.2 Definition (Pseudoterminals of a PTS)
The set of pseudoterminals \( \text{T}_\lambda S \) of a PTS \( \lambda S = \lambda (S, A, R) \) is defined by (we usually just write \( T \))

\[ T := \text{Var} \mid S \mid (\text{T}, \text{T}) \mid (\lambda \text{Var} : \text{T}, \text{T}) \mid (\Pi \text{Var} : \text{T}, \text{T}) \]

where \( \text{Var} \) is the set of variables. We assume there are disjoint subsets \( \text{Var}^s \) of \( \text{Var} \) for all \( s \in S \).

Both \( \lambda \) and \( \Pi \) bind variables in \( (\lambda x : A \ b) \) and \( (\Pi \ell x : A \ b) \) occurrences of \( x \) in \( b \) are bound. Free and bound variables are defined as usual. \( \text{FV}(A) \) denotes the set of variables occurring free in a term \( A \). We take the usual " sloppy" approach to bound variables: terms that are equal up to the renaming of bound variables are identified, and we assume that in all expressions the bound variables are distinct from the free variables. We write \( A = B \) if \( A \) and \( B \) are equal up to renaming of bound variables, and \( A[x = B] \) for \( A \) with \( B \) substituted for the free occurrences of \( x \).
2.3 Definition (Pseudocontexts of a PTS)
The set of pseudocontexts $C_{\text{PS}}$ of a PTS $\lambda S = \lambda (S, A, R)$ is defined by (we just write $C$)

- $\epsilon \in C$,
- $\Gamma, x :: A \in C$ if $\Gamma \in C$, $A \in T$, $\tau \in \text{Var}$ is $\Gamma$-fresh and $x \not\in \text{FV}(A)$.

Here $\epsilon$ denotes the empty context, and a variable $x$ is called $\Gamma$-fresh if $x \not\in \{y\} \cup \text{FV}(B)$ for all $y : B$ occurring in $\Gamma$.

The prefix "pseudo" is used because only the pseudoterms and pseudocontexts that are in the typing relation (i.e., that are well-typed) will ultimately be of interest. These pseudoterms and pseudocontexts will be called the terms and the contexts.

2.4 Convention.

- $s, s', s_1, s_2, \ldots$ range over $S$.
- $\tau, \eta, z$ range over $\text{Var}$
- $a, b, \ldots$ and $A, B, \ldots$ range over $T$.
- $\Gamma, \Gamma', \Gamma_1, \ldots$ range over $C$

- The usual conventions for omitting parentheses are used:
  - Application associates to the left, so $a_1 a_2 \ldots a_n$ is $((\ldots ((a_1 a_2) a_3) \ldots) a_n)$
  - The scope of a $\lambda$- or $\Pi$-abstraction extends to the right as far as the first unmatched closing parenthesis. So $(\lambda x. A \cdot b \cdot c)$ is $(\lambda x. A. (b \cdot c))$, and not $((\lambda x. A) \cdot b) \cdot c$.
  - Outermost parentheses may be omitted.

2.5 Definition. The reduction relations $\triangleright_{\beta} \subseteq T \times T$ and $\triangleright_{\eta} \subseteq T \times T - \beta$- and $\eta$-reduction are defined as usual by

$$
(\lambda x : A \cdot b) \triangleright_{\beta} [x = a] \\
(\lambda x : A \cdot b) \triangleright_{\eta} b \quad \text{if } x \not\in \text{FV}(b)
$$

and all the compatibility rules $\triangleright_{\beta}$ and $\triangleright_{\eta}$ are the reflexive and transitive closures of $\triangleright_{\beta}$ and $\triangleright_{\eta}$. $\simeq_{\beta}$ and $\simeq_{\eta}$ are the reflexive, transitive and symmetric closures of $\triangleright_{\beta}$ and $\triangleright_{\eta}$.

In the rest of this chapter $\eta$-reduction does not play a role. We only discuss the theory of PTSs with just $\beta$-reduction. The theory of PTSs with $\beta$ and $\eta$-reduction, treated in [Gen93], is considerably more complicated. This is because unlike $\beta$-reduction, $\eta$-reduction is not Church-Rosser on the set of pseudoterms.

2.6 Theorem (CR$_{\beta}$) $\beta$-reduction is Church-Rosser (or confluent), i.e.

$$
\forall A, B \in T. [A \simeq_{\beta} B \Rightarrow \exists C \in T. [A \triangleright_{\beta} C \land B \triangleright_{\beta} C]]
$$
2.7 Definition (Typing relation of a PTS)
The typing relation $\vdash_{\lambda S} \subseteq \mathcal{C} \times \mathcal{T} \times \mathcal{T}$ of a PTS $\lambda S = \lambda(S, A, R)$ is the smallest relation closed under the following type inference rules (we just write $\vdash$ if it is clear which $\lambda S$ is meant)

1. **(axiom)** $\varepsilon \vdash s_1 : s_2$ if $s_1, s_2 \in A$

2. **(var)** $\Gamma \vdash A : s$ if $x \in \text{Var}^\mathcal{A}$

3. **(weaken)** $\Gamma, x : A \vdash b : B \quad \Gamma \vdash A : s$

4. **(Πform)** $\Gamma \vdash A : s_1, \Gamma, x : A \vdash b : s_2 \quad \Gamma \vdash (\Pi x. A. B) : s_3$

5. **(Πintro)** $\Gamma, x : A \vdash b : B \quad \Gamma \vdash (\Pi x. A. B) : s \quad \Gamma \vdash (\lambda x. A) : (\Pi x. A. B)$

6. **(Πelim)** $\Gamma \vdash b : (\Pi x. A. B) \quad \Gamma \vdash a : A \quad \Gamma \vdash b \alpha \cdot \tilde{B}[x = a]$

7. **(βconv)** $\Gamma \vdash b : B \quad \Gamma \vdash B' : s \quad B \simeq B' \quad \Gamma \vdash b : B'$

where $s$ ranges over sorts, i.e., $s \in S$. Note that by the definition of the set of pseudocontexts $C$ the variable $x$ is $\Gamma$-fresh in the rules *(var)*, *(weaken)*, *(Πform)* and *(Πintro)*.

$\Gamma \vdash A : B : C$ is short for $\Gamma \vdash A : B$ and $\Gamma \vdash B : C \quad \blacksquare$

If $x$ does not occur free in $B$, $(\Pi x. A. B)$ is written as $A \rightarrow B$. It is easy to see that the following rules are derivable

1. **(→ form)** $\Gamma \vdash A : s_1, \Gamma \vdash B : s_2 \quad \Gamma \vdash A \rightarrow B : s_3$

2. **(→ intro)** $\Gamma, x : A \vdash b : B \quad \Gamma \vdash A \rightarrow B : s \quad \Gamma \vdash (\lambda x. A) : (\Pi x. A. B)$

3. **(→ elim)** $\Gamma \vdash b : A \rightarrow B \quad \Gamma \vdash a : A \quad \Gamma \vdash b \alpha \cdot \tilde{B}[x = a]$

In a given PTS there may be rules $(s_1, s_2, s_3) \in R$ for which the rule *(Πform)* is more general than needed, and just the rule *(→ form)* would suffice.

As already mentioned, the typing relation selects the terms and contexts from the pseudo-terms and pseudo-contexts.

2.8 Definition (Terms, contexts, well-typedness, $\vdash_{\lambda S} \subseteq A$, $\Gamma \vdash a : A$).

1. A pseudo-term $A$ is a $(\lambda S)$-term if $\Gamma \vdash A : B$ or $\Gamma \vdash B : A$ for some $\Gamma$ and $B$.

2. A pseudo-context $\Gamma$ is a $(\lambda S)$-context if $\Gamma \vdash A : B$ for some $A$ and $B$.

3. A term $A$ is well-typed in context $\Gamma$ if $\Gamma \vdash A : B$ or $\Gamma \vdash B : A$ for some $B \in \mathcal{T}$.

4. A term $A$ is inhabitated in context $\Gamma$ if $\Gamma \vdash a : A$ for some $a \in \mathcal{T}$. 

2.1. PTSs

5. A term \( a \) is \textit{typable} in context \( \Gamma \) - written \( \Gamma \vdash a : \_ \) - if \( \Gamma \vdash a \cdot A \) for some \( A \in T \). □

So a pseudoterm is a term iff it is well-typed in some context, and a term is well-typed in some context iff it is typable or inhabited in that context. There can be well-typed terms that are not typable, namely sorts which are at the highest level in the hierarchy given by the axioms \( A \), i.e. those \( s \in S \) for which \( \neg(\exists s' \in S. (s : s') \in A) \). The distinction between well-typed and typable only plays a role in some technical proofs about PTSs.

We will sometimes be interested in the sub-context containing only the declarations of variables that belong to certain sorts.

2.9 DEFINITION. For a context \( \Gamma \) and \( s_1, \ldots , s_n \in S \), the pseudoterm \( \Gamma^{s_1 \ldots s_n} \) is defined by

\[
\varepsilon^{s_1 \ldots s_n} \equiv \varepsilon
\]

\[
(\Gamma, x : A)^{s_1 \ldots s_n} \equiv \left\{ \begin{array}{ll}
\Gamma^{s_1 \ldots s_n} & \text{if } x \in \text{Var}^{s_i} \text{ for some } i \in \{1, \ldots , n\} \\
\Gamma^{s_1 \ldots s_n} & \text{otherwise}
\end{array} \right.
\]

Properties of PTSs

Below we list some of the basic properties of PTSs. Proofs of these properties can be found in [GN91] or [Bar92].

The first two lemmas state that the context behaves as expected.

2.10 LEMMA (Start). Let \( \Gamma \) be a context. Then

1. If \( s : s' \in A \), then \( \Gamma \vdash s : s' \).
2. If \( x : A \in \Gamma \), then \( \Gamma \vdash x : A \). □

2.11 LEMMA (Weakening). If \( \Gamma \) is a context and \( \Gamma' \vdash a : A \) for some \( \Gamma' \subseteq \Gamma \) - i.e. \( x : B \in \Gamma \) for all \( x : B \in \Gamma' \), then \( \Gamma \vdash a : A \). □

The next lemma is used to prove properties by induction on the structure of terms.

2.12 LEMMA (Generation)

1. If \( \Gamma \vdash s \cdot C \) then \( C \equiv_s s' \) for some \( (s : s') \in A \).
2. If \( \Gamma \vdash x : C \) then \( C \equiv_s A \) for some \( x : A \in \Gamma \).
3. If \( \Gamma \vdash (\Pi x : A \cdot B) : C \) then \( C \equiv_s s_3 \), \( \Gamma \vdash A \cdot s_1 \), and \( \Gamma, x : A \vdash B : s_2 \) for some \( (s_1, s_2, s_3) \in R \).
4. If \( \Gamma \vdash (\lambda x : A \cdot b) : C \) then \( C \equiv_s (\Pi x : A \cdot B) \), \( \Gamma \vdash A \cdot s_1 \), \( \Gamma, x : A \vdash B : s_2 \) and \( \Gamma, x : A \vdash B : s_2 \) for some \( B \in T \) and \( (s_1, s_2, s_3) \in R \).
5. If \( \Gamma \vdash b : C \) then \( C \equiv_s B[x := a] \), \( \Gamma \vdash b : (\Pi x : A \cdot B) \) and \( \Gamma \vdash a : A \) for some \( x \in \text{Var} \) and \( A, B \in T \). □

If a term is inhabited then it is a sort or it is typable with a sort.
2.13 LEMMA (Correctness of Types) If $\Gamma \vdash a : A$ then $A \in S$ or $\Gamma \vdash A : s$ for some $s \in S$.  

The collection of inhabitants of a type is closed under reduction:

2.14 LEMMA (Subject Reduction : $SR_\beta$) If $\Gamma \vdash b : B$ and $b \triangleright b'$ then $\Gamma \vdash b' : B$.  

It is possible to restrict the places in a type derivation where the rule (weaken) can be applied.

2.15 LEMMA (Restricted Weakening). If $\Gamma \vdash a : A$, then there is a derivation of this in which all applications of the rule (weaken) are of the form

$$
\frac{\Gamma \vdash b : B \quad \Gamma \vdash A : s}{\Gamma, x \vdash A \vdash b \quad B} \quad x \in \text{Var}^* \text{ and } b \in S \cup \text{Var},
$$

i.e. (weaken) is only used if the subject $b$ is a sort or a variable.

**Proof:** See [Gen93].

This lemma will be useful later, when interpretations are defined by induction on type derivations, as it allows us to restrict the possible form of derivations.

Most - if not all - PTSs that are of interest are functional PTSs.

2.16 DEFINITION. A (specification of a) PTS is called functional if

$$
(s : s') \in A \land (s' : s^\prime) \in A \Rightarrow s' = s^\prime
$$

$$
(s_1, s_2, s_3) \in R \land (s_1, s_2, s_3) \in R \Rightarrow s_3 = s_3
$$

The distinguishing property of the functional PTSs is that the type of a term is unique up to $\beta$-conversion.

2.17 LEMMA (Uniqueness of Types - $UT_\beta$ - for functional PTS).

If $\Gamma \vdash b : B$ and $\Gamma \vdash b : B'$ then $B \equiv_\beta B'$.  

**Proof** See [GN91] or [Bar92].

All PTSs mentioned in this thesis are functional. By UT we can speak of the type of a term, if we only care about its type modulo $\beta$-conversion.

2.18 DEFINITION. A PTS is $\beta$-strongly normalising - written $SN_\beta$ - if all its terms are, i.e. if $\Gamma \vdash a : A$ implies that $a$ and $A$ are $\beta$-strongly normalising, which means that all $\beta$-reduction sequences starting in $a$ and $A$ terminate.

Together, CR and SN imply that convertibility of types is decidable, which is essential for decidability of type checking. Not all PTSs are SN, and SN cannot be proved for large classes of PTSs, unlike CR, SR and UT. For SN we have to consider particular PTSs.
2.19 Definition $(\lambda \rightarrow, \lambda \alpha, \lambda \omega, \lambda C)$.

1. $\lambda \rightarrow$ is the PTS specified by
   \[ S = \{*, \Box\}, \quad A = \{*: \Box\}, \quad R = \{(*, *)\} \]
   $\lambda \rightarrow$ is Church's simply typed lambda calculus, introduced in [Chu40].

2. $\lambda \alpha$ is the PTS specified by
   \[ S = \{*, \Box\}, \quad A = \{*, \Box\}, \quad R = \{(*, *), (\Box, *)\} \]
   $\lambda \alpha$ is the second order or polymorphic typed lambda calculus, also known as system $F$, introduced in [Gir72] and [Rey74].

3. $\lambda \omega$ is the PTS specified by
   \[ S = \{*, \Box\}, \quad A = \{*, \Box\}, \quad R = \{(*, *), (\Box, *), (\Box, \Box)\} \]
   $\lambda \omega$ is the higher order typed lambda calculus, and is essentially the system $F^\omega$, introduced in [Gir72].

4. $\lambda C$ is the PTS specified by
   \[ S = \{*, \Box\}, \quad A = \{*, \Box\}, \quad R = S^2 \]
   $\lambda C$ is the Calculus of Constructions, introduced in [Ch88].

The relation between the systems is obvious from their specifications: $\lambda \rightarrow$ is a subsystem of $\lambda \alpha$, $\lambda \alpha$ is a subsystem of $\lambda \omega$, and $\lambda \omega$ is a subsystem of $\lambda C$. A disadvantage of these compact specifications is that some work is needed to get some idea of what these type systems are, e.g. what types can be formed and which abstractions are allowed. In chapter 3 the system $\lambda \omega$ and a refinement of the system $\lambda C$ will be discussed in depth.

The PTSs defined above are all strongly normalising, because $\lambda C$ – the largest one – is.

2.20 Theorem $\lambda C$ is $SN_\beta$.

This was first proved by Coquand in [Coq85]. An alternative proof is given in [GN91].

The type checking problem - $\Gamma \vdash a A$ - is the problem of deciding whether $\Gamma \vdash a : A$ is derivable for given $\Gamma$, $a$ and $A$. The type inference problem - $\Gamma \vdash a : \ldots$ - is the problem of deciding if a term $a$ is typable in a context $\Gamma$ and, if so, computing its type. In [BJ93] it is proved that type checking is decidable and type inference is computable for all strongly normalising PTSs with a finite set of sorts. These proofs only provide algorithms that are far too inefficient for practical use. Efficient algorithms for some classes of PTSs can be found in [BJMP93] and [Pol93].
2.2 DPTSs

DPTSs, introduced in [SP94], are PTSs extended with a definition mechanism. In a DPTS, terms and contexts can contain definitions of the form \( x = a : A \). A definition \( x = a : A \) introduces \( x \) as an abbreviation for the term \( a \) of type \( A \). A new reduction relation, called \( \delta \)-reduction, is defined to capture the notion of unfolding definitions.

Like a PTS, a DPTS is a 4-tuple consisting of a set of pseudoterms, a set of pseudocontexts, a reduction relation, and a typing relation. And like a PTS, a DPTS is specified by a triple \( S = (S, A, R) \). The DPTS specified by \( S \) is denoted \( \lambda S \).

2.21 DEFINITION (Pseudoterms of a DPTS)

The set of pseudoterms \( T_{\lambda S} \) of a DPTS \( \lambda S_6 = \lambda (S, A, R)_6 \) is defined by (we just write \( T \))

\[
T := \text{Var} \mid S \mid (TT) \mid (\lambda T \cdot T) \mid (\Pi T \cdot T) \mid (\text{Var} = T \cdot T \text{ in } T)
\]

Like \( \lambda \) and \( \Pi \), \( a \) binds a variable in \((x = a : A \text{ in } b)\) occurrences of \( x \) in \( b \) are bound. The notions of free variables, substitution, and \( \lambda \)- and \( \Pi \)-reduction are extended to this larger collection of pseudoterms in the obvious way. For definitions the same conventions for omitting parentheses apply as for \( \lambda \) and \( \Pi \)-abstractions. So \((x = a : A \text{ in } (b : c)) \Rightarrow (x = a : A \text{ in } (b : c))\), and not \(((x = a : A \text{ in } b) : c)\)

2.22 DEFINITION (Pseudocontexts of a DPTS)

The set of pseudocontexts \( C_{\lambda S} \) of a DPTS \( \lambda S_6 = \lambda (S, A, R)_6 \) is defined by (we usually just write \( C \))

- \( \varepsilon \in C \)
- \( \Gamma, x : A \in C \) if \( \Gamma \in C \), \( A \in T \), and \( x \in \text{Var} \) is \( \Gamma \)-fresh and \( x \not\in \text{FV}(A) \)
- \( I, \lambda x : A \in C \) if \( I \in C \), \( x \in \text{Var} \) is \( I \)-fresh and \( x \not\in \text{FV}(a) \cup \text{FV}(A) \)

Here a variable \( x \) is called \( \Gamma \)-fresh if \( \Gamma \not\in \{y\} \cup \text{FV}(B) \) for all \( y : B \) occurring in \( \Gamma \) and \( x \not\in \{y\} \cup \text{FV}(b) \cup \text{FV}(B) \) for all \( y : B \) occurring in \( \Gamma \).

Definitions in pseudocontexts, e.g. \( I, \lambda x : a : A \), \( G \), are called global definitions. Definitions in pseudoterms, e.g. \( (x = a : A \text{ in } b) \), are called local definitions, sometimes also called let-expressions.

2.23 DEFINITION (\( \delta \)-reduction)

The relation \( \vdash \subseteq C \times T \times T \) – called \( \delta \)-reduction – is the smallest relation such that

- \( \Gamma_1, x : a : A \vdash \Gamma_2 \vdash x \xrightarrow{\delta} a \)
- \( \Gamma \vdash (x = a : A \text{ in } b) \xrightarrow{\delta} b \) if \( x \not\in \text{FV}(b) \)

and that is closed under the following compatibility rules

- if \( \Gamma, x : a \vdash b \xrightarrow{\delta} b' \) then \( \Gamma \vdash (x = a : A \text{ in } b) \xrightarrow{\delta} (x = a : A \text{ in } b') \)
- if \( \Gamma, x : A \vdash b \xrightarrow{\delta} b' \) then \( \Gamma \vdash (\Pi x : A \cdot b) \xrightarrow{\delta} (\Pi x : A \cdot b') \)

and \( \Gamma \vdash (\lambda x : A \cdot b) \xrightarrow{\delta} (\lambda x : A \cdot b') \)
• if $\Gamma \vdash a \triangleright_{\delta} a'$ then
  \[ \Gamma \vdash (x = a : A \text{ in } b) \triangleright_{\delta} (x = a' : A \text{ in } b), \]
  \[ \Gamma \vdash (x = A : a \text{ in } b) \triangleright_{\delta} (x = A : a' \text{ in } b), \]
  \[ \Gamma \vdash (a \text{ in } b) \triangleright_{\delta} (a' \text{ in } b), \]
  \[ \Gamma \vdash (b : a) \triangleright_{\delta} (b : a'), \]
  \[ \Gamma \vdash (\Pi x : a \text{ in } b) \triangleright_{\delta} (\Pi x : a' \text{ in } b), \]
  and
  \[ \Gamma \vdash (\lambda x : a \text{ in } b) \triangleright_{\delta} (\lambda x : a' \text{ in } b). \]

We write $\Gamma \vdash a \triangleright_{\beta} b$ if $\Gamma \vdash a \triangleright_{\beta} b$ or $a \triangleright_{\beta} b$. For $\rho \in \{\delta, \beta\}$, $\Gamma \vdash \rho^- \sim$ is the reflexive and transitive closure of $\Gamma \vdash - \rho -$, and $\Gamma \vdash \rho^- \sim$ is the reflexive, transitive and symmetric closure of $\Gamma \vdash - \rho -$.  

So, for example, $(x = a : A \text{ in } b) \triangleright_{\delta} (x = a : A \text{ in } b[x := a]) \triangleright_{\delta} b[x := a]$. The number of steps needed to $\delta$-reduce $(x = a : A \text{ in } b)$ to $(x = a : A \text{ in } b[x := a])$ is exactly the number of occurrences of $x$ in $b$.

In a $\delta$-reduction
\[ \Gamma_1, x = a : A, \Gamma_2 \vdash x \triangleright_{\delta} a \]

none of the free variables of $a$ can be captured by definitions or declarations in $\Gamma_2$. This is because if $\Gamma_1, x = a : A, \Gamma_2 \in C$, then by the definition of $C$ there are no definitions $y = b : B$ or declarations $y : B$ in $\Gamma_2$ for which $y \in \text{FV}(a)$.

Expanding all definitions in a $\lambda S_6$-pseudoterm produces a $\lambda S_6$-pseudoterm:

2 24 DEFINITION ($\delta n f$). For a pseudoterm $a \in T_{\lambda S_6}$ and a pseudocontext $\Gamma \in C_{\lambda S_6}$, the pseudoterm $\delta n f_{\Gamma}(a) \in T_{\lambda S}$ is defined as follows:

\[
\delta n f_{\Gamma}(x) & \equiv \begin{cases} 
\delta n f_{\Gamma_1}(a) & \text{if } \Gamma \equiv \Gamma_1, x = a : A, \Gamma_2 \\
x & \text{otherwise}
\end{cases} \\
\delta n f_{\Gamma}(s) & \equiv s \\
\delta n f_{\Gamma}(a \text{ in } b) & \equiv \delta n f_{\Gamma}(a) \delta n f_{\Gamma}(b) \\
\delta n f_{\Gamma}(\lambda x : A \text{ in } b) & \equiv \lambda x. \delta n f_{\Gamma}(A), \delta n f_{\Gamma,x : A}(b) \\
\delta n f_{\Gamma}(\Pi x : A) \text{ in } B & \equiv \Pi x. \delta n f_{\Gamma}(A) \delta n f_{\Gamma,x : A}(B) \\
\delta n f_{\Gamma}(z = a : A \text{ in } b) & \equiv \delta n f_{\Gamma,z = a : A}(b)
\]

The definition of $\delta n f_{\Gamma}(a)$ is by induction on the number of characters in $a$ plus the number of characters in $\Gamma$ (not counting brackets).

It is not difficult to show that.

2 25 LEMMA. $\delta n f_{\Gamma}(a)$ is the unique $\delta$-normal form of $a$ in $\Gamma$

PROOF. (Sketch) First we prove that $\delta n f_{\Gamma}(a)$ is a $\delta$-normal form of $a$ in $\Gamma$, by proving that $\Gamma \vdash a \triangleright_{\delta} \delta n f_{\Gamma}(a)$ and that $\delta n f_{\Gamma}(a)$ is in $\delta$-normal form. It then follows from $\Gamma \vdash a \triangleright_{\delta} a' \Rightarrow \delta n f_{\Gamma}(a) \equiv \delta n f_{\Gamma}(a')$ that $\delta n f_{\Gamma}(a)$ is the unique $\delta$-normal form of $a$ in $\Gamma$.  

From the existence of unique $\delta$-normal forms it follows that $\delta$-reduction is Church-Rosser and weakly normalising. In fact, $\delta$-reduction has even stronger properties, as given by the next lemma.
2.26 Lemma.

1. **$\text{CR}_{\beta\delta}$**: $\beta\delta$-reduction is Church-Rosser, i.e.
   \[\forall \Gamma \in \mathcal{C}, A, B \in T, \, [\Gamma \vdash A \equiv_{\beta\delta} B \Rightarrow \exists C \in T, \, [\Gamma \vdash A \Rightarrow_{\beta\delta} C \land \Gamma \vdash B \Rightarrow_{\beta\delta} C]\]

2. **$\text{SN}_{\delta}$**: $\delta$-reduction is strongly normalising

**Proof.** (Sketch)

1. To prove $\text{CR}_{\beta\delta}$ we use the fact that unique $\delta$-normal forms exist.

Suppose $\Gamma \vdash a \Rightarrow_{\delta\beta} a_1$ and $\Gamma' \vdash a \Rightarrow_{\delta\beta} a_2$. Then $a, a_1$ and $a_2$ reduce to their $\delta$-normal forms $\text{dnf}_\Gamma(a), \text{dnf}_\Gamma(a_1)$ and $\text{dnf}_\Gamma(a_2)$, respectively. By the following properties:

   (i) if $\Gamma \vdash a \Rightarrow_{\delta\beta} a'$ then $\text{dnf}_\Gamma(a) \equiv \text{dnf}_\Gamma(a')$

   (ii) if $\Gamma \vdash a \Rightarrow_{\delta\beta} a'$ then $\text{dnf}_\Gamma(a) \Rightarrow_{\delta\beta} \text{dnf}_\Gamma(a')$

it follows that $\Gamma \vdash \text{dnf}_\Gamma(a) \Rightarrow_{\delta\beta} \text{dnf}_\Gamma(a_1)$ and $\Gamma \vdash \text{dnf}_\Gamma(a) \Rightarrow_{\delta\beta} \text{dnf}_\Gamma(a_2)$. Finally, by $\text{CR}_{\beta\delta}$ there then is a common $\beta\delta$-reduct of $\text{dnf}_\Gamma(a_1)$ and $\text{dnf}_\Gamma(a_2)$. The whole proof is best illustrated by the following diagram:

![Diagram](image)

2. **$\text{SN}_{\delta}$** is proved by showing that $\text{weight}_\Gamma(a) \in \mathbb{N}$, defined below, decreases with $\delta$-reduction

\[
\begin{align*}
\text{weight}_\Gamma(x) &= \begin{cases} 
\text{weight}_\Gamma(x) + 1 & \text{if } \Gamma \equiv \Gamma_1, x \in A, \Gamma_2 \\
0 & \text{otherwise}
\end{cases} \\
\text{weight}_\Gamma(s) &= 0 \quad \text{if } s \in \mathcal{S} \\
\text{weight}_\Gamma(x = u \ A \text{ in } b) &= \text{weight}_\Gamma(a) + \text{weight}_\Gamma(A) + \text{weight}_\Gamma(x = a \cdot b) + 1 \\
\text{weight}_\Gamma(x \cdot A \cdot b) &= \text{weight}_\Gamma(a) + \text{weight}_\Gamma(b) \\
\text{weight}_\Gamma(\lambda x \cdot A \cdot b) &= \text{weight}_\Gamma(x \cdot A \cdot b) + \text{weight}_\Gamma(A) \\
\text{weight}_\Gamma(\Pi x \cdot A \cdot B) &= \text{weight}_\Gamma(x \cdot A \cdot B) + \text{weight}_\Gamma(A)
\end{align*}
\]

Note that $\delta$-reduction is strongly normalising on the pseudoterms. This in contrast to $\beta$-reduction, which is not strongly normalising on the pseudoterms since for instance $(\lambda x \cdot y \cdot x)(\lambda x \cdot y \cdot x)$ is a pseudoterm $\cdot$, but can only be strongly normalising on a subset of the pseudoterms (e.g. the $\lambda C$-terms).
2.27 **DEFINITION** (Typing relation of a DPTS).

The typing relation \( \Gamma \vdash \lambda S \subseteq C \times T \times T \) of a DPTS \( \lambda S = \lambda(S,A,R) \) is the smallest relation closed under the type inference rules listed in definition 2.7 plus the following rules

\[
\begin{align*}
(\delta_{\text{var}}) & \quad \Gamma, x = a : A \vdash x : A \\
(\delta_{\text{weaken}}) & \quad \Gamma, x = a : A \vdash b : B \\
(\delta_{\text{form}}) & \quad \Gamma, x = a : A \vdash b \cdot s \\
(\delta_{\text{intro}}) & \quad \Gamma, x = a : A \vdash b \cdot (x = a : A \text{ in } B) \cdot s \\
(\delta_{\text{conv}}) & \quad \Gamma \vdash b : B \quad \Gamma \vdash B' : s \\
\end{align*}
\]

where \( s \) ranges over sorts, i.e., \( s \in S \).

The \((\lambda S_{\delta})\)-terms, the \((\lambda S_{\delta})\)-contexts and the notions of being well-typed, typable and inhabited in a context are defined for the DPTSs as for PTSs (see definition 2.8).

**Properties of DPTSs**

It is not difficult to show that most the properties that hold for arbitrary PTSs also hold for DPTSs. Proofs of the following properties can be found in [SP93].

2.28 **LEMMA** (Start). Let \( \Gamma \) be a context. Then

1. If \( s : s' \in A \), then \( \Gamma \vdash s \iff s' \)

2. If \( x : A \in \Gamma \), then \( \Gamma \vdash x : A \).

3. If \( x = a : A \in \Gamma \) then \( \Gamma \vdash x : A \) (and, by \( \text{SR}_S \), also \( \Gamma \vdash a : A \))

2.29 **LEMMA** (Weakening).

If \( \Gamma \) is a context and \( \Gamma' \vdash a : A \) for some \( \Gamma' \subseteq \Gamma \), then \( \Gamma \vdash a : A \)

2.30 **LEMMA** (Correctness of Types).

If \( \Gamma \vdash a : A \) then \( A \in S \) or \( \Gamma \vdash A \iff s \) for some \( s \in S \).

2.31 **LEMMA** (Subject Reduction \( \text{SR}_S \)).

If \( \Gamma \vdash b : B \) and \( \Gamma \vdash b \gg_{S_b} b' \) then \( \Gamma \vdash b' : B \).

Like a PTS, a DPTS is called functional if its specification is functional (see definition 2.16)

2.32 **LEMMA** (Uniqueness of Types - UT\(_{S_b} \) - for functional DPTS).

For functional DPTS if \( \Gamma \vdash b : B \) and \( \Gamma \vdash b : B' \) then \( \Gamma \vdash B \equiv_{S_b} B' \).
2.33 Definition. A DPTS is $\beta\delta$-strongly normalising if all its terms are, i.e. if $\Gamma \vdash a :: A$ implies that $a$ and $A$ are $\beta\delta$-strongly normalising in context $\Gamma$.

Whether extending a PTS with definitions preserves strong normalisation, i.e. whether

$$\lambda S \text{ is } SN_\beta \Rightarrow \lambda S_5 \text{ is } SN_{\beta\delta}$$

is an open problem. Here the local definitions, i.e. definitions in terms (as opposed to the definitions in contexts), are the main complication. In [SP93] $SN_{\beta\delta}$ is proved for many DPTSs, including $\lambda C_\delta$, the Calculus of Constructions extended with definitions. Here we just give a sketch of the proof.

2.34 Theorem. $\lambda C_\delta$ is $SN_{\beta\delta}$

Proof. (Sketch) This is proved by showing there is a function which maps an infinite $\beta\delta$-reduction sequence in $\lambda C_\delta$ to an infinite $\beta$-reduction sequence in Luo's extended Calculus of Constructions, the system ECC. Strong normalisation of ECC is proved in [Luo89].

The functions $[-] \in T_{\lambda S_5} \times C_{\lambda S_5} \rightarrow T_{\lambda S}$ and $[-] \in C_{\lambda S_5} \rightarrow C_{\lambda S}$ are defined as follows:

$$
\begin{align*}
\{x\} & = \begin{cases} \{a\}_{\Gamma_1} & \text{if } \Gamma_1 \equiv \Gamma_2, x = a :: A, \Gamma_2 \\
\tau & \text{otherwise} \end{cases} \\
\{a\} & = s \text{ if } s \in S \\
\{a, b\} & = \{a\} \{b\} \\
\{\lambda x. A, b\} & = \lambda x \{A\} \{b\} \{x\} \\
\Pi x. A, B & = \Pi x \{A\} \{B\} \\
\{z = a :: A \text{ in } b\} & = \{\lambda x. A\} \{b\} \{z = a :: A\} \\
\{e\} & = e \\
\{\Gamma, x :: A\} & = \{\Gamma\}, x :: \{A\} \\
\{\Gamma, x = a :: A\} & = \{\Gamma\}, x :: \{A\} \\
\end{align*}
$$

The only difference between $[-]$ and $\delta S_5[-]$ is in the clause for terms of the form $x = a :: A \text{ in } b$. This difference is crucial for property (i) below.

For this mapping we prove the following properties.

(i) If $a \beta\delta b$ then $\{a\} \beta \beta \{b\}$ for all $\Gamma$, where $\beta \beta$ is the transitive closure of $\beta\delta$.

(ii) If $\Gamma \vdash a \beta\delta b$ then $\{a\} \beta \\overrightarrow{\beta} \{b\}$, where $\overrightarrow{\beta}$ is the reflexive closure of $\beta\delta$.

(iii) If $\Gamma \vdash a :: A$ in $\lambda C_\delta$ then $\{\Gamma\} \beta \{a\} \{A\}$ in ECC.

It follows from $SN_\delta$ that any infinite $\beta\delta$-reduction sequence has an infinite number of $\beta$-steps. So, by (i) and (ii), $[-]$ maps an infinite $\beta\delta$-reduction sequence to an infinite $\beta$-reduction sequence. By (iii), $[-]$ maps $\lambda C_\delta$-terms to ECC-terms. $SN_{\beta\delta}$ of $\lambda C_\delta$ then follows from $SN_\delta$ of ECC.
2.3 Relation between PTSs and DPTSs

Apart from the question whether the DPTS \( \lambda S_9 \) has all the meta-theoretical properties that the PTS \( \lambda S \) has, it is important to understand the relationship between the two systems. In other words, what is the relation between statements of the form \( \Gamma \vdash a : A \), \( \Gamma \vdash a : \_ \) or \( \Gamma \vdash \_ : A \) that hold in \( \lambda S \) and \( \lambda S_9 \)? To answer these questions, the definition of \( \delta \)-normal form is extended to contexts.

2.35 Definition. The \( \delta \)-normal form \( \delta \text{nf}(\Gamma) \in C_{\lambda S} \) of a pseudocontext \( \Gamma \in C_{\lambda S_9} \) is defined as follows

\[
\begin{align*}
\delta \text{nf}(\varepsilon) & \equiv \varepsilon \\
\delta \text{nf}(\Gamma, x : A) & \equiv \delta \text{nf}(\Gamma), x : \delta \text{nf}(A) \\
\delta \text{nf}(\Gamma, x = a : A) & \equiv \delta \text{nf}(\Gamma)
\end{align*}
\]

Definitions can be eliminated in \( \lambda S_9 \)-type derivations to produce \( \lambda S \)-type derivations:

2.36 Theorem (Elimination of definitions).
If \( \Gamma \vdash_{\lambda S_9} a : A \) then \( \delta \text{nf}(\Gamma) \vdash_{\lambda S} \delta \text{nf}(a) : \delta \text{nf}(A) \).

Proof. Straightforward induction on the derivation of \( \Gamma \vdash_{\lambda S_9} a : A \) \( \Box \)

This means that introducing definitions does not increase the expressive power of the system. An immediate consequence is that the extension of a PTS with definitions is conservative. In fact, there are three possible notions of conservativity. Apart from conservativity for statements of the form \( \Gamma \vdash a : A \), we also have conservativity for statements of the form \( \Gamma \vdash a : \_ \) or \( \Gamma \vdash \_ : A \), as defined in definition 2.8.

2.37 Corollary (Conservativity of \( \lambda S_9 \) over \( \lambda S \)).
Let \( \Gamma \) be a \( \lambda S \)-context and \( a \) and \( A \) be \( \lambda S \)-terms. Then

1. \( \Gamma \vdash_{\lambda S_9} a : A \iff \Gamma \vdash_{\lambda S} a : A \).
2. \( \Gamma \vdash_{\lambda S_9} a : \_ \iff \Gamma \vdash_{\lambda S} a : \_ \).
3. \( \Gamma \vdash_{\lambda S_9} \_ : A \iff \Gamma \vdash_{\lambda S} \_ : A \) \( \Box \)

Part 3 of this corollary is the usual notion of conservativity if we think of types as propositions and their inhabitants as proofs. It states that a \( \lambda S \)-term \( A \) is inhabited – i.e. provable – in a \( \lambda S \)-context \( \Gamma \) in \( \lambda S_9 \) iff \( A \) is inhabited in \( \Gamma \) in \( \lambda S \).

For functional systems, there is even a stronger relation between \( \lambda S \) and \( \lambda S_9 \). Theorem 2.36 says that, modulo \( \delta \)-conversion, a \( \lambda S_9 \)-term does not have more types or inhabitants in \( \lambda S_9 \) than its \( \delta \)-normal form has in \( \lambda S \). The following theorem says that, modulo \( \delta \)-conversion, a \( \lambda S_9 \)-term does not have fewer types or inhabitants in \( \lambda S_9 \) than its \( \delta \)-normal form has in \( \lambda S \), provided \( S \) is functional.

2.38 Theorem (Introduction of definitions).
Let \( S \) be a functional specification, and let \( a \) and \( A \) be well-typed in context \( \Gamma \) in \( \lambda S_9 \) (and so \( \Gamma \) is a \( \lambda S_9 \)-context).

If \( \delta \text{nf}(\Gamma) \vdash_{\lambda S} \delta \text{nf}(a) : \delta \text{nf}(A) \) then \( \Gamma \vdash_{\lambda S_9} a : A \).

(In example 2.40 it is shown why the restriction to functional systems is needed.)
PROOF. First we show that the rule

\[
\frac{\Gamma \vdash b : B \quad \Gamma \vdash B \triangleright_s B'}{\Gamma \vdash b : B'}
\]

is admissible in $\lambda S_\delta$

Suppose $\Gamma \vdash b : B$ and $\Gamma \vdash B \triangleright_s B'$ To prove $\Gamma \vdash b : B'$ we only have to prove that $\Gamma \vdash B' : s$ for some sort $s$, because we have the rule ($\beta\delta$conv). By correctness of types (2.30) it follows from $\Gamma \vdash b : B$ that $\Gamma \vdash B \cong_B B'$, and so $B \notin S$. By $\text{SR}_{\gamma\delta}$ it then follows that $\Gamma \vdash B' : s$.

Then we show that the rule

\[
\frac{\Gamma \vdash b : B \quad \Gamma \vdash B \cong_{\gamma\delta} B' \quad B' \text{ is well-typed in } \Gamma}{\Gamma \vdash b : B'}
\]

is admissible in $\lambda S_\delta$

Suppose $\Gamma \vdash b : B$, $\Gamma \vdash B \cong_{\gamma\delta} B'$ and that $B'$ is well-typed in $\Gamma$. Again, it suffices to prove that $\Gamma \vdash B' : s$ for some sort $s$. We distinguish two cases:

- Case 1: $\Gamma \vdash B : C$. $\Gamma \vdash b : B$, so by correctness of types we can distinguish two cases:
  - Case 2.1: $\Gamma \vdash B : s$ By $\text{SR}_{\gamma\delta}$ the common reduct of $B$ and $B'$ has both type $s$ and type $C$, so by UT$_{\gamma\delta}$ $\Gamma \vdash C \cong_{\gamma\delta} s$. But then $\Gamma \vdash C \triangleright_{\gamma\delta} s$, and by the rule ($\beta\delta$RED) it follows from $\Gamma \vdash B' : C$ that $\Gamma \vdash B' : s$
  - Case 2.2: $B \equiv s' \in S$. Then $\Gamma \vdash B \triangleright_{\gamma\delta} s'$, so by $\text{SR}_{\gamma\delta}$ $\Gamma \vdash s' : C$. Thus means that there is some $s' \in S$ such that $\Gamma \vdash C \cong_{\gamma\delta} s$. By the rule ($\beta\delta$RED) it follows from $\Gamma \vdash B' : C$ that $\Gamma \vdash B' : s$.

We are now ready to prove the theorem. Suppose that $a$ and $A$ are well-typed in context $\Gamma$ in $\lambda S_\delta$ and $\text{dnf}(\Gamma) \vdash_{\lambda S_\delta} \text{dnf}_f(a) \cdot \text{dnf}_f(A)$.

To prove $\Gamma \vdash_{\lambda S_\delta} a : A$ we only have to prove $\Gamma \vdash_{\lambda S_\delta} a$. Because if $\Gamma \vdash_{\lambda S_\delta} a : B$ for some $B$, then $\text{dnf}(\Gamma) \vdash_{\lambda S_\delta} \text{dnf}_f(a) \cdot \text{dnf}_f(B)$, by UT$_{\beta}$ $\text{dnf}_f(B) \cong_{\beta} \text{dnf}_f(A)$, so $\Gamma \vdash B \cong_{\gamma\delta} A$, and by ($\beta\delta$CONV) $\Gamma \vdash_{\lambda S_\delta} a : A$

It is not difficult to prove $\Gamma \vdash_{\lambda S_\delta} a : a$ is well-typed in $\Gamma$, so $\Gamma \vdash_{\lambda S_\delta} a$ or $\Gamma \vdash_{\lambda S_\delta} a : a$. If $\Gamma \vdash_{\lambda S_\delta} : a$ then by correctness of types $\Gamma \vdash_{\lambda S_\delta} a : s$ or $a \in S$. If $a \in S$, then it follows from $\text{dnf}(\Gamma) \vdash_{\lambda S_\delta} \text{dnf}_f(a) \cdot \text{dnf}_f(A)$ by the generation lemma (2.12) that $(a : s') \in A$ for some $s' \in S$, and hence by the start lemma (2.10) $\Gamma \vdash_{\lambda S_\delta} a : s'$.

An immediate consequence of theorems 2.36 and 2.38 is that for functional systems a typing statement holds in $\lambda S_\delta$ iff its $\delta$-normal form holds in $\lambda S$.

2.39 COROLLARY (Equivalence of $\lambda S$ and $\lambda S_\delta$).

Let $S$ be a functional specification, and let $a$ and $A$ be well-typed in context $\Gamma$ in $\lambda S_\delta$. Then

1. $\Gamma \vdash_{\lambda S_\delta} a : A \iff \text{dnf}(\Gamma) \vdash_{\lambda S_\delta} \text{dnf}_f(a) \cdot \text{dnf}_f(A)$
2. $\Gamma \vdash_{\lambda S_\delta} a : A \iff \text{dnf}(\Gamma) \vdash_{\lambda S_\delta} \text{dnf}_f(a) \cdot \text{dnf}_f(A)$
3. $\Gamma \vdash_{\lambda S_\delta} a : A \iff \text{dnf}(\Gamma) \vdash_{\lambda S_\delta} \text{dnf}_f(a) \cdot \text{dnf}_f(A)$.
So, modulo $\delta$-conversion, the DPTS $\lambda S_6$ and the PTS $\lambda S$ are the same type system.

Theorem 2.38 does not hold for all (D)PTSs. It is easy to give a counterexample for a system that is not functional:

2.40 COUNTEREXAMPLE. Let $S$ be the specification

$$S = \{ \ast, \Box, \Box' \}, \quad A = \{ \ast, \Box, \ast, \Box' \}, \quad R = \emptyset$$

Then in the context $x = \ast \Box$ the term $x$ has type $\Box$, but not type $\Box'$,

$$x = \ast \Box \quad \vdash_{\lambda S_6} x : \Box$$
$$x = \ast \Box' \quad \not\vdash_{\lambda S_6} x : \Box'$$

whereas the $\delta$-normal form of $x = \ast \Box$ does have type $\Box'$.

The problem is that we record types in definitions. For functional systems this is harmless, since the types are unique up to conversion. But for non-functional systems the choice of a particular type for a definition (e.g. $\Box$ as the type of $x$ in the example above) imposes restrictions. Theorem 2.38 could be extended to all systems by having definitions of the form $x = a$ instead of $x = a A$. However, in a typechecker the types of definitions will be recorded for the sake of efficiency. Otherwise to typecheck a term we have to typecheck its $\delta$-normal form, which can be much longer than the original term. Another reason to include type information in definitions is that in a definition $x = a A$ the term $a$ may be a proof of a proposition $A$. In this case the definition plays the role of a lemma or theorem, and the type $A$ is then typically of more interest than the proof term $a$.

The definition mechanism of a DPTS leaves something to be desired. Many definitions involve parameters. In a DPTS, lambda abstractions have to be used to parameterise definitions. For example, an abbreviation for the composition of functions can be introduced by the definition

$$\text{comp} = \lambda A, B, C \ast. \lambda f \colon A \rightarrow B. \lambda g \colon B \rightarrow C. \lambda x \colon A. g(f \, x).$$

Then for $f : A \rightarrow B$ and $g : B \rightarrow C$ we can write $(\text{comp} \, A \, B \, C \, f \, g)$ for the composition of $f$ and $g$. Using lambda abstractions to parameterise definitions has two disadvantages.

A potential problem is that in a given PTS the required lambda abstractions may not be allowed. For instance, in the simply typed lambda calculus $\lambda \rightarrow$ abstractions over types, e.g. $\lambda A, B, C \ast \ldots$ in the example above, are not allowed.

A more practical problem is that terms such as $(\text{comp} \, A \, B \, C \, f \, g)$ are cluttered with type information. This problem does not only arise with definitions, but it is typical of explicitly typed languages. Often one would want to leave some parameters implicit, to be inferred by the type checker. We cannot expect a type checker to be able to reconstruct all arguments that are omitted. However, in many cases reconstruction of missing parameters is computable. For example, it is not difficult to see how the type parameters $A$, $B$ and $C$ in $(\text{comp} \, A \, B \, C \, f \, g)$ could be reconstructed if they were omitted. For the sake of readability we will sometimes omit parameters (and use infix notation).
Part I

Syntax
Chapter 3

The Basic System: $\lambda\omega_L$

In this chapter the type system $\lambda\omega_L$ is introduced. It consists of

- a programming language, which provides programs and their datatypes.
- a logic, which provides everything needed to reason about these programs. Properties of programs (e.g. specifications of programs) can be expressed in it, and it can be proved that a certain program has a certain property (e.g. meets a certain specification) or not. $\lambda\omega_L$ can be concisely described as a PTS. It is a refinement of the Calculus of Constructions. Instead of having just one universe of types, we distinguish datatypes and propositions, and restrict the dependencies between them. This strict separation between programming language and logic makes it easier to extend the programming language without disturbing the logic, and vice versa. This is exploited in later chapters, where possible extensions of the programming language and of the logic are considered.

The programming language is $\lambda\omega$, the PTS which is essentially Girard’s system $\mathcal{F}^\omega$. So $\lambda\omega_L$ is a logic for reasoning about $\lambda\omega$. The system $\lambda\omega$ is also used as the basis of the programming languages QUEST [Car89] and LEAP [PL89]. Like all PTSs, $\lambda\omega$ is a very bare type system, providing only a few primitives. However, these are very general and powerful ones, making $\lambda\omega$ a very powerful language. In the following chapters, more typing constructors will be introduced as primitives.

In fact, $\lambda\omega_L$ has two subsystems that are copies of $\lambda\omega$. One of these serves as the programming language. terms are programs and types are datatypes. The other serves a logic. terms are proofs and types are propositions. These two copies of $\lambda\omega$ are called $\lambda\omega_s$ and $\lambda\omega_p$. The subscripts refer to the fact that types are interpreted as sets in $\lambda\omega_s$, and as propositions in $\lambda\omega_p$.

Of course, for every PTS we introduce there is an associated DPTS. Depending on which is the best suited, we use one or the other. The PTS is used to explain the expressiveness of the system, the DPTS is used whenever we need the definition mechanism.

We begin by discussing the two interpretations of $\lambda\omega$ – as a programming language and as a logic – in sections 3.1 and 3.2, and then in section 3.3 the programming logic $\lambda\omega_L$ is defined. In section 3.4 we discuss how programs can be constructed together with their correctness proofs. Section 3.5 contains a comparison with the approach to program construction in the Calculus of Constructions using program extraction.
3.1 \( \lambda \omega \) as a programming language: \( \lambda \omega _{2} \)

In this section we discuss the system \( \lambda \omega \) considered as a programming language. The following copy of \( \lambda \omega \) is reserved for the interpretation of \( \lambda \omega \) as a programming language.

3.1 Definition \( \lambda \omega _{2(\downarrow )} \) is the (D)PTS specified by

\[
S = \{ \ast _{s}, \square _{s} \}, \quad A = \{ \ast _{s} : \square _{s} \}, \quad R = \{ (\ast _{s}, \ast _{s}), (\square _{s}, \ast _{s}), (\square _{s}, \square _{s}) \} .
\]

This very compact definition of \( \lambda \omega _{2} \) is not very enlightening. Below we discuss the different kinds of terms that can be distinguished in \( \lambda \omega _{2} \), and the different forms of abstractions that are allowed.

In a PTS there is just one collection of (pseudo)terms, but to understand \( \lambda \omega _{2} \) we will distinguish different subsets for the different "levels" of \( \lambda \omega _{2} \).

1. Programs. This includes data such as booleans, natural numbers or lists, and functions that manipulate these.

2. Datatypes and datatype-constructors. Datatypes are the types of programs. They form a subset of the datatype-constructors. The other datatype-constructors are functions that can be used to construct datatypes, such as a function \( \times \) that maps two datatypes to their product type, or a function list that maps a datatype \( \sigma \) to the datatype of \( \sigma \)-lists.

An important difference between the datatypes and the other datatype-constructors is that the former can be inhabited by programs, whereas the latter cannot. For instance, a function list from datatypes to datatypes cannot be the type of something.

3. Kinds. The kinds are the types of datatype-constructors. The kinds are generated by

\[
\mathbb{K} := \ast _{s} \mid \mathbb{K} \\
\]

\( \ast _{s} \) is the type of all datatypes, \( \ast _{s} \rightarrow \ast _{s} \) is the type of all functions from datatypes to datatypes, etc. For example, list has type \( \ast _{s} \rightarrow \ast _{s} \), and \( \times \) has type \( \ast _{s} \rightarrow \ast _{s} \rightarrow \ast _{s} \).

In practice, only the simplest kind-expressions will ever be used. For a complex kind, for instance \( (\ast _{s} \rightarrow \ast _{s}) \rightarrow (\ast _{s} \rightarrow \ast _{s}) \), it is difficult to think of a datatype-constructor of that type.

There is a fourth level in \( \lambda \omega _{2} \), which consists just of the symbol \( \square _{s} \). \( \square _{s} \) is the type of all the kinds, so \( \ast _{s}, \ast _{s} \rightarrow \ast _{s} \), etc. all have type \( \square _{s} \). It plays an important role in the definition of \( \lambda \omega _{2} \) as a PTS, as it allows a uniform description of the programs, datatype-constructors, and the kinds. Apart from this it is never used.

The kinds, datatype-constructors, datatypes, and programs, are formally defined as follows:

3.2 Definition.

1. If \( \Gamma \vdash \mathbb{K} : \square _{s} \) for some context \( \Gamma \), then \( \mathbb{K} \) is a kind.

2. If \( \Gamma \vdash \sigma : \mathbb{K} \) for some kind \( \mathbb{K} \) and context \( \Gamma \), then \( \sigma \) is a datatype-constructor.
3.1. \( \lambda \omega \) AS A PROGRAMMING LANGUAGE: \( \lambda \omega_s \\n
3. If \( \Gamma \vdash \sigma : \ast_s \) for some context \( \Gamma \), then \( \sigma \) is a \textit{datatype} (and a datatype-constructor).

4. If \( \Gamma \vdash M : \sigma \) for some datatype \( \sigma \) and context \( \Gamma \), then \( M \) is a \textit{program}.

Later, in definition 3.4, it is shown that the distinction between these levels can already be made for the pseudoterms.

Contexts can declare variables from \( \text{Var}^\sigma \) as datatype-constructors and variables from \( \text{Var}^* \) as programs. For example, the context

\[
\text{list} : \ast_s \rightarrow \ast_s, \ n : \text{nat}, \ f : \text{nat} \rightarrow \text{nat}, \ \alpha : \ast_s, \ x : \alpha
\]

declares a datatype-constructor list, datatypes nat and \( \alpha \), and programs (data) \( n, f \) and \( x \). Here \( \text{list, nat, } \alpha \in \text{Var}^\sigma \) and \( n, f, x \in \text{Var}^* \).

3.3 CONVENTION. \( \mathcal{K}, \mathcal{K}_1, \mathcal{K}_2 \) range over kinds. \( \rho, \sigma, \tau \) range over datatypes and the other datatype-constructors. \( \alpha, \beta \) range over \( \text{Var}^\sigma \), i.e. variables that are datatype-constructors. \( M, N, f \) range over programs \( x, y, z \) range over \( \text{Var}^* \), i.e. program-variables.

Each of the PTS-rules enables a certain kind of abstraction, by allowing certain product types to be formed. There are three different forms of abstraction in \( \lambda \omega_s \), one for each of its rules. The rule \((\square_\ast, \square_\ast)\) provides a form of abstraction in datatype-constructors. The rules \((\ast_s, \ast_s)\) and \((\square_\ast, \ast_s)\) provide two forms of abstraction in programs.

The rule \((\ast_s, \ast_s)\) makes it possible to abstract over a \textit{datatype in a program}. This results in programs of the form \((\lambda x. \sigma. M)\), where \( \sigma \) is a datatype. Such a program expects another program (of type \( \sigma \)) as argument. It is a program that maps programs to programs.

The type of such an abstraction is a \textit{function type} of the form \( \sigma \rightarrow \tau \). The rule \((\ast_s, \ast_s)\) allows the formation of these function types

\[
\frac{\Gamma \vdash \sigma : \ast_s \quad \Gamma \vdash \tau : \ast_s}{\Gamma \vdash \sigma \rightarrow \tau : \ast_s}
\]

A simple example of this form of abstraction is \((\lambda x. \sigma. x)\), the identity on a datatype \( \sigma \), which has type \( \sigma \rightarrow \sigma \).

The rule \((\square_\ast, \ast_s)\) makes it possible to abstract over a \textit{kind in a program}. This results in programs of the form \((\lambda \alpha : \mathcal{K}. \sigma. M)\) where \( \mathcal{K} \) is a kind. Such a program expects a datatype-constructor (of type \( \mathcal{K} \)) as argument.

Most abstractions over a kind will be abstractions over the kind \( \ast_s \). This results in programs of the form \((\lambda \alpha : \ast_s. \sigma. M)\). Such a program expects a datatype as argument. It is a program that maps datatypes to programs.

For example, in the program \((\lambda x. \alpha. x)\) - the identity on a datatype \( \alpha \) - we can abstract over all possible datatypes \( \alpha \). This results in \((\lambda \alpha : \ast_s. \lambda x. \alpha. x)\), the \textit{polymorphic} identity. Depending on the datatype this function gets as argument, it produces the identity on that datatype.

Programs of the form \((\lambda \alpha : \mathcal{K}. \sigma. M)\) are called \textit{parametric polymorphic programs}. Depending on the datatype(constructor) such a program gets as argument, it can have many different types. The types of these programs are \textit{polymorphic types} of the form \((\Pi \alpha : \mathcal{K}. \sigma)\). For
example, \((\lambda \alpha \cdot x : \alpha \cdot \alpha) : (\Pi \alpha \cdot x : \alpha \cdot \alpha)\). The rule \((\square, *_*\) allows the formation of these polymorphic types

\[
\frac{\Gamma \vdash K : \square \quad \Gamma, \alpha : K \vdash \tau : \star_s}{\Gamma \vdash (\Pi \alpha : K \cdot \tau) : \star_s}
\]

This kind of abstraction in programs can be used to define so-called generic programs – programs that are parameterised by datatypes – that behave uniformly for a whole class of types. An example of such a program is polymorphic identity defined above. A more interesting example is the program \(\text{reverse} : \Pi \alpha \cdot \text{list} \alpha \rightarrow \text{list} \alpha\) which reverses a list, and can be used for lists of any datatype. Another use of this kind of abstraction in programs involves abstract datatypes. This is treated in more detail in chapter 4.

Finally, the rule \((\square, \square_s\) allows the formation of kinds of the form \(K_1 \rightarrow K_2\).

\[
\frac{\Gamma \vdash K_1 : \square_s \quad \Gamma \vdash K_2 : \square}{\Gamma \vdash \square_{K_1 \rightarrow K_2} : \square}
\]

For example, this rule allows the formation of \(*_s \rightarrow \star_s\), which is the type of functions from datatypes to datatypes such as list. These kinds make it possible to abstract over a kind in a datatype-constructor. This results in datatype-constructors of the form \((\lambda \alpha : K \cdot \sigma)\), where \(K\) is a kind. Such a datatype-constructor expects another datatype-constructor (of type \(K\)) as argument.

An example of such an abstraction is \((\lambda \alpha \cdot \sigma, \alpha \rightarrow \alpha) : \star_s \rightarrow \star_s\), the datatype-constructor that maps a datatype \(\alpha\) to the datatype \(\alpha \rightarrow \alpha\).

Another way to understand the effect of an individual PTS-rule is to consider the dependency between programs and datatypes it introduces. This is used in Barendregt’s \(\lambda\)-cube [Bar92], to characterise the different axes.

- \((\star_s, \star_s\) gives programs that depend on programs
  - For example, the program \((\lambda \tau \cdot \sigma, M)N\) depends on the program \(N\)
- \((\square_s, \star_s\) gives programs that depend on datatypes
  - For example, the program \((\lambda \alpha \cdot \star_s, M)\sigma\) depends on the datatype \(\sigma\)
- \((\square_s, \square_s\) gives datatypes that depend on datatypes
  - For example, the datatype list \(\sigma\) depends on the datatype \(\sigma\)

In definition 3.2 the different levels of \(\lambda \omega\) were defined in terms of the typing relation. This distinction can already be made for the pseudoterms.

3.4 DEFINITION The sets of pseudoterms \(\text{Kind}, \text{Cons}\) and \(\text{Prog}\) are defined by

\[
\begin{align*}
\text{Kind} & \quad = \quad \star_s \mid \text{Kind} \\
\text{Cons} & \quad = \quad \text{Var}^{\square_s} \mid \Lambda \text{Var}^{\square_s} \mid \text{Kind} \mid \text{Cons} \mid \text{Cons Cons} \\
\text{Prog} & \quad = \quad \text{Var}^{\star_s} \mid \Lambda \text{Var}^{\star_s} \mid \text{Cons} \mid \text{Prog} \mid \text{Prog Cons}
\end{align*}
\]

\(\square\)
3.1. \( \lambda \omega \) AS A PROGRAMMING LANGUAGE : \( \lambda \omega_S \)

This definition refines the context-free syntax given for arbitrary PTSs in chapter 2. Note that these three sets of pseudoterms are disjoint. The kinds, datatype-constructors and programs, as defined in definition 3.2 are elements of Kind, Cons and Prog, respectively:

3.5 LEMMA (Classification for \( \lambda \omega_S \)).

1. If \( \Gamma \vdash K : \Box_s \) then \( K \in \text{Kind} \).
2. If \( \Gamma \vdash \sigma : K : \Box_s \) then \( \sigma \in \text{Cons} \).
3. If \( \Gamma \vdash M : \sigma : \ast_s \) then \( M \in \text{Prog} \).

PROOF By induction on the derivation of \( \Gamma \vdash a : A \) we prove

\[
\Gamma \vdash \sigma : A \quad \Rightarrow \quad \begin{cases} \quad A \equiv \Box_s \quad \Rightarrow \quad a \in \text{Kind} \\ \quad \Gamma \vdash A : \Box_s \quad \Rightarrow \quad a \in \text{Cons} \\ \quad \Gamma \vdash A : \ast_s \quad \Rightarrow \quad a \in \text{Prog} \end{cases}
\]

The only non-trivial cases are (\( \Pi \text{form} \)), (\( \Pi \text{intro} \)) and (\( \Pi \text{elim} \)). Here we have to distinguish the different possibilities for the subterms of \( a \), i.e. whether these are kinds, datatype-constructors or programs.

We show just the case that the last step is the rule (\( \Pi \text{form} \)), i.e. the last step in the derivation is

\[
(\Pi \text{form}) \quad \frac{\Gamma \vdash A : s_1 \quad \Gamma, x : A \vdash B : s_2}{\Gamma \vdash (\Pi x . A . B) : s_2}
\]

for some \( (s_1, s_2) \in R \). There are three possibilities for \( (s_1, s_2) \):

- \( (s_1, s_2) \equiv (\Box_s, \Box_s) \). Then, by the IH, \( A, B \in \text{Kind} \). By the definition of Kind then also \( A \rightarrow B \in \text{Kind} \), so we have to show that \( (\Pi x . A . B) \) is \( A \rightarrow B \), i.e. that \( x \notin \text{FV}(B) \). It follows from the definition of Kind that all elements of Kind are closed, so \( x \notin \text{FV}(B) \).

- \( (s_1, s_2) \equiv (\ast_s, \ast_s) \). Then, by the IH, \( A, B \in \text{Cons} \), and so \( A \rightarrow B \in \text{Cons} \). Again we have to show that \( (\Pi x . A . B) \) is \( A \rightarrow B \), i.e. that \( x \notin \text{FV}(B) \). \( \Gamma \vdash A : \ast_s \), so \( x \in \text{Var}^{\ast_s} \). It follows from the definition of Cons that elements of Cons do not contain variables from \( \text{Var}^{\ast_s} \), so \( x \notin \text{FV}(B) \).

- \( (s_1, s_2) \equiv (\Box_s, \ast_s) \). Then, by the IH, \( A \in \text{Kind} \) and \( B \in \text{Cons} \) \( \Gamma \vdash A : \Box_s \), so \( x \in \text{Var}^{\ast_s} \), and hence \( (\Pi x . A . B) \in \text{Cons} \).

Kind, Cons and Prog provide a clear hierarchy between the different levels of (pseudo)terms. Kinds can occur in datatype-constructors and datatype-constructors can occur in programs, but programs cannot occur in datatype-constructors or kinds, and datatype-constructors cannot occur in kinds.

\( \lambda \omega_S \) and its extension with definitions \( \lambda \omega_{S\delta} \) are strongly normalising:

3.6 THEOREM \( \lambda \omega_{S\delta} \) is \( SN_{S\delta} \).

PROOF \( \lambda \omega_{S\delta} \) is a subsystem of \( \lambda C_{\delta} \), and \( \lambda C_{\delta} \) is \( SN_{S\delta} \) (theorem 2.34).
Basic datatypes and datatype-constructors

To use \( \lambda \omega \) as a programming language, some basic datatypes and primitive operations on them are needed. There are representations for many datatypes in \( \lambda \omega \), for example.

3.7 Example (Polymorphic Church-numerals). The context:

\[
\begin{align*}
\text{polynat} & = \Pi \alpha \cdot \ast_{\alpha} \quad (\alpha \to \alpha) \to (\alpha \to \alpha) : \ast_{\alpha}, \\
0 & = \lambda \alpha \cdot \ast_{\alpha} \quad \lambda f. \alpha \to \alpha : \lambda x : \alpha. x : \ast_{\alpha}, \\
S & = \lambda n. \text{polynat} \quad \lambda \alpha \cdot \ast_{\alpha} \quad \lambda f. \alpha \to \alpha : \lambda x : \alpha. \Pi n f x : \text{polynat} \to \text{polynat}
\end{align*}
\]

defines a representation for the natural numbers, the so-called polymorphic Church-numerals. These representations behave as natural numbers from a computational point of view, i.e., if we consider their reduction behaviour. For example, a function plus : polynat \to polynat \to polynat can be defined such that plus \( (S^n 0) (S^m 0) \lesssim (S^{n+m} 0) \).

In \( \lambda \omega \), there are representations for products, sums and existential types (or abstract datatypes), as well as many "basic" types, such as the empty type, a unit type, and booleans. In fact, there are representations for all free term algebras, as shown in [BB85]. As representations of datatypes these encodings have well-known limitations (see for instance [CP90]). First of all, their reduction behaviour can be very inefficient. For example, for a predecessor function \( \text{pred} : \text{polynat} \to \text{polynat} \), the reduction \( \text{pred} (S^{n+1} 0) \overset{\beta}{\Rightarrow} S^n 0 \) requires \( O(n) \) steps, and it is not possible to define a function \( \text{pred} \) such that \( \text{pred} (S^n \tau) \overset{\beta}{\Rightarrow} \tau \) for variables \( \tau \). Moreover, in \( \lambda \omega \), none of the properties we need, for example the induction principle for \( \text{polynat} \), are provable. So, if we want to reason about programs, it is not helpful to use these unnatural encodings.

In the following chapters, different datatypes and datatype-constructors will be added as primitives, even though there may be encodings for them in \( \lambda \omega \). This gives us direct control over their interpretation in the model. For example, product types \( \sigma \times \tau \) can then be directly interpreted as products in the model, and not as an interpretations of their \( \lambda \omega \)-encodings. This makes it easier to extend the programming language with certain operations, or the logic with certain axioms, on the basis of the model. Another advantage is that a direct implementation of these primitives can be more efficient than encodings.
3.2 \( \lambda \omega \) AS A LOGIC: \( \lambda \omega_p \)

In this section we discuss the system \( \lambda \omega \) considered as a logic. The types are now interpreted as propositions instead of datatypes, and the terms as proofs instead of programs. In comparison with the discussion of \( \lambda \omega_s \), the emphasis is now more on the types than on the terms.

The following copy of \( \lambda \omega \) is reserved for the interpretation of \( \lambda \omega \) as a logic:

3.8 Definition. \( \lambda \omega_{p(d)} \) is the (D)PTS specified by

\[
S = \{ \ast_p, \Box_p \}, \quad A = \{ \ast_p : \Box_p \}, \quad R = \{ (\ast_p, \ast_p), (\Box_p, \ast_p), (\Box_p, \Box_p) \}.
\]

The same levels can be distinguished as in \( \lambda \omega_s \), but now their interpretation is different. The different levels of \( \lambda \omega_p \)-terms are called

1. **Proofs.** The proofs are sometimes called *proof terms* to stress that they are \( \lambda \)-terms that represent natural deduction proofs. For human readers, the usefulness of proof terms is limited, because they become quickly too long to be readable. They are useful representations of proofs for machine manipulation. Verifying correctness of proofs amounts to type-checking them.

2. **Propositions and prop-constructors.** The propositions are the types of the proofs. If a proof \( p \) has as type the proposition \( P \), this is read as "\( p \) is a proof of \( P \)."

The propositions form a subset of the prop-constructors. The other prop-constructors are functions that can be used to construct propositions. This includes the logical connectives, for example a function \( \land \) that maps two propositions to their conjunction, or a function \( \neg \) that maps a proposition to its negation.

3. **Prop-kinds.** The prop-kinds are the type of prop-constructors. The prop-kinds are generated by

\[
\mathcal{P} = \ast_p | \mathcal{P} \to \mathcal{P}.
\]

\( \ast_p \) is the type of all propositions, \( \ast_p \to \ast_p \) is the type of all functions from propositions to propositions, etc. For example, \( \neg \) has type \( \ast_p \to \ast_p \), and \( \land \) has type \( \ast_p \to \ast_p \to \ast_p \).

The fourth level in \( \lambda \omega_p \) consists of just the symbol \( \Box_p \). \( \Box_p \) is the type of all the prop-kinds, e.g. \( \ast_p, \ast_p \to \ast_p \), etc. all have type \( \Box_p \).

3.9 Definition

1. If \( \Gamma \vdash \mathcal{P} : \Box_p \) for some context \( \Gamma \), then \( \mathcal{P} \) is a *prop-kind*.

2. If \( \Gamma \vdash P : \mathcal{P} \) for some prop-kind \( \mathcal{P} \) and some context \( \Gamma \), then \( P \) is a *prop-constructor*.

3. If \( \Gamma \vdash P : \ast_p \) for some context \( \Gamma \), then \( P \) is a *proposition* (and a prop-constructor).

4. If \( \Gamma \vdash p : P \) for some proposition \( P \) for some context \( \Gamma \), then \( p \) is a *proof*. 

\[\square\]
The distinction between these different levels can already be made for the pseudoterms, exactly as is done for \( \lambda \omega_L \). This will be done later for the whole of \( \lambda \omega_L \).

Contexts can declare prop-constructors and proofs. The former are variables in \( \text{Var}^{\square_*} \), the latter are variables in \( \text{Var}^{\ast_*} \). For example, the context
\[
\ast_p \rightarrow \ast_p, \quad P \cdot \ast_p, \quad p \cdot \neg P
\]
declares prop-constructors \( \neg \) and \( P \) and a proof \( p \). Here \( \neg, P \subseteq \text{Var}^{\square_*} \) and \( p \subseteq \text{Var}^{\ast_*} \). The declaration \( p : \neg P \) in the context is an assumption (or an axiom), via the assumption that there is a proof \( p \) of the proposition \( \neg P \).

3.10 CONVENTION. \( \mathcal{P}, \mathcal{P}_1, \mathcal{P}_2 \) range over prop-kinds. \( P, Q, R, S, T \) range over propositions and the other prop-constructors. \( p, q \) range over proofs.

We do not reserve special variables for ranging over \( \text{Var}^{\square_*} \) and \( \text{Var}^{\ast_*} \). \( P, Q \) can be elements of \( \text{Var}^{\square_*} \), and \( p, q \) can be elements of \( \text{Var}^{\ast_*} \). □

The rules \((\ast_p, \ast_p)\) and \((\Box_p, \ast_p)\) provide two ways of forming propositions. The rule \((\ast_p, \ast_p)\) allows the formation of implication
\[
\frac{\Gamma \vdash P \quad \ast_p}{\Gamma \vdash P \Rightarrow Q \quad \ast_p}
\]
Here \( \Rightarrow \) is just another notation for \( \rightarrow \) that reflects its intended interpretation. The associated introduction and elimination rules are:

\[(\Rightarrow \text{intro}) \quad \frac{\Gamma, p \vdash Q \quad \Gamma \vdash \Box_p \vdash Q}{\Gamma \vdash (\lambda p : P \ q) : P \Rightarrow Q}\]
\[(\Rightarrow \text{elim}) \quad \frac{\Gamma \vdash q \quad P \Rightarrow Q \quad \Gamma \vdash p \cdot P}{\Gamma \vdash q \ p \cdot Q}
\]
A proof of \( P \Rightarrow Q \) is a function which maps proofs of \( P \) to proofs of \( Q \), which is the Brouwer-Heyting-Kolmogorov interpretation of implication. Omitting the proof terms \( p, q, (\lambda p : P \ q) \) and \( q \ p \) leaves the usual introduction and elimination rules for implication in natural deduction.

The rule \((\Box_p, \ast_p)\) allows higher order universal quantification
\[
\frac{\Gamma \vdash \mathcal{P} : \Box_p \quad \Gamma \vdash P \quad \mathcal{P} \vdash \Box_p \vdash \ast_p}{\Gamma \vdash (\forall p : \mathcal{P} \ P) : (\forall p : \mathcal{P}) \vdash \ast_p}
\]
Here \( \forall \) is just another notation for \( \Pi \). If \( \mathcal{P} \) is \( \ast_p \) this results in quantification over all propositions, as in second order logic. This makes it possible for example to form the proposition \((\forall P : \ast_p \rightarrow P \Rightarrow P)\).

Finally, the rule \((\Box_p, \Box_p)\) allows the formation of prop-kinds of the form \( \mathcal{P}_1 \rightarrow \mathcal{P}_2 \)
\[
\frac{\Gamma \vdash \mathcal{P}_1 : \Box_p \quad \Gamma \vdash \mathcal{P}_2 \quad \Box_p}{\Gamma \vdash \mathcal{P}_1 \rightarrow \mathcal{P}_2 \quad \Box_p}
\]
For example, it provides the prop-kind \( \ast_p \rightarrow \ast_p \), the type of \( \neg \) and \( \ast_p \rightarrow \ast_p \rightarrow \ast_p \), the type of \( \vee \) and \( \wedge \). It also makes it possible to abstract over a prop-kind in propositions and prop-constructors. For example, the propositional connective \( \neg \) can be defined as
\[(\lambda P : \ast_p \ P \Rightarrow \text{False}) \cdot \ast_p \rightarrow \ast_p, \text{where False is the proposition representing falsehood.}\]
Basic propositions and prop-constructors.

To use $\lambda\omega_p$ as a logic, some basic logical connectives and their properties are needed. These could be declared in the context, but it is well-known that all connectives are definable in terms of implication and higher order universal quantification.

3.11 Definition. $\Gamma_{\text{LOGIC}}$ is the context

\[
\begin{align*}
\text{False} &= (\forall P:*_p, P:*_p), \\
\text{True} &= (\forall P:*_p, P \Rightarrow P:*_p), \\
\neg &= \lambda P:*_p, P \Rightarrow \text{False}:*_p -*_p, \\
\land &= \lambda P, Q:*_p, (\forall R:*_p, (P \Rightarrow Q \Rightarrow R) \Rightarrow R):*_p -*_p -*_p, \\
\lor &= \lambda P, Q:*_p, (\forall R:*_p, (P \Rightarrow R) \Rightarrow (Q \Rightarrow R) \Rightarrow R):*_p -*_p -*_p, \\
\leftrightarrow &= \lambda P, Q:*_p (P \Rightarrow Q) \wedge (Q \Rightarrow P):*_p -*_p -*_p.
\end{align*}
\]

This context defines the propositional constants truth (True) and falsehood (False) and the logical connectives negation ($\neg$), conjunction ($\land$), disjunction ($\lor$), and bi-implication ($\leftrightarrow$).

For a propkind $\mathcal{P}$ we can define

\[
\exists_{\mathcal{P}} := \lambda \mathcal{P}:\Box_{\mathcal{P}}, \exists_{\mathcal{P}} (\forall R:*_p, (\forall X:\mathcal{P}(PX) \Rightarrow R) \Rightarrow R) \Rightarrow (\mathcal{P} \Rightarrow *_p) \Rightarrow *_p.
\]

Then for a term $(\lambda X: \mathcal{P}. P) : \mathcal{P} \Rightarrow *_p$, the term $\exists_{\mathcal{P}}(\lambda X: \mathcal{P}. P)$ represent the higher order existential quantification "$(\exists X: \mathcal{P}. P)$". The definition of $\exists_{\mathcal{P}}$ is parameterised by a propkind $\mathcal{P}$. We cannot abstract over $\mathcal{P}$ and define $\exists$ as follows

\[
\exists = \lambda \mathcal{P}:\Box_{\mathcal{P}}, \exists_{\mathcal{P}} \\
\Pi K: \Box_{\mathcal{P}} (\mathcal{P} \Rightarrow *_p) \Rightarrow *_p,
\]

because the abstraction $\lambda \mathcal{P}:\Box_{\mathcal{P}}$ is not allowed in $\lambda\omega_p$.

The $\lambda\omega_s$-counterparts of some of the $\lambda\omega_p$-encodings given above – i.e. these terms with all subscripts $p$ replaced by the subscript $s$ – can be used to represent certain datatype-constructors. For instance, the encoding of $\land$ can be used to represent product types, and the encoding of $\lor$ can be used to represent disjoint sum types. At the end of section 3.1, it was already mentioned that such encodings of datatype-constructors in $\lambda\omega_s$ have some shortcomings. The encodings of the logical connectives in $\lambda\omega_p$ is less problematic. Firstly, all their intuitionsistic properties, i.e. their introduction and elimination principles, are provable in $\lambda\omega_p$. For example, in $\lambda\omega_p$ we can prove $(\forall P:*_p, \text{False} \Rightarrow P), (\forall P, Q:*_p, P \Rightarrow (P \lor Q))$, and $(\forall P, Q:*_p, (P \land Q) \Rightarrow P)$. Note that the quantification over propositions makes it possible to express these introduction and elimination principles inside the system $\lambda\omega_p$. Secondly, it is easy to show that these representations have the right interpretation in the proof-irrelevance model given in chapter 6 (see example 6.27).

Consistency

When we use $\lambda\omega_p$ as a logic, we are interested in the question whether it is consistent. $\lambda\omega_p$ is consistent, in the sense that not all propositions are provable. This is equivalent with saying that $\text{False}$, as defined in 3.11, is not provable. The definition mechanism does not affect consistency: by corollary 2.39 $\lambda\omega_p$ is consistent if $\lambda\omega_p$ is consistent.
Of course, which propositions are provable depends on the assumptions in the context. For example, in a context containing the assumption \( p : \text{False} \) all propositions are provable. A context is called consistent if not all propositions are provable in it. Using corollary 2.39 we can relate consistency of a context in \( \lambda \omega_p \) and \( \lambda \omega_{p6} \): a context is consistent in \( \lambda \omega_{p6} \) iff its \( \delta \)-normal form is consistent in \( \lambda \omega_p \).

3.12 Theorem (Consistency of \( \lambda \omega_p \)) False is not provable in \( \lambda \omega_{p6} \) in the context \( \Gamma_{\text{Logic}} \).

By corollary 2.39 this is equivalent with saying that \( \forall P \forall P, P \) is not provable in \( \lambda \omega_p \) in the empty context. There are two ways to prove this theorem. The syntactic way is to use the fact that \( \lambda \omega_p \) is SN. From SN it follows that False is not provable: if it were, it would have a proof in normal-form, and a simple syntactic argument shows that no inhabitant of False can be in normal form. A semantic proof can be given using the proof-irrelevance model of \( \lambda \omega_p \) (see lemma 6.31.) The advantage of the second proof is that it can easily be extended to prove consistency of certain contexts, for example:

3.13 Theorem (Consistency of classical logic). False is not provable in the context \( \Gamma_{\text{Logic}} \) extended with the assumption classical \( \forall P \forall P, (\neg P \Rightarrow P) \).

Proof. See lemma 6.31
3.3 The programming logic $\lambda\omega_L$

In this section we introduce the programming logic $\lambda\omega_L$, which contains both $\lambda\omega_s$ and $\lambda\omega_p$. As mentioned earlier, $\lambda\omega_L$ can be divided into two parts: a programming language and a logic for reasoning about this programming language. The relationship between the two parts is asymmetric. We want to be able to say things about the programming language in the logic, but we do not want to be able to say things about the logic in the programming language. Because programs and datatypes will not be allowed to depend on proofs or propositions, $\lambda\omega_L$ will be a conservative extension of the programming language.

$\lambda\omega_s$ serves as the programming language and $\lambda\omega_p$ as part of the logic. $\lambda\omega_p$ alone does not suffice as logic. To reason about $\lambda\omega_s$-constructs 4 more PTS-rules will be added. These rules will allow the formation of proofs and propositions that depend on programs and datatypes.

$\lambda\omega_L$ can be embedded in the Calculus of Constructions, the system $\lambda C$ defined in section 2.19. In fact, it is a subsystem of one of the variants of the Calculus of Constructions defined in [PM89b], as we will see in section 3.5.

Before defining $\lambda\omega_L$, we consider which PTS-rules are required for reasoning about $\lambda\omega_s$-programs and datatypes.

To express properties of programs we need predicates and relations on datatypes. Predicates can be seen as propositional-valued functions, i.e., the type of a predicate on a datatype $\sigma$ is $\sigma \rightarrow *_p$. Similarly, a relation on binary predicate on a datatype $\sigma$ is of type $\sigma \rightarrow \sigma \rightarrow *_p$. For instance, the ordering $\leq$ on the type of natural numbers $\mathsf{nat}$ has type $\mathsf{nat} \rightarrow \mathsf{nat} \rightarrow *_p$.

Equality of programs of type $\sigma$ is a relation $=_\sigma \colon \sigma \rightarrow \sigma \rightarrow *_p$. Like $*_p$, the terms $*_p$ and $\sigma \rightarrow *_p$ are prop-kinds, i.e., they have type $\square_p$. Their formation requires the PTS-rule $(*_p, \square_p)$:

$$\frac{\Gamma \vdash \sigma \quad \Gamma \vdash p : \square_p}{\Gamma \vdash \sigma \rightarrow p : \square_p}$$

For every datatype $\alpha$ a relation of type $\alpha \rightarrow \alpha \rightarrow *_p$ is needed that is the notion of equality for that datatype. This can be achieved by having a single polymorphic equality relation $=_L$ of type $(\Pi \alpha \cdot *_p : \alpha \rightarrow \alpha \rightarrow *_p)$. Then for all datatypes $\sigma$, $(=_L \sigma) : \sigma \rightarrow \sigma \rightarrow *_p$, i.e., $(=_L \sigma)$ is a relation on $\sigma$. For all terms $M$ and $N$ of type $\sigma$, $(=_L \sigma M N) : *_p$, i.e., $(=_L \sigma M N)$ is a proposition. Like $\sigma \rightarrow *_p$ and $\sigma \rightarrow *_p$, the term $(\Pi \alpha \cdot *_p : \alpha \rightarrow *_p)$ is a prop-kind, i.e., it has type $\square_p$. The formation of $(\Pi \alpha \cdot *_p : \alpha \rightarrow *_p)$ requires the PTS-rule $(\square_p, \square_p)$:

$$\frac{\Gamma \vdash \square_p \quad \Gamma \vdash \alpha \quad \Gamma \vdash \square_p}{\Gamma \vdash (\Pi \alpha \cdot *_p : \square_p)}$$

$\lambda\omega_p$ provides higher-order universal quantification. This means that we can quantify over all propositions, e.g., $(\forall P : *_p \ldots)$, over all functions from propositions to propositions, e.g., $(\forall P : *_p \rightarrow *_p \ldots)$, etc. In $\lambda\omega_L$ more possibilities for quantification are needed. For universal quantification over all elements of a datatype the PTS-rule $(*_p, *_p)$ is needed:

$$\frac{\Gamma \vdash \sigma \quad \Gamma \vdash \tau \colon \sigma \rightarrow *_p}{\Gamma \vdash (\forall \tau : \sigma) : *_p}$$

Using this rule, the proposition $\forall x : \mathsf{nat} \cdot (\leq x x)$ can be formed.
For universal quantification over all elements of a kind the PTS-rule \((\Box_s, \ast_p)\) is needed:

\[
\frac{\Gamma \vdash \mathcal{K} \cdot \Box_s \quad \Gamma, \alpha \vdash P : \ast_p}{\Gamma \vdash (\forall \alpha, \mathcal{K} \cdot P) : \ast_p}
\]

By taking \(\mathcal{K} \equiv \ast_s\), this rule allows universal quantification over all datatypes. For example, this is used in the proposition \(\forall \alpha : \ast_s, \forall x : \alpha (=_L \alpha x x)\), which expresses reflexivity of the relation \(=_L\) for all datatypes \(\alpha\).

We have now discussed all the rules of \(\lambda\omega_L\).

3.14 **Definition.** \(\lambda\omega_L(d)\) is the (D)PTS specified by

\[
S = \{\ast_s, \Box_s, \ast_p, \Box_p\} \\
A = \{(*_s \cdot \Box_s), (*_p \cdot \Box_p)\} \\
R = \{(*_s \cdot \ast_s), (*_s \cdot \Box_s), (*_p \cdot \ast_p), (*_p \cdot \Box_p), (\Box_s, \Box_s), (\Box_s, \ast_s), (\Box_s, \Box_p), (\Box_p, \ast_p), (\Box_p, \Box_p)\}
\]

The levels of terms we distinguish in \(\lambda\omega_L\) are those of \(\lambda\omega_s\) and \(\lambda\omega_p\), i.e. kinds, datatypes and datatype-constructors, programs, prop-kinds, propositions and prop-constructors, and proofs. They are defined as in definitions 3.2 and 4.9.

Observe that when \(R\) is regarded as a matrix, we only have rules below or on the diagonal from the top-left to the bottom-right. The system \(\lambda\omega_L\) consists of

- \(\lambda\omega_s\) for the programs and their datatypes \(\{(*_s \cdot \Box_s), (*_s \cdot \ast_s), (*_s \cdot \ast_s)\}\),
- \(\lambda\omega_p\) for the propositions and their proofs: \(\{(*_p \cdot \Box_p), (*_p \cdot \ast_p), (*_p \cdot \ast_p)\}\),
- all possible dependencies of propositions and proofs on programs and types, provided by all rules of the form \((s_1 \cdot s_2)\) \(\{(*_s \cdot \Box_p), (*_s \cdot \ast_p), (*_s \cdot \Box_p), (*_s \cdot \ast_p)\}\)

\(\lambda\omega_L\) does not have all possible PTS-rules. It does not have the rules

- \((\ast_s, \Box_s)\).

As a result, there are no datatypes that depend on programs. An example of a datatype depending on a program is the type (lesser than \(n\)) that consists of all natural numbers smaller than \(n\). Such datatypes are often simply called dependent types. They drastically change the nature of type system: it increases the expressive power to the extent that datatypes can express complete specifications. In chapter 1 we already discussed why we do not want such a very expressive type system for programs. In section 3.5 the main consequence of including the rule \((\ast_s, \Box_s)\) the need for program extraction – is discussed.

If datatypes can depend on programs, then deciding equality of datatypes involves deciding equality of programs. A basic problem with this is that we want equality of datatypes to be decidable - otherwise type checking is undecidable, whereas for programs we typically want an equality which is extensional and (hence) undecidable.
3.3 The Programming Logic $\lambda_{\omega L}$

• $(*_{p}, \Box_{p})$.
  As a result, there are no propositions that depend on proofs. With such propositions properties of proofs can be expressed. We are only interested in proving properties of programs and not in proving properties of proofs. Hence there is no need for proof-dependent propositions.

• $(-p, \neg p)$ As a result, there are no propositions or datatypes that depend on propositions or proofs. The consequences of these dependencies are discussed in section 3.5.

Because there are no rules of the form $(-p, \neg p)$, $\lambda_{\omega L}$ is a conservative extension of the programming language $\lambda_{\omega}$, i.e. in $\lambda_{\omega L}$ we have the same kinds, datatype-constructors and programs as in $\lambda_{\omega}$:

3.15 Theorem (Conservativity of $\lambda_{\omega L}$ over $\lambda_{\omega}$).
Suppose $\Gamma \vdash_{\lambda_{\omega L}} a : A$ and $a$ is a program, datatype-constructor or a kind (i.e. $\Gamma \vdash_{\lambda_{\omega L}} A \circ_{s}$, $\Gamma \vdash_{\lambda_{\omega}} A : \Box_{s}$, or $A \equiv \Box_{s}$ )
Then $\Gamma^{\omega_{L}} \vdash a : A$

Proof. Induction on the derivation of $\Gamma \vdash a : A$.

As for $\lambda_{\omega}$, the different syntactic categories of $\lambda_{\omega L}$ can already be distinguished for the pseudoterms. It follows from the conservativity of $\lambda_{\omega L}$ over $\lambda_{\omega}$ that the kinds, datatype-constructors and programs of $\lambda_{\omega L}$ are elements of Kind, Cons and Prog as defined in definition 3.4. For the prop-kinds, prop-constructors and proofs we define:

3.16 Definition. The sets of pseudoterms $P_{\text{kind}}$, $P_{\text{Cons}}$ and $\text{Proof}$ are defined by

\[
P_{\text{kind}} := \ast_{p} | P_{\text{kind}} \rightarrow P_{\text{kind}}
\]
\[
P_{\text{Cons}} := \text{Var}_{\bar{p}} | \lambda \text{Var}_{\bar{p}}^{*}.\text{Var}_{\bar{p}} \cdot P_{\text{Cons}} \cdot P_{\text{Cons}} \cdot P_{\text{Prog}}
\]
\[
P_{\text{Proof}} := \text{Var}_{\bar{p}}^{*} | \lambda \text{Var}_{\bar{p}}^{*}.P_{\text{Cons}} \cdot \text{Proof} \cdot \text{Proof} \cdot \text{Proof} \cdot \text{Proof} \cdot \text{Proof}
\]

where $A \in \{\lambda, \forall\}$

Note that the different sets of pseudoterms for the different levels of $\lambda_{\omega L}$ can be defined in the following order: Kind, Cons, Prog, Pkind, PCons and Proof. Each of these sets only depends on the ones that precede it in this order. This is caused by the fact that the set of $\lambda_{\omega L}$-rules $R$ in definition 3.14 does not include any rules above the diagonal. It will play an important role in chapter 6, where the semantics of the $\lambda_{\omega L}$ is treated, because it means that the interpretation of the different levels can be defined in the same order.

3.17 Lemma (Classification for $\lambda_{\omega L}$).

1. If $\Gamma \vdash K : \Box_{s}$, then $K \in \text{Kind}$.
2. If $\Gamma \vdash \sigma : \mathcal{K} : \Box$, then $\sigma \in \text{Cons}$

3. If $\Gamma \vdash M : \sigma : *_{p}$ then $M \in \text{Prog}$

4. If $\Gamma \vdash \mathcal{P} : \Box_{p}$ then $\mathcal{P} \in \text{Pkind}$

5. If $\Gamma \vdash P : \mathcal{P} : \Box_{p}$ then $P \in \text{PCons}$

6. If $\Gamma \vdash p : \mathcal{P} : *_{p}$ then $p \in \text{Proof}$

**Proof.** Parts 1 to 3 immediately follow theorem 3.15 and lemma 3.5. The proof of the other parts is then similar to that of lemma 3.5: by induction on the derivation of $\Gamma \vdash \alpha : A$ we prove

$$
\Gamma \vdash a : A \Rightarrow \begin{cases} 
A \equiv \Box_{p} & \Rightarrow a \in \text{Pkind} \\
\Gamma \vdash A : \Box_{p} & \Rightarrow a \in \text{PCons} \\
\Gamma \vdash A : *_{p} & \Rightarrow a \in \text{Proof}
\end{cases}
$$

$\lambda \omega_{L}$ can be embedded in $\lambda C$, the Calculus of Constructions, simply by erasing the subscripts of $*$ and $\Box$:

**3.18 Lemma.** If $\Gamma \vdash a : A$ in $\lambda \omega_{L}(\mathcal{B})$, then $\Gamma \vdash |a| : |A|$ in $\lambda C(\mathcal{B})$, where $|z|$ is $z$ with $*$ substituted for $*_{s}$ and $*_{p}$ and $\Box$ substituted for $\Box_{s}$ and $\Box_{p}$

**Proof.** Induction on the derivation. In fact, it suffices to observe that erasing the subscripts in the specification of $\lambda \omega_{L}(\mathcal{B})$ produces the specification of $\lambda C(\mathcal{B})$.

What makes the system $\lambda \omega_{L}$ a lot simpler than $\lambda C$ is that there are fewer dependencies between the different levels. In $\lambda C$ different levels similar to those of $\lambda \omega_{L}$ can be distinguished, namely kinds, constructors and programs, but these are all mutually dependent. In other words, elements of one of these levels can occur as subexpressions of elements of any other.

By lemma 3.18 it follows immediately from the fact that $\lambda C(\mathcal{B})$ is strongly normalising that $\lambda \omega_{L}$ and its extension with definitions $\lambda \omega_{L}(\mathcal{B})$ are.

**3.19 Theorem.** $\lambda \omega_{L}(\mathcal{B})$ is $\text{SN}_{\mathcal{B}}$.

**Basic propositions and prop-constructors.**

In $\lambda \omega_{L}$ there are three forms of existential quantification: over a prop-kind $\mathcal{P}$, over a datatype $\sigma$ and over a kind $\mathcal{K}$, i.e. of the form $(\exists \alpha : \mathcal{P}, \mathcal{P})$, $(\exists \alpha : \mathcal{P}, \mathcal{P})$ and $(\exists \alpha : \mathcal{K}, \mathcal{P})$, respectively. In definition 3.11 it was shown how in $\lambda \omega_{B}$ the first form of existential quantification can be defined in terms of $\forall$ and $\Rightarrow$. The other two can be defined similarly.

**3.20 Definition.** Existential quantification over a datatype $(\exists)$ and over a kind $\mathcal{K}$ $(\exists_{\mathcal{K}})$ are defined by

$$
\exists = \lambda \alpha. *_{s} : \lambda \mathcal{P}. \alpha \rightarrow *_{*_{p}} \quad \forall \mathcal{R} *_{p} \quad (\forall x \alpha (P x) \Rightarrow R) \Rightarrow R \\
(\exists \alpha. *_{s} : (\alpha \rightarrow *_{p}) \rightarrow *_{p} \\
\exists_{\mathcal{K}} = \lambda \mathcal{P} \mathcal{K} \rightarrow *_{p} : \forall \mathcal{R} *_{p} \quad (\forall \alpha : \mathcal{K} (P \alpha) \Rightarrow R) \Rightarrow R \\
(\mathcal{K} \rightarrow *_{p}) \rightarrow *_{p}
$$

$\square$
3.3. **THE PROGRAMMING LOGIC $\lambda \omega_L$**

In the first definition we have abstracted over all possible datatypes $\alpha$. In the second definition we cannot abstract over all possible kinds $K$, because this abstraction is not allowed in $\lambda \omega_L$.

To use $\lambda \omega_L$ as a programming logic, some basic predicates and their properties are needed. These can be declared in the context, together with the properties we require of them. Another option is to define them in $\lambda \omega_L$. In [PPM90] it is shown how inductively defined propositions, predicates and relations can be represented in the Calculus of Constructions. The same technique can be used in $\lambda \omega_L$. The most important relation – equality of programs – can be defined in $\lambda \omega_L$ as follows:

321 **DEFINITION (Leibniz' Equality).** $\Gamma_{LEIBNIZ}$ is the context

$$= _L = \lambda \alpha \cdot \lambda x, y: \alpha \forall P, \alpha \rightarrow *_{p}, (P x) \Rightarrow (P y)$$

$$\Pi \alpha \cdot \alpha \rightarrow \alpha \rightarrow *_{p}$$

This context defines Leibniz’ equality for programs. $= _L$ will be written infix, with its first argument as a subscript instead of $L$. So $(= _L \sigma M N)$ is written as $M = _\sigma N$. From now on, we always assume that $\Gamma_{LEIBNIZ}$ is part of the context, so that we can always use $= _L$ to express equality of programs in $\lambda \omega_L$.

Despite its asymmetric definition, the predicate $= _L$ has all the required properties:

- It is reflexive, because all $\beta \delta$-convertible programs are Leibniz’ equal, as shown below.

Suppose $\Gamma \vdash M : \sigma$, $\Gamma \vdash N : \sigma$ and $\Gamma \vdash M \equiv_{\beta \delta} N$. Then there is an inhabitant – i.e. a proof – of $M = _\sigma N$ in context $\Gamma$. As an illustration of a formal proof in the logic, this proof and its type derivation are given below. We use the notation for natural deduction described in [Ned90], with "flags" denoting the scope of declarations.

1. $P \sigma \rightarrow *_{p}$

2. $p : P M$

3. $p : P N$

4. $(\lambda P P M. p) : P M \Rightarrow P N$

5. $M \equiv_{\beta \delta} N$, ($\beta \delta$conv)

6. $(\lambda P. \sigma \rightarrow *_{p}, \lambda P P M. p) : (\forall P. \sigma \rightarrow *_{p}, P M \Rightarrow P N)$

7. $\Pi \sigma \cdot \alpha \rightarrow \alpha \rightarrow *_{p}$

8. $\forall \alpha \cdot (\forall \sigma \cdot \forall x, y: \sigma \ (x = _\sigma y) \Rightarrow \forall Q : \sigma \rightarrow *_{p}, (Q x) \Rightarrow (Q y))$

- We can substitute equals for equals in propositions, because

$$\forall \sigma \cdot \forall x, y: \sigma \ (x = _\sigma y) \Rightarrow \forall Q : \sigma \rightarrow *_{p}, (Q x) \Rightarrow (Q y)$$

is provable in $\lambda \omega_L$, as is shown below. Using this property it can be proved that $= _L$ is symmetric and transitive.
In lemma 6.48 it is shown that \( =_L \) is in fact interpreted as equality in the model.

As illustrated above, type derivations for proof terms correspond closely to conventional natural deduction proofs. Proof terms will usually be omitted in such derivations and in typing judgements. Instead of \( \Gamma \vdash p : P \), we then write \( \Gamma \vdash p : P \).

There are important differences between \( \beta\delta \)-conversion and Leibniz' equality. Whereas \( \beta\delta \)-conversion is defined for all (pseudo)terms, Leibniz' equality just for programs of the same type. The most important difference is that properties of Leibniz' equality can be assumed. For example, we can assume that two programs \( M \) and \( N \) of type \( \sigma \) are Leibniz equal by introducing an assumption \( p : M =_\sigma N \) in the context. As will be shown later in example 6.48, \( =_L \) is interpreted as equality in the model. Consequently, any properties that hold for equality of programs in the model can safely be added as axioms. We will introduce axioms for Leibniz' equality that make it an extensional equality. As a consequence, Leibniz' equality for functions, e.g., \( f =_\sigma g \), will be undecidable. On the other hand, \( \beta\delta \)-conversion of all \( \lambda\omega_L \)-terms is decidable, because \( \beta\delta \)-reduction is Church-Rosser and strongly normalising.

Consistency

As for \( \lambda\omega_p \), we are interested in the consistency of \( \lambda\omega_L \).

3.22 Theorem (Consistency of \( \lambda\omega_L \)): False is not provable in \( \lambda\omega_L \) in the context \( \text{LOGIC} \).

As for \( \lambda\omega_p \), there are two ways to prove consistency of \( \lambda\omega_L \): a syntactic proof using the fact that \( \lambda\omega_L \) is SN, or a semantic proof using the proof-irrelevance model of \( \lambda\omega_L \) given in chapter 6 (see lemma 6.49). And as for \( \lambda\omega_p \), the second proof can easily be extended to prove consistency of certain contexts and axioms.

For instance, we want to use classical logic, and we want to assume that equality of functions is extensional, i.e., that

\[
\begin{align*}
\forall \sigma \cdot f =_\sigma f' & \iff (\forall \alpha : \sigma \cdot f \alpha =_\sigma f' \alpha) \\
\forall \sigma \cdot g =_\sigma g' & \iff (\forall \alpha : \sigma \cdot g \alpha =_\sigma g' \alpha)
\end{align*}
\]

for all \( f, f' : \sigma \rightarrow \tau \) and \( g, g' : (\Pi \alpha : \sigma \cdot \tau) \) The implications from left to right immediately follow from the definition of Leibniz' equality, but the implications from right to left have to be introduced as axioms.
3.3. THE PROGRAMMING LOGIC $\lambda\omega_L$

3.23 Definition. AXIOM is the set of axioms containing

\[
\text{classic : } \forall P, \neg P \Rightarrow P,
\]
\[
AX_{\sigma \rightarrow \tau} : \forall f, g : \sigma \rightarrow \tau. (\forall x : \sigma. (f x) =_{\tau} (g x)) \Rightarrow f =_{\sigma \rightarrow \tau} g,
\]
\[
AX_{\Pi\alpha : K \cdot \sigma} : \forall f, g : (\Pi\alpha : K \cdot \sigma). (\forall \alpha : K. (f \alpha) =_{\sigma} (g \alpha)) \Rightarrow f =_{\Pi\alpha : K \cdot \sigma} g
\]

for all $\sigma \rightarrow \tau, (\Pi\alpha : K \cdot \sigma) \in \text{Cons}$. \qed

We lack the necessary quantifications to express axioms in AXIOM in a finite number of $\lambda\omega_L$-axioms. We could quantify over all datatypes $\sigma, \tau : \forall x$ in $AX_{\sigma \rightarrow \tau}$, but we cannot quantify over all kinds $K : \square x$ in $AX_{\Pi\alpha : K \cdot \sigma}$.

3.24 Lemma (Consistency of AXIOM in $\lambda\omega_L$).
False is not provable in a context containing only axioms from AXIOM.

Proof. See lemma 6.49. \qed

So it is safe to use classical logic in $\lambda\omega_L$, and to assume that equality of programs is extensional.
3.4 Program and Proof Development

The system $\lambda\omega_L$ has been defined so that the problem of program construction can be stated as follows:

given a \textit{datatype} $\sigma$, i.e. $\sigma : *$,
- a \textit{predicate} $P$ over that datatype, i.e. $P : \sigma \rightarrow *_p$

find
- a \textit{program} $M$ of type $\sigma$, i.e. $M : \sigma$
- a \textit{proof} $p_M$ that $M$ satisfies $P$, i.e. a proof $p_M : P M$.

A pair $(\sigma, P)$ consisting of a datatype and a predicate forms a specification. A pair $(M, p_M)$ consisting of a program $M : \sigma$ and proof $p_M : P M$ is a solution of this specification. We usually refer to the predicate $P$ or the proposition $P M$ as the specification.

The datatype $\sigma$ is only a partial specification. It gives some information about the program we want, for example that it should be a function from nat to nat, but not all of it. In the predicate $P$, however, all the required properties of the program can be expressed. It defines a subset of the datatype $\sigma$. This expressiveness comes at a price: in general it is not decidable whether a program $M$ satisfies a predicate $P$, whereas it is decidable whether it has type $\sigma$.

To show that $M$ satisfies $P$, a proof $p_M$ has to be supplied.

We can think of the $\lambda\omega_L$-proofs and predicates as annotation of the $\lambda\omega_L$-programs and datatypes. Programs are annotated with proofs that they satisfy certain properties; datatypes are annotated with predicates.

<table>
<thead>
<tr>
<th>$\lambda\omega_L$</th>
<th>$\lambda\omega_L$ annotation</th>
</tr>
</thead>
<tbody>
<tr>
<td>datatype $\sigma$, $\Gamma \vdash \sigma : *_s$</td>
<td>predicate $P$, $\Gamma \vdash P : \sigma \rightarrow *_p$</td>
</tr>
<tr>
<td>program $M$, $\Gamma \vdash M : \sigma : *_s$</td>
<td>proof $p_M$, $\Gamma \vdash p_M : (P M) : *_p$</td>
</tr>
</tbody>
</table>

Not only the datatypes, but also the other datatype-constructors can be annotated. This will be discussed later, in subsection 3.4.3.

Despite the fact that a program and its correctness proofs are separate objects, we should not first have to find a program and afterwards prove its correctness. Ideally, programs and their correctness proofs should be constructed hand in hand. In the remainder in this section we look at a strategy for the compositional development of programs and proofs. Here the program is constructed, together with its correctness proof, by stepwise refinement. For this, pairs of derivable inference rules are needed, consisting of

(i) a $\lambda\omega_L$-derivation rule, that gives the type of a program in terms of the types of its component parts, and

(ii) an associated $\lambda\omega_L$-derivation rule, that gives a proof that this program satisfies a specification in terms of proofs that its component parts satisfy certain specifications.

So (i) is a type derivation rule for programs, and (ii) is a type derivation rule for proofs. Such pairs of derivation rules, consisting of a type derivation rule and an associated proof rule, will be called \emph{coupled derivation rules}. These coupled derivation rules can be used to develop a program together with its correctness proof. For every programming language-construct there is usually a unique type inference rule. However, there may be more than one associated proof rule, for specifications of different forms.
A specification may have to be of a certain form in order to construct a program and its correctness proof together. For \(\lambda\text{omega}\)-rules for forming a datatype there are corresponding rules in \(\lambda\text{omega}_L\) for forming specifications on that datatype, which produce specifications of the right form.

So we are interested in pairs of inference rules, that can be used to derive types for pairs \((M, p_M)\), consisting of a program and a correctness proof, or for pairs \((\sigma, P)\), consisting of a datatype and a predicate.

Although in \(\lambda\text{omega}_L\) program and proof construction both come down to finding an inhabitant of a certain type, there are important practical differences. We do care which particular program \(M\) we find, whereas we do not care (as much) which particular proof \(p_M\) we find. This means we do not have to be able to read proof terms in the same way we want to read programs. The proof term \(p_M\) is usually much longer than the program \(M\). Indeed, proof terms quickly become too long to be readable, in which case they will usually be omitted.

### 3.4.1 Coupled derivation rules for function types

First we look for \(\lambda\text{omega}_L\)-proof rules to accompany the \(\lambda\text{omega}_L\)-type derivation rules for the introduction and elimination of function types. There are two programming language constructs involving function types, namely abstraction and application. In the examples below we consider how for programs of a certain form properties can be proved.

To make a clear distinction between judgements concerning programs and datatypes, and judgements concerning proofs and propositions, judgements \(\Gamma \vdash a : A\), where \(a\) and \(A\) are \(\lambda\text{omega}_L\)-terms - i.e. programs, datatype-constructors, or kinds - are written in boldface for the time being.

#### 3.25 Example (Abstraction).

Suppose we want a program \(f\) of type \(\sigma \to \tau\) satisfying a specification \((\forall x : \sigma. P x \Rightarrow Q x (f x))\), where \(\Gamma \vdash P : \sigma \to \ast_p\) and \(\Gamma \vdash Q : \sigma \to R \to \ast_p\).

So we want a program \(f\) and a proof \(p_f\) such that

\[
\Gamma \vdash f : \sigma \to \tau \quad \Gamma \vdash p_f : \forall x : \sigma. P x \Rightarrow Q x (f x)
\]

We can try a program of the form \((\lambda x : \sigma. M)\) for some \(M\). We then have to find a program \(M\) and a proof \(p_M\) such that

\[
\begin{align*}
(i) & \quad \Gamma, x : \sigma \vdash M : \tau \\
(ii) & \quad \Gamma, x : \sigma, p_x : P x \vdash p_M : Q x M
\end{align*}
\]

From (i) it follows that \((\lambda x : \sigma. M)\) has the right type and from (ii) it follows that it satisfies the specification

\[
\begin{align*}
\Gamma \vdash (\lambda x : \sigma. M) : \sigma & \to \tau \\
\Gamma \vdash (\lambda x : \sigma. \forall p_x. P x \Rightarrow Q x M) : \forall x : \sigma. P x \Rightarrow Q x ((\lambda x : \sigma. M)x)
\end{align*}
\]

#### 3.26 Example (Application).

Suppose we want a program \(M\) of type \(\tau\) satisfying the specification \(Q'M\), where \(\Gamma \vdash \tau \to \ast_p\), and \(\Gamma \vdash Q' : \tau \to \ast_p\). So we want a program \(M\) and a proof \(p_M\) such that

\[
\begin{align*}
\Gamma \vdash M : \tau \\
\Gamma \vdash p_M : Q'M
\end{align*}
\]
We can try a program of the form \( fN \), with \( N \) possibly occurring in the specification \( Q' \). Then for some \( \sigma : *_p, P : \sigma \rightarrow *_p \) and \( Q : \sigma \rightarrow \tau \rightarrow *_p \) such that \((QN) \models \beta \sigma Q' \) we have to find a program \( N \) with a proof \( p_N \) such that

\[
(i) \Gamma \vdash N \ \sigma \quad (ii) \Gamma \vdash p_N \ \ P \ N
\]

and a program \( f \) with a proof \( p_f \) such that

\[
(iii) \Gamma \vdash f : \sigma \rightarrow \tau \quad (iv) \Gamma \vdash p_f : \forall x : \sigma. \ P_\cdot \ x = \ Q_\cdot \ (f_\cdot \ x)
\]

From (i) and (iii) it follows that \( fN \) has the right type, and from (ii) and (iv) it follows that \( fN \) satisfies the specification \( Q' \):

\[
\Gamma \vdash fN : \tau \quad \Gamma \vdash p_f_\cdot \ N_\cdot \ P \cdot \ Q_\cdot \ (fN) \ \models \beta \sigma Q'(fN)
\]

In the previous example, the choice for a program of the form \((\lambda x : \sigma. \ M)\) was suggested by the type \( \sigma \rightarrow \tau \) of the program. The choice for a program of the form \((fN)\) is not suggested by just the shape of its datatype (rather like to the choice of proving a proposition \( \psi \) by proving \( \phi \Rightarrow \psi \) and \( \phi \) is not suggested by the shape of \( \phi \) ).

In the examples above the predicates (specifications) on function types \( \sigma \rightarrow \tau \) are of the form

\[
\lambda f : \sigma \rightarrow \tau. \ \forall x : \sigma. \ P_\cdot \ x = Q_\cdot \ (f_\cdot \ x) \quad (\sigma \rightarrow \tau) \rightarrow *_p
\]

where \( \Gamma \vdash P : \sigma \rightarrow *_p \) and \( \Gamma \vdash Q : \sigma \rightarrow \tau \rightarrow *_p \). Here \( P \) is the precondition, and \( Q \) the postcondition. Not all predicates on a function type \( \sigma \rightarrow \tau \) are of this form. However, all predicates that express some input-output relation (between input \( x \) and output \( f x \)) are of this form. Note that for predicates of this form, different choices for \( P \) and \( Q \) are possible (e.g. \( P' = \lambda x : \sigma. \ \text{True} \) and \( Q' = \lambda y : \sigma. \ \lambda y : \tau. \ P_\cdot \ x = Q_\cdot \ (f_\cdot \ x) \)). For the \( \lambda \omega_2 \)-derivation rule for forming function types there is a corresponding derivable \( \lambda \omega_2 \)-derivation rule for forming predicates of this form:

\[
\frac{\Gamma \vdash \sigma : *_p \quad \Gamma \vdash \tau : *_p}{\Gamma \vdash \sigma \rightarrow \tau : *_p} \quad \frac{\Gamma \vdash P : \sigma \rightarrow *_p \quad \Gamma \vdash Q : \sigma \rightarrow \tau \rightarrow *_p}{\Gamma \vdash (\lambda f : \sigma \rightarrow \tau. \ \forall x : \sigma. \ P_\cdot \ x = Q_\cdot \ (f_\cdot \ x)) : (\sigma \rightarrow \tau) \rightarrow *_p}
\]

For \( \Gamma \vdash \sigma : *_p, \tau : *_p, \ P : \sigma \rightarrow *_p, Q : \sigma \rightarrow \tau \rightarrow *_p \) the following coupled derivation rules for \( \rightarrow \)-introduction and elimination are derivable

\[
\frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash (\lambda x : \sigma. \ M) : \sigma \rightarrow \tau} \quad \frac{\Gamma, x : \sigma, p_\cdot : \ P_\cdot \ x = P_\cdot \ M \ \ Q_\cdot \ M}{\Gamma \vdash (\lambda x : \sigma. \ P_\cdot \ x = P_\cdot \ M) : (\forall x : \sigma. \ P_\cdot \ x = Q_\cdot \ ((\lambda x : \sigma. \ M)_\cdot \ x))} \quad \frac{\Gamma \vdash f : \sigma \rightarrow \tau \quad \Gamma \vdash p_f : (\forall x : \sigma. \ P_\cdot \ x = Q_\cdot \ (f_\cdot \ x))}{\Gamma \vdash p_f_\cdot \ N_\cdot \ P \cdot \ Q_\cdot \ (fN) \quad \Gamma \vdash fN : \tau}
\]

### 3.4.2 Coupled derivation rules for polymorphic types

We now discuss proof rules to accompany the introduction and elimination rules for a polymorphic type \((\Pi_\cdot \ A : \cdot \sigma. \ \tau)\)
For predicates on polymorphic data types we could consider predicates that have a form similar to that of the predicates on function types. This would mean that on a datatype \((\Pi \alpha : K \rightarrow * p)\) we have predicates of the following form:

\[ \lambda f : (\Pi \alpha : K \rightarrow * p) \forall \alpha \, K \, P \, \alpha \Rightarrow Q \, \alpha (f \alpha) : (\Pi \alpha : K \rightarrow * p) \]

where \(P : K \rightarrow * p\) and \(Q : (\Pi \alpha : K \rightarrow * p)\). However, there are few - if any - interesting predicates \(P\) on a kind \(K\). So instead we consider specifications of the form

\[ \forall (\alpha : \rightarrow \rightarrow ) \rightarrow f (f \alpha) \Rightarrow (\Pi \alpha : K \rightarrow * p) \]

where \(\alpha : K \Rightarrow Q : \rightarrow * p\). For such specifications we can find proof rules to accompany the introduction and elimination rules for a polymorphic type \((\Pi \alpha : K \rightarrow * p)\)

Note that the dependency of \(Q\) on \(\alpha\) is left "implicit". It could be made explicit by considering predicates \(Q\) with \(Q : (\Pi \alpha : K \rightarrow * p)\) instead of \(\alpha : K \Rightarrow Q : \rightarrow * p\). This would result in specifications of the form \(\lambda f : (\Pi \alpha : K \rightarrow * p) \forall \alpha : K Q \alpha (f \alpha)\). Our only reason for not doing this is that the dependency of \(\tau\) on \(\alpha\) is also implicit.

For the \(\lambda \omega\)-derivation rule for forming polymorphic types there is a corresponding derivable \(\lambda \omega L\)-derivation rule for forming specifications of the form (i):

\[ \Gamma, \alpha : \rightarrow \rightarrow \rightarrow * p \quad \Gamma, \alpha : K \Rightarrow \rightarrow \rightarrow \rightarrow \rightarrow * p \]

For \(\Gamma, \alpha : K \Rightarrow \rightarrow \rightarrow \rightarrow \rightarrow * p, Q : \rightarrow \rightarrow \rightarrow \rightarrow * p\) the following coupled derivation rules for \(\Pi\)-introduction and elimination are derivable:

\[ \Gamma, \alpha : K \Rightarrow M \rightarrow \tau * p \quad \Gamma, \alpha : K \Rightarrow \rightarrow \rightarrow \rightarrow \rightarrow * p \]

The inference rules above can be specialised for specifications of a certain form, namely where \((\forall \alpha : K \, Q (f \alpha))\) is of the form \((\forall \alpha : K \, \forall P : P \ldots)\), with \(P\) some prop-kind that possibly depends on \(\alpha\). This means the specification is of the form

\[ \lambda f : (\Pi \alpha : K \rightarrow * p) \forall \alpha : K \forall P : P \, Q (f \alpha) : (\Pi \alpha : K \rightarrow * p) \]

with \(\alpha : K, P : P \Rightarrow Q : \rightarrow * p\). Typically, if \(K\) is \(*\), i.e. \(\forall \alpha : K\) is a quantification over all datatypes, then \(\forall P : P\) will be a quantification over all predicates of a certain type.

For the \(\lambda \omega\)-derivation rule for forming polymorphic types there is a corresponding \(\lambda \omega L\)-derivation rule for forming predicates of the form (ii):

\[ \Gamma, \alpha : K \Rightarrow \rightarrow \rightarrow \rightarrow * p \quad \Gamma, \alpha : K \Rightarrow \rightarrow \rightarrow \rightarrow \rightarrow * p \]

\[ \Gamma, \alpha : K, P : P \Rightarrow \rightarrow \rightarrow \rightarrow * p \quad \Gamma, \alpha : K \forall P : P \, Q (f \alpha) \rightarrow * p \]
For $\Gamma; \alpha: \mathcal{K}, P, P \vdash \tau: \star, Q \quad \tau \rightarrow \star$, the following coupled derivation rules for $\Pi$-introduction and elimination are derivable

$$
\begin{align*}
\Gamma, \alpha : \mathcal{K} & \vdash M : \tau \\
\Gamma & \vdash (\lambda \alpha \mathcal{K}, M) : (\Pi \alpha : \mathcal{K}, \tau) \\
\Gamma, \alpha : \mathcal{K}, P, P & \vdash p_M Q M \\
\Gamma & \vdash (\lambda \alpha \mathcal{K}, \lambda P, P) \cdot \forall \alpha \mathcal{K} \forall P, P Q M \\
& \equiv_B \forall \alpha \mathcal{K} \forall P, P, Q((\lambda \alpha \mathcal{K}, M) \alpha)
\end{align*}
$$

$$
\begin{align*}
\Gamma & \vdash \rho : \mathcal{K} \\
\Gamma & \vdash f : (\Pi \alpha : \mathcal{K}, \tau) \\
\Gamma & \vdash f \rho : \tau[\alpha := \rho] \\
\Gamma & \vdash p_f \cdot \forall \alpha \mathcal{K} \forall P, P Q(f \alpha) \\
\Gamma & \vdash R : P[\alpha := \rho] \\
\Gamma & \vdash p_f R \cdot Q[\alpha := \rho][P := R](f \rho)
\end{align*}
$$

3.27 EXAMPLE The polymorphic identity

$$\text{id} = (\lambda \alpha \star, \lambda \tau \alpha, \tau) \quad (\Pi \alpha \star, \alpha \rightarrow \alpha)$$

satisfies the specification

$$\forall \alpha \star, \forall P \alpha \rightarrow \star, \forall \tau, \alpha, P x \Rightarrow P(\text{id} \alpha x)$$

Note that if we swap the second and third universal quantification, this becomes $\delta$-equal to

$$\forall \alpha \star, \forall x \alpha \Rightarrow \alpha =_\alpha (\text{id} \alpha x), \text{ with } =_\alpha \text{ as defined in definition 3.21.}$$

It follows from

$$\alpha \star, x \alpha \vdash x : \alpha$$

by the $\rightarrow$- and $\Pi$-introduction rules that id has type $(\Pi \alpha \star, \alpha \rightarrow \alpha)$. It follows from

$$\alpha : \star, P \alpha \rightarrow \star, \tau \alpha, P x \vdash P x \vdash P x$$

by the associated proof rules that id satisfies the specification mentioned above. These two derivations are:

$$
\begin{align*}
\alpha : \star, x \alpha \vdash x : \alpha & \quad \alpha : \star, P \alpha \rightarrow \star, \tau \alpha, P x \vdash P x \vdash P x \\
\vdash \text{id} : (\Pi \alpha \star, \alpha \rightarrow \alpha) & \quad \vdash \forall \alpha \star, \forall P \alpha \rightarrow \star, \forall \tau, \alpha, P x \Rightarrow P((\lambda \alpha \alpha x) \alpha)
\end{align*}
$$

More and larger building blocks than just abstraction and application will be used for programs. Associated type derivation rules are needed to type programs constructed using these building blocks, and associated proof rules are needed to prove correctness of programs.

We will give a simple example of the development of a program with its correctness proof. But first two examples are given that introduce two basic datatypes, booleans and natural numbers, and coupled derivation rules for them.
3.28 EXAMPLE (Booleans). The following context introduces the booleans:

```plaintext
bool : *s ,
true : bool ,
false : bool ,
if : \forall \alpha:*s , \alpha \to \alpha \to bool \to \alpha ,
P_{bool} : \forall \alpha:*s \forall P.bool \to \alpha \to *p ,
 p_{if} : \forall \alpha:*s \forall P.bool \to \alpha \to *p ,
   \forall \alpha \forall x P.true \to x \Rightarrow 
   \forall \alpha \forall x P.false \Rightarrow 
   \forall \alpha \forall x P. (if \ b \ then \ x \ else \ y)
```

This context assumes that the two booleans are distinct and gives the specification of if. We write \( (\text{if} \ b \ \text{then} \ x \ \text{else} \ y) \) for \((\text{if} \ (\neg b) \ \text{then} \ x \ \text{else} \ y) \) (true \&\& \&\& \text{false} \&\& \&\& \text{true}) , so the type parameter \( \alpha \) is left implicit. \text{false} \neq _{bool} \text{true} is short for \((\text{false} \neq _{bool} \text{true}) \) with \( \neg \) and \( =_{bool} \) as defined in definitions 3.11 and 3.21. Note that the specification of if is indeed of the form we discussed earlier.

Using \( p_{if} \) we can define the following proof \( p'_{if} \):

\[
p'_{if} = \lambda b, \alpha, Q, x, p_x, y, p_y : p_{if} (\lambda x:bool. \lambda a: \alpha. b =_{\text{bool}} b \Rightarrow Q a) x p_x y p_y
\]

This gives the following coupled derivation rules for if:

\[
\begin{array}{c}
\Gamma \vdash b : \text{bool} \\
\Gamma \vdash M : \sigma \\
\Gamma \vdash N : \sigma
\end{array}
\]

\[
\begin{array}{c}
\frac{}{\Gamma \vdash \text{if} \ b \ \text{then} \ M \ \text{else} \ N : \sigma} \\
\frac{}{\Gamma, M : Q \ M} \\
\frac{}{\Gamma, N : Q \ N}
\end{array}
\]

\[
\frac{}{\Gamma \vdash (p'_{if} \ b) \text{bool} Q M \ (\lambda p.M) N \ (\lambda p.N)) : Q(\text{if} \ b \ \text{then} \ M \ \text{else} \ N)}
\]

for \( \Gamma \vdash \sigma : *s \) and \( Q : \sigma \to *p \).

Here the proof terms have already become too complicated to read. In the following examples they will be omitted.

\[\square\]

3.29 EXAMPLE (Natural Numbers). The following context introduces the natural numbers and a primitive recursor with its specification:

```plaintext
nat : *s ,
0 : nat ,
S : nat \to nat ,
primrec \Pi \alpha:*s , \alpha \to (\text{nat} \to \alpha \to \alpha) \to \text{nat} \to \alpha ,
P_{primrec} \forall \alpha:*s \forall P.nat \to \alpha \to *p ,
   \forall \alpha \forall x P. 0 x \Rightarrow 
   \forall f : nat \to \alpha \to \alpha. (\forall n:nat. y:\alpha. P n y \Rightarrow P(Sn) (f n y)) \Rightarrow 
   \forall n:nat. P n (\text{primrec} \alpha x f n)
```

Note that the specification of primrec is indeed of the form discussed earlier. This specification results in the following coupled derivation rules for primrec:

\[ \Gamma \vdash M : \sigma \]
\[ \Gamma, n : \text{nat}, \text{rec} : \sigma \vdash N : \sigma \]
\[ \Gamma \vdash \text{primrec} \sigma M (\lambda n \text{nat} \lambda \text{rec} : \sigma N) : \text{nat} \to \sigma \]
\[ \Gamma \vdash p_M \quad P \circ M \]
\[ \Gamma, n : \text{nat}, \text{rec} : \sigma, p_{\text{rec}} : P \text{ rec} \vdash p_N \quad P (S n) N \]
\[ \Gamma \vdash \ldots .. f = \text{primrec} \sigma M (\lambda n \text{nat} \lambda \text{rec} : \sigma N) : \text{nat} \to \sigma \]
\[ \text{in } \forall \text{ nat}. \ P n (f n) \]

for \( \Gamma \vdash \sigma : * \) and \( P \cdot \text{nat} \to \sigma \to *_p \)

3.30 Example. Using the booleans and natural numbers introduced in the previous example we now construct a program that tests if a natural number is odd or even. For this the predicates \( \text{Even} \) and \( \text{Odd} \) and their relevant properties are declared:

\( \text{Even, Odd} : \text{nat} \to *_p, \)
\( a \circ 0 : \text{Even } 0, \)
\( a \circ 1 : \forall \text{ nat}. \text{Even } n \Rightarrow \text{Odd } (S n), \)
\( a \circ 2 : \forall \text{ nat}. \text{Odd } n \Rightarrow \text{Even } (S n), \)

We define

\[ P = \lambda n \text{nat} \lambda b \text{bool}. (\text{Even } n \land b =_{\text{bool} \text{true}}) \lor (\text{Odd } n \land b =_{\text{bool} \text{false}}) \]

It is easy to prove \( (P n \text{ true } \Leftrightarrow \text{Even } n) \) and \( (P n \text{ false } \Leftrightarrow \text{Odd } n) \). For the implication from left to right we need \( \text{false } \neq_{\text{bool} \text{true}} \).

We are looking for a program \( \text{even } \cdot \text{nat} \to \text{bool} \) that satisfies the specification \( \forall \text{ nat}. P n (\text{even } n) \), so we are looking for a program \( \text{even} \) and a proof \( p_{\text{even}} \) such that

\[ \vdash \text{even } \cdot \text{nat} \to \text{bool} \]
\[ \vdash p_{\text{even}}, \forall \text{ nat}. P n (\text{even } n) \]

We choose to use the primitive recursor primrec for this program, i.e., \( \text{even} \) will be of the form \( \text{primrec} \text{nat} M (\lambda n \text{nat} \lambda b 0 \text{bool} N) \) for certain \( M \) and \( N \). By the coupled derivation rules for primrec this leaves us with the task of finding programs \( M \) and \( N \) with proofs \( p_N \) and \( p_M \) such that

\[ \vdash M : \text{bool}, p_M : P \circ M \]
\[ n \cdot \text{nat}, b : \text{bool}, P n b \vdash N : \text{bool}, p_N, P (S n) N \]

\( P \circ M \equiv_{\text{Lb}} (\text{Even } 0 \land M =_{\text{bool} \text{true}}) \lor (\text{Odd } 0 \land M =_{\text{bool} \text{false}}) \), so we choose \( M =_{\text{true}} \). Then we have to prove \( P 0 \text{ true } \), which follows from \( \text{Even } 0 \).

We choose \( N \equiv_{\text{Lb}} (\text{if } b \text{ then } N_1 \text{ else } N_2) \) for some \( N1 \) and \( N2 \). This amounts to distinguishing the cases \( b \) is true and \( b \) is false, and by \( P n b \) this means distinguishing the cases that \( n \) is even and \( n \) is odd. We then have to find \( N_1 \) and \( N_2 \) with proofs \( p_{N_1} \) and \( p_{N_2} \) such that

\[ n \cdot \text{nat}, b : \text{bool}, p_b : P n b, p =_{\text{bool} \text{true}} \vdash N_1 : \text{bool}, p_{N_1}, P (S n) N_1 \]
3.4. PROGRAM AND PROOF DEVELOPMENT

and

\[ n : \text{nat}, b : \text{bool}, p_b : P n b, p : b =_{\text{bool}} \text{false} \vdash N_2 : \text{bool}, p_{N_2} : P (S n) N_2. \]

Finally, if \( P n b \) and \( b =_{\text{bool}} \text{false} \), then \( \text{Even} n \), and hence \( \text{Odd} (S n) \). Similarly, if \( P n b \) and

\[ b =_{\text{bool}} \text{false}, \text{then} \text{Odd} n, \text{and hence} \text{Even} (S n). \text{Odd} (S n) \text{is equivalent with} P (S n) \text{false}, \text{Even} (S n) \text{with} P (S n) \text{true}. \text{So we take} N_1 \equiv \text{false} \text{and} N_2 \equiv \text{true}, \text{and then proofs} p_{N_1} \text{and} p_{N_2} \text{can be found such that} \]

\[ n : \text{nat}, b : \text{bool}, p_b : P n b, p : b =_{\text{bool}} \text{true} \vdash p_{N_1} : P (S n) \text{false} \]

\[ n : \text{nat}, b : \text{bool}, p_b : P n b, p : b =_{\text{bool}} \text{false} \vdash p_{N_2} : P (S n) \text{true} \]

\[ \square \]

3.4.3 Other datatype-constructors

So far, we have only considered the annotation of programs and datatypes. Programs are annotated with (correctness) proofs, datatypes with predicates. In \( \lambda \omega \), there are other datatype-constructors besides the datatypes. We now consider how these can be annotated in \( \lambda \omega_L \).

These other datatype-constructors are functions for constructing datatypes, such as \( \text{list}: *_{\text{a}} \rightarrow *_{\text{a}}, \text{and} \times: *_{\text{a}} \rightarrow *_{\text{a}} \rightarrow *_{\text{a}} \). They can be annotated with functions for constructing predicates. For instance, the datatype-constructors \( \text{list}: *_{\text{a}} \rightarrow *_{\text{a}}, \) which maps datatypes to datatypes, could be annotated with a polymorphic function \( \text{LIST} \), that maps predicates to predicates:

\[ \text{LIST} : (\Pi \alpha: *_{\text{a}} \rightarrow *_{\text{a}}) \rightarrow (\text{list } \alpha) \rightarrow *_{\text{p}} \]

So for any datatype \( \alpha \), \( \text{LIST } \alpha \) maps a predicate on \( \alpha \) to a predicate on \( \text{list } \alpha \). The obvious choice for \( \text{LIST} \) is of course the function that maps a predicate \( P: \alpha \rightarrow *_{\text{p}} \) on \( \alpha \) to the predicate "\( P \) holds for all elements" on \( \text{list } \alpha \). This function \( \text{LIST} \) can be seen as a "lifted" version of \( \alpha \). Of course, not all interesting predicates on a datatype \( \text{list } \alpha \) are of the form

\[ \text{LIST } \alpha \ P \] for some \( P \), but some are. For example, we can expect that any polymorphic program \( f : (\Pi \alpha: *_{\text{a}} \rightarrow *_{\text{p}}) \rightarrow (\text{list } \alpha) \rightarrow *_{\text{p}} \) will satisfy

\[ \forall \alpha: *_{\text{a}}, \forall P: \alpha \rightarrow *_{\text{p}} . \forall l (\text{list } \alpha) . \text{LIST } \alpha \ P \ l \Rightarrow (\text{LIST } \alpha \ P \ f \ l) \].

This means that the list that is the output of \( f \) can only contain elements that occur in the list that is its input.

In the remainder of this section, it will be shown that, for any closed datatype-constructor \( \text{list}: *_{\text{a}} \rightarrow *_{\text{a}} \), in \( \lambda \omega \), there exists a lifted version \( \text{LIST} \) in \( \lambda \omega_L \) such that all closed programs \( f : (\Pi \alpha: *_{\text{a}} \rightarrow *_{\text{p}}) \rightarrow (\text{list } \alpha) \rightarrow *_{\text{p}} \) satisfy property (i). To do this, lifted versions of all datatype-constructors will be defined. In general, a datatype-constructor \( \sigma : K \) can be annotated by a lifted version, which is of type \( \text{type}_\text{of lift} \_G: (\sigma) \).

3.3.1 DEFINITION. For datatype-constructors \( \sigma \) of kind \( K \), with \( \Gamma \vdash \sigma : K \square_\sigma \), the \( \lambda \omega_L \)-propkind \( \text{type}_\text{of lift} \_G: (\sigma) \), with \( \Gamma \vdash \text{type}_\text{of lift} \_G: (\sigma) : \square_\sigma \), is defined as follows:

\[ \text{type}_\text{of lift} \_G: (\sigma) \equiv \sigma \rightarrow *_{\text{p}} \]

\[ \text{type}_\text{of lift} \_G: (\sigma) \equiv (\Pi \alpha: K \rightarrow \text{type}_\text{of lift} \_G: (\sigma \alpha)) \]

So \( \text{type}_\text{of lift} \_G: (\sigma) \equiv \Pi \alpha: *_{\text{a}} \rightarrow *_{\text{p}} \rightarrow (\text{list } \alpha) \rightarrow *_{\text{p}} \), which is indeed the type for \( \text{LIST} \) we gave earlier.
3.32 Example. The annotation of a datatype-construct \( \times \to * \to * \) would be of type

\[
type_{\flat} \Pi_{x} (x \to *_{p}) \to (\Pi \beta *_{p} (\beta \to *_{p}) \to (\alpha \times \beta) \to *_{p})
\]

where \( \times \) is written infix. So \( \times \) - a function that maps two datatypes to a datatype - can be annotated with a (polymorphic) function that maps two predicates to a predicate. The obvious candidate is the function which maps the predicates \( P \) on \( \alpha \) and \( Q \) on \( \beta \) to the predicate "\( P \) holds for the left component and \( Q \) for the right component" on \( \alpha \times \beta \).

For a closed datatype-construct \( \sigma \), it is possible to define a "lifted" version \( \text{lift}_\sigma \), a prop-constructor of type \( \text{type}_{\flat} \Omega_{\sigma} \), by induction on the structure of \( \sigma \).

3.33 Definition. For a datatype-construct \( \sigma \) the prop-constructor \( \text{lift}_\sigma \) is defined by

\[
\text{lift}_\sigma = P_\sigma \quad \text{if } \sigma \text{ is a variable}
\]

\[
\text{lift}_\sigma \Pi_{x} (x \to *) \equiv \lambda f (\Pi_{x} (x \to *)) \forall x. P_\sigma \to *_{p} P (f x)
\]

\[
\text{lift}_\sigma (\Pi_{x} (x \to *)) \equiv \lambda f (\Pi_{x} (x \to *)) \forall x. P_\sigma \to *_{p} (\Pi_{x} (x \to *)) \text{lift}_\sigma (f x)
\]

\[
\text{lift}_\sigma (\Pi^{\alpha} (\Pi_{\beta} (\Pi_{x} (x \to *))) \equiv \lambda f (\Pi^{\alpha} (\Pi_{\beta} (\Pi_{x} (x \to *)))) \forall x. P_\sigma \to *_{p} (\Pi^{\alpha} (\Pi_{\beta} (\Pi_{x} (x \to *)) \text{lift}_\sigma (f x))
\]

Here we assume that for every variable \( \alpha \in \text{Var}_\Omega \) there is a variable \( P_\alpha \in \text{Var}_\Omega \).

3.34 Example. For the datatypes \( (\Pi_{x} (x \to *)) \) and \( (\Pi^{\alpha} (\Pi_{x} (x \to *)) \to \alpha) \) we get

\[
\text{lift}_{\Pi^{\alpha} (\Pi_{x} (x \to *))} \equiv \lambda f (\Pi^{\alpha} (\Pi_{x} (x \to *)) \forall x. P_\sigma \to *_{p} (\Pi_{x} (x \to *)) \text{lift}_\sigma (f x)
\]

\[
\text{lift}_{\Pi^{\alpha} (\Pi_{x} (x \to *)) \to \alpha} \equiv \lambda f (\Pi^{\alpha} (\Pi_{x} (x \to *)) \forall x. P_\sigma \to *_{p} (\Pi^{\alpha} (\Pi_{x} (x \to *)) \text{lift}_\sigma (f x))
\]

3.35 Example. Suppose \( \text{list} : * \to * \) is a closed datatype-construct. Let \( \text{LIST} \equiv \text{lift}_{\text{list}} \). Then definition 3.33 results in the following predicate on \( (\Pi_{x} (x \to *)) \to (\text{list} \alpha) \)

\[
\text{lift}_{\Pi_{x} (x \to *)} (\Pi_{x} (x \to *)) \equiv \lambda f (\Pi_{x} (x \to *)) \forall x. P_\sigma \to *_{p} (\Pi_{x} (x \to *)) \text{lift}_\sigma (f x)
\]

\[
\text{lift}_{\Pi_{x} (x \to *)} (\text{list} \alpha) \equiv \lambda f (\Pi_{x} (x \to *)) \forall x. P_\sigma \to *_{p} (\Pi_{x} (x \to *) \text{lift}_\sigma (f x))
\]

3.36 Lemma. If \( \epsilon \vdash \sigma : \text{Var} \), then \( \epsilon \vdash \text{lift}_\sigma : \text{type}_{\flat} \Omega_{\sigma} \).

Proof. A straightforward induction on the structure of \( \sigma \) proves that if \( \Gamma \vdash \lambda \omega \alpha : \text{Var} \), then \( \text{lift}(\Gamma) \vdash \lambda \omega \text{lift}_\sigma \triangleq \text{type}_{\flat} \Omega_{\sigma} \).

Here we assume that for all variables \( \alpha \in \text{Var}_\Omega \) and \( x \in \text{Var}_\Omega \) there are variables \( P_\alpha \in \text{Var}_\Omega \), and \( p_\alpha \in \text{Var}_\Omega \).
3.4. PROGRAM AND PROOF DEVELOPMENT

This means that, for closed datatypes \( \sigma \), \( \text{lift}_\sigma : \text{type}_\omega \phi \) is a predicate on \( \sigma \). We already saw examples of such predicates in examples 3.34 and 3.35. All closed programs of type \( \sigma \) satisfy this predicate.

3.37 Theorem. If \( \epsilon \vdash M : \sigma : *_\pi \), then there is a proof \( p_M \) such that \( \epsilon \vdash p_M : (\text{lift}_\sigma M) \).

Proof. The proof \( p_M \) can be found by applying the \( \lambda \omega \)-derivation rules coupled to the \( \lambda \omega \)-derivation rules used in this derivation of \( M : \sigma \). A straightforward induction on the structure of \( M \) proves that if \( \Gamma \vdash \lambda \omega \alpha M : \sigma : *_\pi \), then \( \text{lift}(\Gamma) \vdash \lambda \omega \text{lift}_M : \text{lift}_\sigma M \), where

\[
\begin{align*}
\text{lift}_x & \equiv p_x \text{ if } x \text{ is a program variable} \\
\text{lift}_\alpha & \equiv P_\alpha \text{ if } \alpha \text{ is a datatype-constructor variable} \\
\text{lift}_{\lambda \tau \rho} M & \equiv \lambda x : \rho. \lambda p_x \text{ lift}_\rho x. \text{lift}_M \\
\text{lift}_{\lambda \rho \kappa} M & \equiv \lambda \alpha : \kappa. \lambda P_x : \text{type}_\omega \phi (\alpha). \text{lift}_M \\
\text{lift}_{MN} & \equiv \text{lift}_M N \text{ lift}_N \\
\text{lift}_{M\rho} & \equiv \text{lift}_M \rho \text{ lift}_\rho
\end{align*}
\]

Here we assume that for all variables \( \alpha \in \text{Var}_{\omega}^\pi \) and \( \pi \in \text{Var}_{\pi}^* \) there are variables \( P_\alpha \in \text{Var}_{\omega}^\pi \) and \( p_\pi \in \text{Var}_{\pi}^* \).

3.38 Example. In example 3.34 we saw that

\[
\begin{align*}
\text{lift}_{\Pi \alpha \pi} \alpha \equiv \lambda f : (\Pi \alpha : *_\pi. \alpha). \forall P. \alpha \rightarrow *_\rho \ P (f \alpha) \\
\text{lift}_{\Pi \alpha \pi} \alpha \rightarrow \alpha \equiv \lambda g : (\Pi \alpha : *_\pi. \alpha \rightarrow \alpha). \forall P. \alpha \rightarrow *_\rho \ \forall x : \alpha. P x \Rightarrow P (g \alpha x)
\end{align*}
\]

Now by theorem 3.37, for all closed programs \( f : (\Pi \alpha : *_\pi. \alpha) \) and \( g : (\Pi \alpha : *_\pi. \alpha \rightarrow \alpha) \) there are proofs of \( (\forall P. \alpha \rightarrow *_\rho. \ P (f \alpha)) \) and \( (\forall P. \alpha \rightarrow *_\rho. \ \forall x : \alpha. P x \Rightarrow P (g \alpha x)) \).

This means that, for a datatype \( \alpha \), \( g \alpha \) does not just map programs of type \( \alpha \) to programs of type \( \alpha \), but it also maps elements of any subset of \( \alpha \) to elements of that subset. This is also the case if this subset is a singleton subset, so this leaves only one possibility for \( g \alpha \), namely the identity on \( \alpha \).

Similarly, for a datatype \( \alpha \), \( f \alpha \) is not just a program of type \( \alpha \), but also an element of every subset of \( \alpha \), including the empty subset.Clearly, no such \( f \) can exist.

What theorem 3.37 is basically saying is that any subset of a \( \lambda \omega \)-datatype could be allowed as a new datatype. Theorem 3.37 does not say anything about the relation between programs \( f \rho \) and \( f \sigma \) that are obtained by applying a single polymorphic program \( f : (\Pi \alpha \kappa. \alpha) \) to different datatypes, like the notion of parametricity discussed in for instance [Rey83] [Wad89].
3.5 Comparison with Program Extraction in \( \lambda C \)

In [PM89b] Paulin-Mohring describes an approach to program construction that uses program extraction. This approach is quite different from the one we propose, as already discussed in the introduction. However, it involves closely related type systems, which is why we discuss it here in a bit more detail.

Program extraction is used in internal programming logics. Here the Curry-Howard-de Bruijn isomorphism is exploited by identifying the notions of program and proof and the notions of type and specification (to a certain extent). This idea dates back to Heyting's semantics of constructive proofs: a constructive proof \( p \) of \( \forall x. \sigma \) \( \vdash P \vdash Q x y \) contains an algorithm which, given a term \( x \) and a proof \( p_x \) of \( P x \), returns a term \( y \) and a proof \( p_y \) of \( Q x y \) (together, this witness \( y \) and proof \( p_y \) form a proof of \( \exists y. \tau \vdash Q x y \)). The type of \( p \) gives all the relevant information about this algorithm: it is its specification. Sufficiently expressive type systems, such as Martin-Löf's Type Theory and the Calculus of Constructions, can be used as programming logics in this way.

The main problem with this approach is that proofs contain redundant information. Typically, a large part of \( p \) is devoted to the computation of \( p_y \), and as programmers we are only interested in \( y \). As a result, \( p \) is inefficient and difficult to read.

One way to get rid of these irrelevant computations is to extract programs from proofs. In [PM89b] it is described how programs can be extracted from proofs in a variant of the Calculus of Constructions. The extracted programs are typable in \( \lambda \omega \). For example, a \( \lambda \omega \)-program \( f : \sigma \to \tau \) satisfying \( \forall x. \sigma \vdash P \vdash Q x (f x) \) is extracted from a constructive proof of \( \forall x. \sigma \vdash P \vdash (\exists y. \tau \vdash Q x y) \). The proofs from which programs are extracted are constructed in the following variant of the Calculus of Constructions:

3.39 Definition \( \lambda C_{\text{ps}} \) is the PTS specified by

\[
S = \{*, \mathbb{C}_s, *, \mathbb{P}_s, \mathbb{P}_p\}, \quad A = \{*, \mathbb{C}_s, *, \mathbb{P}_s : \mathbb{P}_p\}, \quad R = S \times S
\]

In [PM89b] the sort \( * \) of \( \lambda C_{\text{ps}} \) is called Spec, and \( *_p \) is called Prop.

In this system, we can no longer think of all types \( * \) as datatypes, nor of all terms \( M : \sigma \) as programs. For example, it is possible to form a program-dependent-type such as \((\leq n \cdot m) *_s\), where \( \leq \cdot \text{nat} \to \text{nat} \to *_s\), that consists of (constructive) proofs that \( n \) is less than \( m \). Inhabitants of \( *_s \) are called informative propositions, and inhabitants of \( *_p \) are called non-informative propositions.

The distinction between \( *_s \) and \( *_p \) is needed to control which parts of a proof are extracted to produce a program. The extraction procedure discards proofs of non-informative propositions, and keeps only the proofs of informative propositions. For instance, in order to extract a program of type \( \sigma \to \tau \) from a proof of \( \forall x. \sigma \vdash P x \to (\exists y. \tau \vdash Q x y) \), the types \( \sigma \) and \( \tau \) have to be informative, i.e. \( \sigma, \tau \to *_s \), and the types \( P x \) and \( Q x y \) have to be non-informative, i.e. \( P x, Q x y : *_p \).

The extraction procedure uses two mappings, \( E \) and \( R \). The function \( E \) extracts programs and datatypes from \( \lambda C_{\text{ps}} \)-proofs and propositions, the function \( R \) extracts the associated correctness proofs and predicates.
3.5. COMPARISON WITH PROGRAM EXTRACTION IN $\lambda C$

3.40 Theorem ([PM89b]). There are mappings $\mathcal{E}$ and $\mathcal{R}$ such that:

- if $\Gamma \vdash s : *_s$ in $\lambda C_{ps}$, then
  \[ \mathcal{E}(\Gamma) \vdash \mathcal{E}(s) : *_s \text{ in } \lambda \omega_s, \text{ and} \]
  \[ \mathcal{R}(\Gamma) \vdash \mathcal{R}(s) : \mathcal{E}(s) \rightarrow *_p \text{ in } \lambda \omega_L \text{ extended with the rule } (*_p, \Box_p). \]
- if $\Gamma \vdash s : *_s$ in $\lambda C_{ps}$, then
  \[ \mathcal{E}(\Gamma) \vdash \mathcal{E}(s) : \mathcal{E}(S) \text{ in } \lambda \omega_s, \text{ and} \]
  \[ \mathcal{R}(\Gamma) \vdash \lambda \omega_L \mathcal{R}(s) : \mathcal{R}(S) \mathcal{E}(s) \text{ in } \lambda \omega_L \text{ extended with the rule } (*_p, \Box_p). \]

In [PM89b] the sort $*_s$ of $\lambda \omega_s$ is called Data. □

So if $S$ is an informative proposition, then $\mathcal{E}(S)$ is a datatype and $\mathcal{R}(S)$ is a predicate on that datatype. If $s$ is a constructive proof of an informative proposition $P$, then $\mathcal{E}(s)$ is a program of type $\mathcal{E}(S)$ and $\mathcal{R}(s)$ is a proof that this program satisfies the predicate $\mathcal{R}(s)$.

The example below shows how correctness proof and program are intertwined in a constructive proof.

3.41 Example. Suppose $\Gamma \vdash \sigma, \tau : *_s$, $\Gamma \vdash \Pi : \sigma \rightarrow *_p$ and $\Gamma \vdash Q : \sigma \rightarrow \tau \rightarrow *_p$ in $\lambda \omega_L$ (and hence in $\lambda C_{ps}$). Define the informative $\lambda C_{ps}$-proposition $S$ as follows

\[ S = \forall x : \sigma. \Pi x \Rightarrow (\exists y : \tau. Q x y) : *_s. \]

Then

\[ \mathcal{E}(S) = \sigma \rightarrow \tau \]
\[ \mathcal{R}(S) = \lambda f : \sigma \rightarrow \tau. \forall x : \sigma. \Pi x \Rightarrow Q x (f x) \]

Suppose that $M$ is a $\lambda \omega_s$-term such that $\Gamma, x : \sigma \vdash M : \tau$. Suppose that in $\lambda C_{ps}$ we have the following inhabitant of $S$

\[ s = \lambda x : \sigma. \lambda p : \Pi x. \lambda q : \tau. \exists y : Q x y. M p M : S, \]

where $\exists y : Q x y. M p M$ is a proof of $(\exists y : \tau. Q x y)$ consisting of a witness $M$ and a proof $p_M : Q x M$. Then

\[ \mathcal{E}(s) = \lambda x : \sigma. M : \mathcal{E}(S) \]
\[ \mathcal{R}(s) = \lambda x : \sigma. \lambda p : \Pi x. \lambda q : \tau. \mathcal{E}(s) \mathcal{R}(s) : \mathcal{R}(S) \mathcal{E}(s) \]

3.42 Theorem. Any program $M : \sigma \rightarrow *_p$ and correctness proof $p_M : S M : *_p$ that can be constructed in $\lambda \omega_L$ can also be obtained by program extraction from a proof of an informative proposition in $\lambda C_{ps}$.

Proof. The simplest way is to take as the $\lambda C_{ps}$-proposition $(\exists x : \sigma. S x) : *_s$, and as its (constructive) proof the pair consisting of the witness $M$ and proof $p_M$ that it is indeed a witness.

Note that this is not the only way, and not the best. There are many proofs of different informative propositions from which a certain program and correctness proof can be extracted. For example, a program $f : \sigma \rightarrow \tau$ satisfying $\forall x : \sigma. P x \Rightarrow Q x (f x)$ can be extracted from a proof of $\forall x : \sigma. P x \Rightarrow (\exists y : \tau. Q x y)$ or $\exists f : \sigma \rightarrow \tau. P \tau \Rightarrow Q x (f x)$ The whole idea behind using program extraction is that we prefer to prove the former, To prove the latter we have to provide a program with the witness and a separate correctness proof, so in this case there is no real need for an extraction procedure to obtain these from the proof. □
Not all programs and correctness proofs that are obtained by program extraction from a \( \lambda C_{ps} \)-proof can be constructed in \( \lambda \omega_L \). This is because \( R \) produces predicates and correctness proofs that are typeable in \( \lambda \omega_L \) extended with \( (\#_p, \square_p) \). This extra rule allows the formation of propositions depending on proofs, i.e. propositions that express properties of proofs. However, using this rule goes against the idea that the inhabitants of \( *_p \) are non-informative propositions, whose proofs do not have any computational meaning.
Chapter 4

Simple Extensions

Like all PTSs, the systems introduced in the previous chapter provide only very few primitives for term and type formation. In this chapter they are extended with more type constructors. In addition to the dependent product type constructor \( \Pi \), we introduce the type constructors \( \times \), \(+\) and \( \Sigma \), for the formation of (labelled) cartesian products, (labelled) disjoint sums, and weak dependent sums, respectively.

Especially in the programming language we want more primitives for term and type formation than those available in \( \lambda \omega \). We want more datatypes than just polymorphic types \((\Pi \alpha : K. \sigma)\) and function types \(\sigma \rightarrow \tau\), and more ways of constructing programs than just lambda abstraction and application. The extensions provide a richer syntax for the programming language. The labelled products and sums provide record and variant types. The dependent sums provide abstract datatypes.

In the logic the new type constructors provide the logical connectives conjunction, disjunction and existential quantification as primitives. In the logic there is not such a pressing need for more primitives for terms and types as in the programming language. Readability of proof terms is not as important as readability of programs. Also, we are not interested in the reduction behaviour of proofs.

The strength of the type systems is not really increased by the new type constructors. There are encodings of all the new types in the original systems, except for the labelled products and sums. There are several reasons for introducing \(+\), \(\times\) and \(\Sigma\) as primitive notions. Having them as primitives means that we can choose their interpretations in a model (which may be different from the interpretations of their encodings), which makes it easier to introduce specific axioms for them in the logic. Also, if \(+\), \(\times\) and \(\Sigma\) are primitives, they can be implemented more efficiently. Finally, there is no way to encode labels and labelled products and sums in \(\lambda \omega_L\).

The new primitives do not introduce new dependencies between the different levels, so that the hierarchy formed by these levels does not change.

Before we extend the particular type systems with \(+\), \(\times\) and \(\Sigma\), we first consider in section 4.1 how the new type constructors can be included in the PTS-framework. Then in sections 4.2 and 4.3 the programming language \(\lambda \omega\), and the programming logic \(\lambda \omega_L\) are extended with \(+\), \(\times\) and \(\Sigma\). The resulting system are called \(\lambda \omega^+_L\) and \(\lambda \omega^*_L\). Finally, in section 4.4 we consider the construction of programs with their correctness proofs.
4.1 Extending PTSs with +, × and Σ

In this section the PTS-framework is extended to include more types than just the dependent product types (Πx:A, B), namely

- cartesian product types A × B and labelled cartesian products,
- disjoint sum types A + B and labelled disjoint sums,
- dependent sum types (Σx:A, B) (also known as existential or weak sum types)

We do not intend to give the most general extension of PTSs with these additional type constructors, only one that is general enough for our purposes. In particular, for + and Σ-types more powerful elimination rules can be given. The different type constructors are treated as uniformly as possible. We compare different notations for + and Σ-types, and choose one which emphasizes the similarity between them. Later we may use one of the other notations if this is easier to read in a particular situation.

In the specification (S, A, R) of a PTS the set of rules R specifies which Π-types can be formed. For every new type constructor an additional set of rules will be required to specify which types can be formed with it. The set of rules R controlling the formation of Π-types will be called RΠ from now on.

4.1 Definition.
A specification of a (D)PTS with +, × and Σ is a 6-tuple (S, A, RΠ, RΣ, R×, R+) with

- S is a set of symbols called the sorts
- A ⊆ S × S,
- RΠ, RΣ ⊆ S × S,
- R×, R+ ⊆ S.

If S = (S, A, RΠ, RΣ, R×, R+) is a specification, then λS denotes the PTS with +, × and Σ it specifies, and λΣ denotes the DPTS with +, × and Σ it specifies.

One simplification compared with the original definition of a PTS-specification (definition 2.1) is that RΠ ⊆ S × S instead of RΠ ⊆ S × S × S. For the system we are interested in no rules (s1, s2, s3) with s2 ≠ s3 are needed to control the formation of Π-types (or Σ-types, for that matter). As a result, the definition of functional can be simplified:

4.2 Definition. A (system specified by s) specification (S, A, RΠ, RΣ, R×, R+) is called functional if A is a function, i.e. if

(s, s') ∈ A ∧ (s, s'') ∈ A ⇒ s' = s''.

Extending a PTS or DPTS with +, × and Σ-types comes down to

- extending the set of pseudoterm with new language constructs.
4.1. EXTENDING PTSs WITH +, × AND Σ

- adding new reduction rules, and
- adding new type inference rules.

The extension with +, × or Σ can be defined simultaneously for PTSs and DPTSs. In the remainder of this section we give for each individual type constructor the new pseudoterms, reduction rules and inference rules. The (binary) cartesian products $A \times B$ and disjoint sums $A + B$ are special cases of the labelled ones. Because they are so much more familiar they are first treated separately.

Each new type constructor comes with its β- and η-reduction rules. As in the definition of PTSs in chapter 2, we will only have β-reduction in the type systems. The reason is that, as in chapter 2, the η-rules complicate matters because they destroy the Church-Rosser property for the pseudoterms. Also, for labelled products the η-rule will turn out to be a conditional rule that depends on the typing relation. The models that are discussed later will be extensional and respect η-equality.

4.1.1 Cartesian Products

Cartesian product types are of the form $A \times B$. The type $A \times B$ is the type of pairs consisting of a term of type $A$ and a term of type $B$. The associated term constructions are pairing and projection. The pair consisting of $a$ and $b$ is denoted by $(a, b)$. The first component of a pair $c$ is denoted by $c.1$, the second by $c.2$. The formation of product types is controlled by a set of rules $R^X \subseteq S$. The type $A \times B$ can be formed only for types $A$ and $B$ that inhabit a sort $s \in R^X$.

4.3 DEFINITION (Extension of (D)PTS with Cartesian Products).

The extension of a (D)PTS with cartesian products types is specified by a set of rules $R^X \subseteq S$. The set of pseudoterms is extended as follows:

$$T ::= .. | T \times T | (T, T) | T 1 | T 2 .$$

The following reduction rule is added:

$$(a_1, a_2).s \triangleright_\beta a_1 ,$$

and the following type inference rules:

\[
\begin{align*}
  (\times \text{form}) & \quad \frac{\Gamma \vdash A : s \quad \Gamma \vdash B : s}{\Gamma \vdash A \times B : s} \quad \text{if } s \in R^X \\
  (\times \text{intro}) & \quad \frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B \quad \Gamma \vdash A \times B : s}{\Gamma \vdash (a, b) : A \times B} \\
  (\times \text{elim1}) & \quad \frac{\Gamma \vdash c : A \times B}{\Gamma \vdash c.1 : A} \\
  (\times \text{elim2}) & \quad \frac{\Gamma \vdash c : A \times B}{\Gamma \vdash c.2 : B}
\end{align*}
\]

The η-rule for products is $(c.1, c.2) \triangleright_\eta c$. As is well known, the combination of β-reduction with this rule — known as surjective pairing — is not Church-Rosser for the untyped lambda calculus, and so it is also not Church-Rosser on the set of pseudoterms.
4.1.2 Disjoint Sums

Before we give the definition of (D)PTSs with disjoint sum types, we first discuss some of the possible alternatives for the syntax.

Disjoint sum types are of the form \( A + B \). The formation of disjoint sums is controlled by a set of rules \( R^+ \subseteq S \), in the same way the formation of product types is controlled by \( R^\times \). The formation rule for \(+\)-types is

\[
\frac{\Gamma \vdash A : a \quad \Gamma \vdash B : b}{\Gamma \vdash A + B : a + b} \quad \text{if } a, b \in R^+
\]

The disjoint sum or discriminated union of two type \( A \) and \( B \), \( A + B \), is the union of two disjoint copies of \( A \) and \( B \). Informally, its inhabitants can be seen as pairs \((1, a)\) and pairs \((2, b)\) with \( a \) of type \( A \) and \( b \) of type \( B \). For sum types we have two introduction rules:

\[
\frac{I \vdash p : A + B}{I \vdash p : A + B} \quad \frac{I \vdash a : A \quad I \vdash b : B}{I \vdash \text{in}_{A+B} (\downarrow a) : A + B}
\]

The subscript \( A + B \) of \( \text{in} \) is awkward but necessary for type inference. We will sometimes omit these subscripts if it is clear from the context what they should be. For instance, if we know that \( f : A + B \rightarrow C \), then the subscript \( A + B \) could be omitted in the term \( f(\text{in}_{A+B} 1 \ a) \).

The parameter \( a \) in \( \text{in}_{A+B} 1 \ a \) could be treated as the argument in an ordinary application. Then the injection \( \text{in}_{A+B} 1 \) would be typable without its argument of type \( A \), namely as

\[
\Gamma \vdash \text{in}_{A+B} 1 : A + B
\]

However, this is only possible if the function type \( A \rightarrow A + B \) can be formed, which requires \((a, s) \in R^\downarrow\). One could go one step further, and treat \( \text{in}_{A+B} 1 \) as the selection of the first component of a pair. Then the injection into the sum type \( A + B \) would be typed as

\[
\Gamma \vdash \text{in}_{A+B} : (A \rightarrow A + B) \times (B \rightarrow A + B)
\]

But this is only possible if the product type \((A \rightarrow A + B) \times (B \rightarrow A + B)\) can be formed, which not only requires \((a, s) \in R^\downarrow\), but also \( s \in R^\times \). In the systems we consider it will be possible to type the injection \( \text{in}_{A+B} \) without its two arguments.

The elimination principle for a disjoint sum type involves a case distinction between terms constructed using the left injection and those constructed using the right injection. One possibility is to use a case-expression, with the inference rule

\[
(i) \quad \frac{\Gamma, x : A \vdash c_1 : C \quad \Gamma, y : B \vdash c_2 : C \quad I \vdash d : A + B}{\Gamma \vdash (\text{case } d \text{ of } \text{in} 1 x \mapsto c_1 \mid \text{in} 2 y \mapsto c_2 \text{ esac}) : C}
\]

and reduction rules

\[
(\text{case } \text{in}_{A+B} 1 \ a) \text{ of } \text{in} 1 x \mapsto c_1 \mid \text{in} 2 y \mapsto c_2 \text{ esac} \quad \text{D} \quad c_1[x := a] \\
(\text{case } \text{in}_{A+B} 2 \ b) \text{ of } \text{in} 1 x \mapsto c_1 \mid \text{in} 2 y \mapsto c_2 \text{ esac} \quad \text{D} \quad c_2[y := b] \\
(\text{case } c \text{ of } \text{in} 1 x \mapsto (\text{in}_{A+B} 1 \ i) \mid \text{in} 2 y \mapsto \text{in}_{A+B} 2 \ y \text{ esac}) \quad \text{D} \quad c
\]
4.1. EXTENDING PTSs WITH +, × AND Σ

case is a binding operator: in the term (case c of (in.1 x) ⊸ c₁ | (in.2 y) ⊸ c₂ esac) it binds
x in c₁ and y in c₂. If we use lambda-abstraction for these bindings, we obtain a less verbose
notation for the elimination principle for sum types:

\[ (\text{\textbf{ii}) } \Gamma \vdash f : A \to C \quad \Gamma \vdash g : B \to C \quad \Gamma \vdash A + B : s \quad \Gamma \vdash f \circ g : A + B \to C \]

\( f \circ g \) is the function that maps a term \((\text{in}_{A+B}.1 \ a)\) to \(a\), and a term \((\text{in}_{A+B}.1 \ b)\) to \(\text{g \ b}\). The
computation rules for \(f \circ g\) are

\[ f \circ g \; (\text{in}_{A+B}.1 \ a) \; \triangleright_{\beta} \; f \; a \]

\[ f \circ g \; (\text{in}_{A+B}.2 \ b) \; \triangleright_{\beta} \; g \; b \]

The \(\eta\)-rule for \(f \circ g\) is easiest to state in terms of \(\text{in}_{A+B}.1\) and \(\text{in}_{A+B}.2\):

\[ (\text{in}_{A+B}.1 \; \triangleright \; \text{in}_{A+B}.2) \; c \; \triangleright_{\eta} \; c \]

The term (case \(d\) of \(\text{in}.1 \ x \mapsto c₁ \mid \text{in}.2 \ y \mapsto c₂ \; \text{esac}\)) can easily be expressed in terms of \(\triangleright\),
namely as \(((\lambda x : A. \; c₁) \triangleright (\lambda y : B. \; c₂)) \; d\). Depending on the situation, the notation using case or
\(\triangleright\) may be preferable. Sometimes the case-construct is a little easier to read, for example in
the \(\eta\)-rule. On the other hand, the more compact notation using \(\triangleright\) is useful to express some
equalities of functions on sum types, e.g.

\[ h_{\circ}(f \circ g) =_{\rho₁ + \rho₂ = \sigma} (h_{\circ}f) \triangleright (h_{\circ}g) \]

where \(f : \rho₁ \to \sigma\), \(g : \rho₂ \to \sigma\) and \(h \; \sigma \to \tau\).

There is subtle difference between the elimination rules (i) and (ii) given above, namely
in the restrictions they impose on the possible choices for \(C\). Rule (ii) is more restrictive
than rule (i). In (ii) it follows from the premisses that the types \(A \to C\) and \(B \to C\) can be
formed, which means that \(\Gamma \vdash C \cdot s\) for some \((s, s') \in \mathbb{R}^{1}\). In (i) on the other hand nothing
is required of \(C\). We will require that the domain and the range of \(f \circ g\) have the same sort:

\[ (\text{\textbf{iii}) } \Gamma \vdash f : A \to C \quad \Gamma \vdash g : B \to C \quad \Gamma \vdash A + B : s \quad \Gamma \vdash C \cdot s \quad \Gamma \vdash f \circ g : A + B \to C \]

There are two ways to generalise this elimination rule, but these generalisations will not be
included. One possibility is to allow the range of \(f \circ g\) to be of another sort than its domain.
Another is to allow \(f \circ g\) to have a dependent type. The most liberal elimination rule for
\(\circ\)-types, combining these two possibilities, is

\[ \Gamma, x : A \vdash c₁ : C[z := \text{in}_{A+B}.1 \; x] \quad \Gamma, y : B \vdash c₂ : C[z := \text{in}_{A+B}.2 \; y] \quad \Gamma \vdash d : A + B \quad \Gamma, z : A + B \vdash C : s \]

\[ \Gamma \vdash (\text{case } d \text{ of } \text{in}.1 \; \triangleright \; c₁ \mid \text{in}.2 \; \triangleright \; c₂ \; \text{esac}) : C[z := d] \]

Later, in discussion 4.38, we will discuss possible uses of these generalisations and our reasons
for excluding them.

Instead of the binary operator \(\triangleright\) we will use a unary one that takes a pair as argument.
Then \(f \circ g\) is in fact \(\triangleright(f, g)\), and the elimination rule becomes:

\[ (\text{\textbf{+elim}) } \Gamma \vdash h : (A \to C) \times (B \to C) \quad \Gamma \vdash A + B : s \quad \Gamma \vdash C \cdot s \quad \Gamma \vdash \triangleright h : A + B \to C \]
CHAPTER 4  SIMPLE EXTENSIONS

This rule is only equivalent with the rule (iii) if the product \((A \rightarrow C) \times (B \rightarrow C)\) can be formed, which requires \(s \in R^\times\). In the systems we consider this will not be a problem, since we will always have \(R^\times = R^+\). The only reason for using the unary \(\nabla\) is that it is easy to generalise to \(n\)-ary sums and labelled sums. It is also more similar to the notation used for \(\Sigma\)-types.

The \(\beta\)-reduction rule becomes

\[
\nabla h \ (\text{in}_{A+B} \ 1 \ b) \quad \eta \quad h \ . \ b
\]

The term \(\nabla (f, g)\) has the expected reduction behaviour, except that now two steps are needed instead one:

\[
\nabla (f, g) \ (\text{in}_{A+B} \ 1 \ a) \quad \eta \quad (f, g).1 \ a \quad \eta \quad f \ a
\]

\[
\nabla (f, g) \ (\text{in}_{A+B} \ 2 \ b) \quad \eta \quad (f, g).2 \ b \quad \eta \quad g \ b
\]

The \(\eta\)-rule for \(\nabla\) is easiest to state in terms of \(\text{in}_{A+B}\)

\[
\nabla \text{in}_{A+B} \ c \quad \eta \quad c
\]

4.4 Definition (Extension of (D)PTS with Disjoint Sums)

The extension of a (D)PTS with disjoint sum types is specified by a set of rules \(R^+ \subseteq S\). The set of pseudoterm is extended as follows

\[T := \cdot \ | T + T \ | \text{in}_{T+T} \ 1 \ T \ | \text{in}_{T+T} \ 2 \ T \ | \nabla \ T\]

The following reduction rule is added

\[
\nabla h \ (\text{in}_{A+B} \ 1 \ a) \quad \eta \quad h \ . \ a \quad \text{for } i \in \{1, 2\}
\]

and the following type inference rules:

\[
\begin{align*}
(+\text{form}) & \quad \Gamma \vdash A : s \quad \Gamma \vdash B : s \\
(+\text{intro1}) & \quad \Gamma \vdash A + B : s \quad \Gamma \vdash A \cdot A \\
(+\text{intro2}) & \quad \Gamma \vdash A + B : s \quad \Gamma \vdash B \quad B \\
(+\text{elim}) & \quad \Gamma \vdash h : \{(A \rightarrow C) \times (B \rightarrow C)\} \quad \Gamma \vdash A + B : s \quad \Gamma \vdash C : s \\
\end{align*}
\]

4.5 Convention  Of the type constructors \(-\), \(+\), and \(\times\), the type constructor \(-\rightarrow\) has the lowest priority and \(\times\) the highest.

4.1.3 Dependent Sums

As for the disjoint sum types, before we give the definition of PTSs extended with dependent sum types, we first discuss some of the alternatives.

Dependent sum types are of the form \((\Sigma r : A \ B)\). The type constructor \(\Sigma\) can be seen as an infinitary version of \(+\), the type \(B_1 + B_2\) is "\(\Sigma t \in \{1, 2\} \ B_t\)." Like inhabitants of \(B_1 + B_2\)
are pairs \((i, b)\) consisting of an index \(i \in \{1, 2\}\) and a term \(b : B_i\), inhabitants of \((\Sigma x : A. B)\) are essentially pairs \((a, b)\) consisting of a term \(a : A\) and a term \(b : B[x := a]\).

There are (at least) two kinds of \(\Sigma\)-types, known as weak and strong \(\Sigma\)-types, with different elimination rules. The \(\Sigma\)-types we use are the weak ones. The difference with the strong \(\Sigma\)-types are explained at the end of this section.

In the programming language \(\Sigma\)-types can be used as abstract datatypes, as explained in [MP84]. Examples of this are given in examples 4.25 and 4.27. As a logical connective, \(\Sigma\) is simply the existential quantifier \(\exists\). The rules for \(\Sigma\)-types look most familiar if \(\Sigma\) is read as \(\exists\); the introduction and elimination rule for \(\Sigma\) are then the usual introduction and elimination rule for an existential quantification.

The formation of dependent sums is controlled by a set \(R^\Sigma\), with \(R^\Sigma \subseteq S \times S\). The formation rule for \(\Sigma\)-types is:

\[
\frac{\Gamma \vdash A : s_1 \quad \Gamma, x : A \vdash B : s_2}{\Gamma \vdash (\Sigma x : A. B) : s_2}
\]

if \((s_1, s_2) \in R^\Sigma\)

There will be no need to generalise this by having rules that are triples \((s_1, s_2, s_3)\) instead of pairs \((s_1, s_2)\) and replacing \(s_2\) in the conclusion by \(s_3\).

The introduction rule for \(\Sigma\)-types is:

\[
\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B[x := a]}{\Gamma \vdash \textsf{in}_{\Sigma x : A B} a b : (\Sigma x : A. B)}
\]

If we read \(\exists\) for \(\Sigma\), then the rule above becomes the usual introduction rule for existential quantification: to prove \((\exists x : A. B)\) we have to provide a witness \(a : A\) with a proof of \(B[x := a]\). The term \((\textsf{in}_{\Sigma x : A B} a b)\) can be seen as a pair \((a, b)\). However, the elimination rule for \(\Sigma\)-types will not allow direct access to the two components \(a\) and \(b\) of an inhabitant \((\textsf{in}_{\Sigma x : A B} a b)\) of a \(\Sigma\)-type.

As for the \(\Sigma\)-types, the injection into a \(\Sigma\)-type could be typed without its two arguments,

\[
\textsf{in}_{\Sigma x : A B} : (\Pi x : A. B \rightarrow (\Sigma x : A. B))
\]

provided that this type can be formed. If \((\Sigma x : A. B)\) has been formed using \((s_1, s) \in R^\Sigma\), then we need \((s_1, s)\). \((s, s) \in R^\Sigma\) to form the type \((\Pi x : A. B \rightarrow (\Sigma x : A. B))\).

As for \(\Sigma\)-types, there are different ways to express the elimination principle for \(\Sigma\)-types. One way, similar to the case-expression for \(\Sigma\)-types, is a where-expression with the typing rule

\[
\frac{\Gamma, x : A, y : B \vdash c : C \quad \Gamma \vdash d : (\Sigma x : A. B) \quad \Gamma \vdash C : s}{\Gamma \vdash (\text{where} \ (x \ y) = d) : C}
\]

and reduction rules

\[
\begin{align*}
\text{c where } (x \ y) = (\text{in}_{\Sigma x : A B} a b) & \Rightarrow_B c[x := a][y := b] \\
\text{c where } (x \ y) = (\text{in}_{\Sigma x : A B} x y) & \Rightarrow_B \text{c}
\end{align*}
\]

where \(\Rightarrow_B\) is a binding operator; in the term \((c \ (x \ y) = d)\) it binds \(x\) and \(y\) in \(c\). Using lambda-abstraction for these bindings produces an operator similar to the \(\nabla\) for \(\Sigma\)-types, with the following typing rule:

\[
\frac{\Gamma \vdash f : (\Pi x : A. B \rightarrow C) \quad \Gamma \vdash (\Sigma x : A. B) \quad s \quad \Gamma \vdash C : s}{\Gamma \vdash \nabla f : (\Sigma x : A. B) \rightarrow C}
\]
Note that if we read $\exists$ for $\Sigma$, $\forall$ for $\Pi$ and $\Rightarrow$ for $\rightarrow$, this is the normal elimination rule for existential quantification: if $(\forall x : A. \, B \Rightarrow C)$ then $(\exists x : A. \, B) \Rightarrow C$. The premise $\Gamma \vdash C : s$ guarantees that $x \notin \text{FV}(C)$.

The $\beta$-reduction rule for $\nabla$ is

$$\nabla f \left( \text{in}_{\Sigma x \ A} a \, b \right) \quad \xrightarrow{\beta} \quad f \ a \ b$$

The $\eta$-rule is easiest to express in terms of $\text{in}_{\Sigma x \ A} B$:

$$\nabla \text{in}_{\Sigma x \ A} B \ c \quad \xrightarrow{\eta} \quad c$$

The term $\left( c \text{ where } (in \ x \ y) = d \right)$ can be expressed in terms of the more primitive $\nabla$, namely as $\nabla (\lambda x : A. \, \lambda y : B. \, c) \ d$.

As in the elimination rule for $\Pi$-types, we have the possibility of controlling the possible sorts of $C$ in the elimination rules above. As for the $\Pi$-types, we will only allow eliminations where the type of range $C$ is the same sort as the type of domain $(\Sigma x \ A \ B)$.

**4.6 Definition (Extension of (D)PTS with $\Sigma$-types)**

The extension of a (D)PTS with $\Sigma$-types is specified by a set of rules $R^\Sigma \subseteq S \times S$. The set of pseudoterms is extended as follows

$$T = \left( (\Sigma \text{Var} \ T. \ T) \mid \text{in}_{\Sigma \text{Var}} T \right) \ T \ T \ | \ \nabla T$$

The following reduction rule is added

$$\nabla f \left( \text{in}_{\Sigma x \ A} B \ a \ b \right) \quad \xrightarrow{\beta} \quad f \ a \ b$$

and the following type inference rules

$$\text{(\Sigmaform)} \quad \frac{\Gamma \vdash A : s_1 \quad I, x : A \vdash B : s_2}{\Gamma \vdash (\Sigma x : A. \ B) : s_2} \quad \text{if } (s_1, s_2) \in R^\Sigma$$

$$\text{(\Sigmaintro)} \quad \frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B[x := a]}{\Gamma \vdash \text{in}_{\Sigma x \ A} B \ a \ b : (\Sigma x : A. \ B)}$$

$$\text{(\Selim)} \quad \frac{\Gamma \vdash f : (\Pi x : A. \ B \Rightarrow C) \quad \Gamma \vdash (\Sigma x : A. \ B) : s \quad \Gamma \vdash C : s}{\Gamma \vdash \nabla f : (\Sigma x : A. \ B) \Rightarrow C}$$

The elimination rule for $\Sigma$-types can be generalised in the same directions as the one for $\Pi$-types. One possibility is to allow the range of $\nabla f$ to be of another sort than its domain. Another is to allow $\nabla f$ to have a dependent type. The most liberal elimination rule for $\Sigma$-types, combining these two possibilities, is

$$\frac{\Gamma, x : A, y : B \vdash c \ c[z := \text{in}_{\Sigma x \ A} B \ x \ y]}{\Gamma \vdash \left( c \text{ where } (in \ x \ y) = d \right) : C \ z}$$

With this elimination rule the $\Sigma$-types become so-called strong $\Sigma$-types, as used in Martin-Lof's type theories. The $\Sigma$-types in definition 4.6 — with the elimination rule (\Selim) — are known as weak $\Sigma$-types. Inhabitants of a strong $\Sigma$-type $(\Sigma x \ A \ B)$ are pairs $(a, b)$ with $a : A$
and $b : B[x := a]$ for which we do have direct access to the two components $a$ and $b$. Using the inference rule above it is possible to define functions

\[
\begin{align*}
\pi_1 & : (\Sigma x : A. \ B) \rightarrow A \\
\pi_2 & : (\Pi z : (\Sigma x : A. \ B) \ B[x := \pi_1 z])
\end{align*}
\]

such that

\[
\begin{align*}
\pi_1(\textup{in}_{\Sigma A} B a b) & \triangleright_{\beta} a \\
\pi_2(\textup{in}_{\Sigma A} B a b) & \triangleright_{\beta} b
\end{align*}
\]

This means that the strong sums $(\Sigma x : A. \ B)$ with $x \not\in \text{FV}(B)$, is just a product type $A \times B$. So strong sums can be seen as a generalisation of cartesian products.

4 7 REMARK. Even with the "weak" elimination rule rule $(\Sigma \text{elim})$ given in definition 4.6, it is possible to define the projections $\pi_1$ and $\pi_2$ for certain $(\Sigma x : A. \ B)$. A function $\pi_1$ satisfying (i) is definable if $(\Sigma x : A. \ B)$ is formed using a rule $(s_1, s_2) \in R^\Sigma$ with $s_1 = s_2$, namely as $\nabla(\lambda x : A. \lambda y : B. \ x)$. A function $\pi_2$ satisfying (ii) is definable using $(\Sigma \text{elim})$ if $x \not\in \text{FV}(B)$, namely as $\nabla(\lambda x : A. \lambda y : B. \ y)$. So, if the weak sum $(\Sigma x : A. \ B)$ is formed using a rule $(s, s) \in R^\Sigma$ and $x \not\in \text{FV}(B)$, then it is just a cartesian product type $A \times B$.

4.1.4 Labelled Products

Labelled products are generalisations of the cartesian product types $A \times B$ introduced earlier. They will be used as record types in the programming language. We have to introduce a collection of labels, and two very simple judgements involving labels:

4.8 DEFINITION.

1. $\mathcal{L}$ is the set of all labels. We assume $0, 1, 2, \ldots \in \mathcal{L}$.

2. For judgements of the form $\langle l_1, \ldots, l_n \rangle : \Box_{\text{label}}$ and $l : \langle l_1, \ldots, l_n \rangle$, where $l, l_1, l_2, \ldots \in \mathcal{L}$, we have the following inference rules

\[
\frac{l_1, \ldots, l_n \in \mathcal{L} \text{ and all } l_i \text{ distinct}}{\langle l_1, \ldots, l_n \rangle : \Box_{\text{label}}}
\]

\[
\frac{l \in \{l_1, \ldots, l_n\}}{\langle l_1, \ldots, l_n \rangle : \Box_{\text{label}}}
\]

Because $0, 1, 2, \ldots \in \mathcal{L}$, we will be able to consider unlabelled products as special cases of labelled ones. Beware that the labels $0, 1, 2, \ldots$, and the natural numbers used as data in the programming language are not the same and belong to different syntactic categories.

Labelled product types are of the form $\Pi(l_1 : A_1, \ldots, l_n : A_n)$. Their inhabitants are terms of the form $(l_1 \mapsto a_1, \ldots, l_n \mapsto a_n)$. These terms are essentially mappings from labels to terms. The formation of labelled products is controlled by the same set of rules as the cartesian products. So the type $\Pi(l_1 : A_1, \ldots, l_n : A_n)$ can be formed if all the $A_i$ inhabit the same same
sort $s \in R^s$. Although that labelled products are written using "\(\Pi\)", we will still refer to them as \(x\)-types, and reserve the name \(\Pi\)-types for the dependent products (\(\Pi x A. B\)).

Clearly the order of the fields "\(a_1:A_i\)" and "\(a'_i\)" in terms \(\Pi(l_1:A_1, \ldots, l_n:A_n)\) and \(\langle l_1 \mapsto a_1, \ldots, l_n \mapsto a_n \rangle\) is irrelevant. Terms that are equal up to permutations of fields are identified, in the same way as terms that are equal up to renaming of bound variables are identified.

We will also allow the empty product type \(\Pi()\). This type is a type with only one inhabitant, namely the empty mapping () from labels to terms. This type requires some special attention. For every $s \in R^s$ there is an empty product \(\Pi()\). So if there is more than one $s$ in \(R^s\), these types \(\Pi()\) and their inhabitants () have to get a subscript $s$ to distinguish them. Otherwise we lose the property that the type of a term is unique up to conversion. As far as the syntax is concerned, we do not gain anything by using the empty product type \(\Pi()\) as the unit type. Special type inference rules have to be given for the empty product because its introduction and formation rule do not have any premises. But as far as the semantics is concerned, the empty product can be treated as any other product

4.9 Definition (Extension of \((D)PTS\) with \(x\)-types)
The extension of a \((D)PTS\) with labelled product types - or simply \(x\)-types for short - is specified by a set of rules \(R^x \subseteq S\)
The set of pseudoterms is extended as follows

\[ T := \ldots | \Pi(L; T, \ldots, L; T) | \langle L \mapsto T, \ldots, L \mapsto T \rangle | T \ldots | \Pi() \ldots | () \ldots \]

The following reduction rule is added

\[ (l_1 \mapsto a_1, \ldots, l_n \mapsto a_n).l_i \vdash a_i \]

and the following type inference rules

\[ \begin{align*}
& (x\text{form}) \quad \frac{\langle l_1, \ldots, l_n \rangle \cdot \text{label} \quad \Gamma \vdash A_i \quad \text{s for } i = 0 \ldots n}{\Gamma \vdash \Pi(l_1:A_1, \ldots, l_n:A_n) \quad s} & \text{if } s \in R^x \text{ and } n \neq 0 \\
& (x\text{intro}) \quad \frac{\Gamma \vdash a_i \quad A_i \text{ for } i = 0 \ldots n \quad \Gamma \vdash \Pi(l_1:A_1, \ldots, l_n:A_n) \quad s}{\Gamma \vdash \langle l_1 \mapsto a_1, \ldots, l_n \mapsto a_n \rangle : \Pi(l_1:A_1, \ldots, l_n:A_n)} \\
& (x\text{elim}) \quad \frac{\Gamma \vdash b \quad \Pi(l_1:A_1, \ldots, l_n:A_n) \quad l_i \cdot \langle l_1, \ldots, l_n \rangle}{\Gamma \vdash b.l_i : A_i} \\
& (\Pi()\text{form}) \quad \epsilon \vdash \Pi() \quad s \quad \text{if } s \in R^x \\
& (\Pi()\text{intro}) \quad \epsilon \vdash () \quad s \quad \frac{\epsilon \vdash \Pi() \quad s}{\epsilon \vdash () \cdot \Pi()} \\
\end{align*} \]

The rules \((x\text{form}), (x\text{intro})\) and \((x\text{elim})\) are similar to the original \(PTS\) rules for formation, introduction and elimination of dependent products (\(\Pi x A. B\)). Having $s \in R^x$ can be seen as having \((\text{label}, s) \in R^x\).

The $\eta$-reduction rule for labelled products is

\[ (l_1 \mapsto a, l_1, \ldots, l_n \mapsto a.l_n) \vdash_\eta a \quad \text{if } a \Pi(l_1:A_1, \ldots, l_n:A_n) \]
4.1. EXTENDING PTSs WITH \( +, \times \) AND \( \Sigma \)

Note that that this rule depends on the type of \( a \). This is another reason to exclude \( \eta \)-
reduction. For all the type systems in this thesis, the typing relation depends on the reduction
relation (namely in the conversion rule (\( \beta \text{conv} \)), but the reduction relation does not depend
on the typing relation. Including the \( \eta \)-rule above would mean that the reduction relation in
turn depends on the typing relation, so that the reduction relation can no longer be defined
before the typing relation is defined.

For the empty product, the direction of the \( \eta \)-rule above does not make sense. It has to
be reversed:

\[
\alpha \triangleright_\eta \emptyset \quad \text{if } \alpha : \Pi \emptyset
\]

In fact, for the \( \eta \)-rules there is not a natural direction as there is for all the \( \beta \)-rules.

Because we assume all the natural numbers are labels, unlabelled products can be treated
as a special case of labelled products.

4.10 NOTATION (Unlabelled \( n \)-ary products)

For terms \( A_1, \ldots, A_n \) and \( a_1, \ldots, a_n \) we write \( A_1 \times \ldots \times A_n \) for the \( n \)-ary product type
\( \Pi(1; A_1, \ldots, \pi; A_n) \), and \( (a_1, \ldots, a_n) \) for the \( n \)-tuple \( (1 \mapsto a_1, \ldots, n \mapsto a_n) \).

Note that the reduction and inference rules for \( \Pi(1; A, 2; B) \) are indeed exactly the ones
given for \( A \times B \) earlier. So the extension with \( \times \)-type given in definition 4.9 subsumes the
one given in definition 4.3.

4.1.5 Labelled Sums

Labelled sum types, generalisations of the disjoint sum types \( A + B \) discussed earlier, are of the form \( \Sigma(l_1; A_1, \ldots, l_n; A_n) \). The inhabitants of \( \Sigma(l_1; A_1, \ldots, l_n; A_n) \) are essentially pairs
\( (l_i, a_i) \) with \( a_i \) of type \( A_i \). The formation of labelled sums is controlled by the same set of
rules \( R^+ \) as the disjoint sum types

\[
\frac{\Gamma \vdash A_1 : s \ldots \Gamma \vdash A_n : s}{\Gamma \vdash \Sigma(l_1; A_1, \ldots, l_n; A_n) : s} \quad \text{if } s \in R^+.
\]

The introduction rule for labelled sum types is

\[
\frac{\Gamma \vdash a_i : A_i \quad l_i : (l_1, \ldots, l_n)}{\Gamma \vdash \text{in}_{\Sigma(l_1; A_1, \ldots, l_n; A_n)} l_i a_i : \Sigma(l_1; A_1, \ldots, l_n; A_n)}
\]

As for the disjoint sum, the subscript of \( \text{in}_{\Sigma(l_1; A_1, \ldots, l_n; A_n)} l_i \) is necessary for type inference. A
possible way of avoiding these subscripts would be to allow some form of subtyping. The
type \( \Sigma(l_1; A_i) \) would then be a subtype of \( \Sigma(l_1; A_1, \ldots, l_n; A_n) \), so for \( a_i : A_i \) the term \( (l, a_i) \)
would have type \( \Sigma(l_1; A_i, \ldots, l_n; A_n) \), and also the supertype \( \Sigma(l_1; A_1, \ldots, l_n; A_n) \). Subtyping will not be
treated in this thesis.

The injection \( \text{in}_{\Sigma(l_1; A_1, \ldots, l_n; A_n)} l_i, a \) could be typed without its argument \( a \), namely as

\[
\text{in}_{\Sigma(l_1; A_1, \ldots, l_n; A_n)} l_i : A_i \rightarrow \Sigma(l_1; A_1, \ldots, l_n; A_n)
\]
or even without the projection \( l_i \), namely as

\[
\text{in}_{\Sigma(l_1; A_1, \ldots, l_n; A_n)} : \Pi(l_1; A_1 \rightarrow \Sigma(l_1; A_1, \ldots, l_n; A_n), \ldots, l_n; A_n \rightarrow \Sigma(l_1; A_1, \ldots, l_n; A_n))
\]
CHAPTER 4 SIMPLE EXTENSIONS

Of course this is only possible if these types can be formed. As for the unlabelled binary sums, different ways to write the elimination principle exist. One possibility is a case-expression of the form (case \( d \) of in \( l_1 \ x_1 \mapsto c_1 \mid \ldots \ | \ t_n \ x_n \mapsto c_n \)) with the type inference rule

\[
\Gamma \vdash d : \Sigma(l_1; A_1, \ldots , l_n; A_n) \quad \Gamma, x_i : A_i \vdash c_i : C \quad \text{for } i = 0 \ldots n
\]

\[
\Gamma \vdash (\text{case } d \text{ of in } l_1 \ x_1 \mapsto c_1 \mid \ldots \ | \ t_n \ x_n \mapsto c_n) : C
\]

and the reduction rules:

\[
\begin{align*}
\text{(case } (\text{in}_{\Sigma(l_1; A_1, \ldots , l_n; A_n)} \ l_i, a_i) \text{ of in } l_1 \ x_1 \mapsto c_1 \mid \ldots \ | \ t_n \ x_n \mapsto c_n) & \Rightarrow_B \ c_i[l_i := a_i] \\
\text{(case } c \text{ of in } l_1 \ x_1 \mapsto \text{in}_{\Sigma(l_1; A_1, \ldots , l_n; A_n)} \ l_n \ x_n | \ldots \ | \ t_n \ x_n \mapsto \text{in}_{\Sigma(l_1; A_1, \ldots , l_n; A_n)} \ l_n \ x_n) & \Rightarrow_B \ c
\end{align*}
\]

We will use a generalisation of \( \nabla \), with the inference rule

\[
\Gamma \vdash f \cdot \Pi(l_1; A_1, \ldots , l_n; A_n \rightarrow C) \quad \Gamma \vdash \Sigma(l_1; A_1, \ldots , l_n; A_n) : s \quad \Gamma \vdash C : s
\]

\[
\Gamma \vdash \nabla f : \Sigma(l_1; A_1, \ldots , l_n; A_n) \rightarrow C
\]

So, as for the unlabelled binary disjoint sums, only eliminations where the type of the range \( C \) is the same as the type of domain \( \Sigma(l_1; A_1, \ldots , l_n; A_n) \) are allowed.

The \( \beta \)-reduction rules for \( \nabla \) is

\[
\nabla h \ (\text{in}_{\Sigma(l_1; A_1, \ldots , l_n; A_n)} \ l_i, a) \Rightarrow_B h \ l_i, a.
\]

The \( \eta \)-rule is easiest to express in terms of \( \text{in}_{\Sigma(l_1; A_1, \ldots , l_n; A_n)} \):

\[
\nabla \text{in}_{\Sigma(l_1; A_1, \ldots , l_n; A_n)} \ c \Rightarrow_\eta \ c.
\]

To compare the inference rule for \( \nabla \) with the one for case, note that if \( \Gamma, x_i \vdash c_i : C \), then

\[
\Gamma \vdash (\lambda x_i; A_i, c_i) \ A_i \rightarrow C,
\]

and then

\[
\Gamma \vdash (l_1 \mapsto (\lambda x_1; A_1, c_1), \ldots , l_n \mapsto (\lambda x_n; A_n, c_n)) : \Pi(l_1; A_1 \rightarrow C, \ldots , l_n; A_n \rightarrow C).
\]

The term \( (\text{case } d \text{ of in } l_1 \ x_1 \mapsto c_1 \mid \ldots \ | \ t_n \ x_n \mapsto c_n) \) can be expressed in terms of \( \nabla \), namely as \( \nabla (l_1 \mapsto (\lambda x_1; A_1, c_1), \ldots , l_n \mapsto (\lambda x_n; A_n, c_n)) a \). This term has the correct reduction behaviour:

\[
\nabla (l_1 \mapsto f_1, \ldots , l_n \mapsto f_n) \ (\text{in}_{\Sigma(l_1; A_1, \ldots , l_n; A_n)} \ l_i, a) \Rightarrow_\beta (l_1 \mapsto f_1, \ldots , l_n \mapsto f_n) \ l_i, a.
\]

Like the empty product type \( \Pi() \), the empty sum type \( \Sigma() \) requires some extra attention. The empty sum type \( \Sigma() \) is an empty type, for which there is no introduction rule to construct inhabitants. For every \( s \in R^+ \) there is an empty sum \( \Sigma() \). Like \( \Pi() \), those get a subscript \( s \) to distinguish them. To preserve uniqueness of types more has to be done. Instantiating the elimination rule above for the empty sum produces

\[
\Gamma \vdash f : \Pi() \quad \Gamma \vdash \Sigma() : s \quad \Gamma \vdash C : s
\]

\[
\Gamma \vdash \nabla f : \Sigma() \rightarrow C
\]

This means that for any \( f : \Pi() \), the term \( \nabla f \) can have many types, because its range can be any type \( C : s \). To preserve uniqueness of types, the range of \( \nabla f \) is written as a subscript.

So the elimination rule for empty sums becomes

\[
\Gamma \vdash f : \Pi(), s \quad \Gamma \vdash \Sigma(), s \quad \Gamma \vdash C : s
\]

\[
\Gamma \vdash \nabla f : \Sigma(), s \rightarrow C
\]
4.1 EXTENDING PTSs WITH +, \times AND \Sigma

4.11 DEFINITION (Extension of (D)PTS with ++-types).
The extension of a (D)PTS with labelled sum types – or simply + types for short – is specified
by a set of rules $R^+ \subseteq S$.
The set of pseudoterms is extended as follows

$$
T = \ldots | \Sigma (L_T \ldots L_T) | \text{ln}_ \Sigma (L_T \ldots L_T) T T | \Delta T | \nabla T | \Delta T T | \Sigma \Omega s .
$$

The following reduction rule is added

$$
\nabla h (\text{ln}_ \Sigma (L_A A_n), l_i a) \Rightarrow h \cdot l_i a ,
$$

and the following type inference rules

\[ (+\text{form}) \frac{(l_1, \ldots, l_n) : \text{label} \Gamma \vdash A_i \cdot s \text{ for } i = 0 \ldots n}{\Gamma \vdash \Sigma (l_1; A_1, \ldots, l_n; A_n) : s} \quad \text{if } s \in R^+ \text{ and } n \neq 0 \]

\[ (+\text{intro}) \frac{\Gamma \vdash A_i : A_i \quad \Gamma \vdash \Sigma (l_1 A_1, \ldots, l_n A_n) : s}{\Gamma \vdash \text{ln}_ \Sigma (l_1 A_1, \ldots, l_n A_n) \vdash A_i : l_i a_i \vdash \Sigma (l_1 A_1, \ldots, l_n A_n)}\]

\[ (+\text{elim}) \frac{\Gamma \vdash f : \Sigma (l_1 A_1, \ldots, l_n A_n) \to C}{\Gamma \vdash \nabla f : \Sigma (l_1 A_1, \ldots, l_n A_n) \to C} \quad \text{if } s \in R^+ \]

(\Sigma(\cdot)\text{form})

$$
\epsilon \vdash \Sigma \epsilon \cdot s : s
$$

(\Sigma(\cdot)\text{elim})

$$
\frac{\Gamma \vdash f : \Pi \epsilon \cdot s \quad \Gamma \vdash \Sigma \epsilon \cdot s : \Pi \epsilon \cdot s \quad \Gamma \vdash C : s}{\Gamma \vdash \nabla f C : \Sigma \epsilon \cdot s \to C}
$$

For labelled sums the notation using case seems more natural than the one using $\nabla$. The
notation using $\nabla$ – or rather the infix $\nabla$ – is useful for unlabelled sums:

4.12 NOTATION (Unlabelled n-ary sums)

For terms $A_1, \ldots, A_n$ and $f_1, \ldots, f_n$ we write $A_1 + \ldots + A_n$ for the n-ary sum
$\Sigma (1 : A_1, \ldots, n : A_n)$, and $f_1 \nabla \ldots \nabla f_n$ for $\nabla (1 \mapsto f_1, \ldots, n \mapsto f_n)$.

Note that the reduction and inference rules for $\Sigma (1 : A, 2 : B)$ are indeed exactly the ones
given for $A + B$ earlier. So the extension with ++-types given in definition 4.11 subsumes the
two given in definition 4.4.

4.1.6 Properties of (D)PTSs extended with +, \times and \Sigma

Extending a PTS or DPTS with +, \times and \Sigma preserves all the properties of arbitrary PTSs
or DPTSs listed in chapter 2. For the reduction relation the property of Church-Rosser is
preserved:

4.13 LEMMA. $\beta$-reduction is Church-Rosser.

\textbf{Proof.} This can be proved by the usual Tait-Martin-Lof method. Another way is to use
the theory of Combinatory Reduction Systems (CRSs) and verify that $\Rightarrow$ is an orthogonal CRS
(see [KOR93]).
4.14 Lemma \( \delta \)-reduction is Church-Rosser.

Proof. This can be proved in exactly the same way as in lemma 2.26, i.e. using the fact that \( \vdash_\beta \) is CR and the fact that \( \delta \)-normal forms exist. \( \square \)

All other properties of PTSs and DPTSs in chapter 2 are proved by induction on type derivations or by induction on the structure of terms. Extending these induction proofs for the new inference rules and new term-constructions is completely straightforward. We just list the main properties.

4.15 Lemma (Correctness of Types)
For all (D)PTSs with \( +, \times \) and \( \Sigma \): if \( \Gamma \vdash a : A \) then \( A \in S \) or \( \Gamma \vdash A = s \) for some \( s \in S \). \( \square \)

4.16 Lemma (SR\(_\beta \) Subject Reduction).
For all PTSs with \( +, \times \) and \( \Sigma \): if \( \Gamma \vdash b : B \) and \( b \vdash_\beta b' \) then \( \Gamma \vdash b' : B \). \( \square \)

4.17 Lemma (UT\(_\beta \) Uniqueness of Types).
For all functional PTSs with \( +, \times \) and \( \Sigma \): if \( \Gamma \vdash b : B \) and \( \Gamma \vdash b : B' \) then \( B \equiv_\beta B' \). \( \square \)

4.18 Lemma (SR\(_{\beta \delta} \) Subject Reduction)
For all DPTSs with \( +, \times \) and \( \Sigma \): if \( \Gamma \vdash b : B \) and \( \Gamma \vdash b \vdash_\beta b' \) then \( \Gamma \vdash b' : B \). \( \square \)

4.19 Lemma (UT\(_{\beta \delta} \) Uniqueness of Types)
For all functional DPTSs with \( +, \times \) and \( \Sigma \): if \( \Gamma \vdash b : B \) and \( \Gamma \vdash b : B' \) then \( \Gamma \vdash B \equiv_\beta B' \). \( \square \)

4.20 Theorem (Elimination of definitions)
For all specifications \( S \) if \( \Gamma \vdash_\lambda S a \vdash A \) then \( \text{hnf}(\Gamma) \vdash_\lambda S \text{hnf}_f(a) : \text{hnf}_f(A) \). \( \square \)
4.2 Extension of the Programming Language

The programming language $\lambda\omega_s$ is extended to provide with more datatypes as primitives:

4.21 Definition. $\lambda\omega^+_s(\mathcal{E})$ is the (D)PTS with $+$, $\times$ and $\Sigma$ specified by

$$
\begin{align*}
S & = \{*, \emptyset, \}
A & = \{* \times \emptyset\}
R^\mathcal{E} & = \{(\emptyset, \emptyset), (\emptyset, *, (*, *))\}
R^\Sigma & = \{(\emptyset, *)\}
R^* = R^+ & = \{*\}
\end{align*}
$$

The new datatypes that can be formed using $R^* = \{*\}$ are unlabelled product types of the form $\sigma_1 \times \ldots \times \sigma_n$, inhabited by programs of the form $(M_1, \ldots, M_n)$, and labelled products types - or record types - of the form $\Pi(l_1: \sigma_1, \ldots, l_n: \sigma_n)$, inhabited by programs of the form $(l_1 \mapsto M_1, \ldots, l_n \mapsto M_n)$. The empty product $\Pi(\emptyset)$ provides a datatype with just one inhabitant, for which we introduce a more suggestive name $\mathcal{E}$

4.22 Definition (Unit Type).
The datatype Unit and its inhabitant unit are defined by the following context $\Gamma_{UNIT}$,

$$
\begin{align*}
\text{Unit} & = \Pi(\emptyset) : * \\
\text{unit} & = \langle \emptyset \rangle : \text{Unit}
\end{align*}
$$

The new datatypes that can be formed using $R^+ = \{*\}$ are unlabelled sum types of the form $\sigma_1 + \ldots + \sigma_n$ and labelled sum types also known as variant types - of the form $\Sigma(l_1: \sigma_1, \ldots, l_n: \sigma_n)$. The empty sum gives us an empty datatype.

4.23 Definition (Empty Type). The datatype Empty is defined by the following context $\Gamma_{EMPTY}$

$$
\Gamma_{EMPTY}
$$

4.24 Definition (Booleans). The datatype bool and its elements true and false are defined by the following context $\Gamma_{BOOL}$

$$
\begin{align*}
\text{bool} & = \text{Unit} + \text{Unit} : * \\
\text{true} & = \text{in}_{\text{Unit} + \text{Unit}} 1 \text{ unit} : \text{bool} \\
\text{false} & = \text{in}_{\text{Unit} + \text{Unit}} 2 \text{ unit} : \text{bool} \\
\text{if} & = \lambda a: * : \lambda x: \text{bool}. \lambda y: \sigma. \bot a: \text{Unit}. x, y: \text{Unit}. y \in (\lambda u: \text{Unit}. x, \lambda u: \text{Unit}. y) \ b \\
\text{if} & = \lambda a: * : \lambda b: \text{bool} \rightarrow a \rightarrow a \rightarrow a
\end{align*}
$$

For programs $b: \text{bool}, M_1 : \tau$ and $M_2 : \tau$ we write $(\text{if } b \text{ then } M_1 \text{ else } M_2)$ for $(\text{if } \tau M_1 M_2 b)$. Note that the type parameter $\tau$ is omitted. It not difficult to see that this missing parameter can be reconstructed (it is the type of $M_1$ and $M_2$).
The term \((\text{if } b \text{ then } M_1 \text{ else } M_2)\) reduces as expected:

\[
\begin{align*}
\Gamma_{\text{UNIT}}, \Gamma_{\text{BOOL}} & \vdash \text{if true then } a_1 \text{ else } a_2 \quad \bowtie_{\text{gen}} \quad a_1 \\
\Gamma_{\text{UNIT}}, \Gamma_{\text{BOOL}} & \vdash \text{if false then } a_1 \text{ else } a_2 \quad \bowtie_{\text{gen}} \quad a_2
\end{align*}
\]

We will always assume that \(\Gamma_{\text{BOOL}}, \Gamma_{\text{UNIT}}\) and \(\Gamma_{\text{EMPTY}}\) are part of the context.

The new datatypes that can be formed using \(\mathcal{R}^\Sigma = \{(\mathcal{O}, *_s)\}\) are of the form \((\Sigma \alpha \mathcal{K}, \sigma)\). These datatypes are the types of programs of the form (\(\text{in}_{\mathcal{K}} \sigma \tau N\)). Such programs can be understood as a pairs \((\tau, N)\) consisting of a datatype-constructor \(\tau\) and a program \(N\) of type \(\sigma[\alpha := \tau]\). \(\Sigma\)-types can be used as abstract datatypes. For a thorough explanation of this we refer to [MP84]. Two examples are given below.

**4.25 Example.** We consider a simple abstract datatype, for lists of booleans. An abstract datatype consists of a datatype and a collection of operations on it. These operations provide the only way to manipulate inhabitants of that datatype. For an abstract datatype of boolean lists we want a datatype \(\text{boollist}\) with the following operations:

\[
\begin{align*}
\text{empty} : & \quad \text{boollist} \\
\text{cons} : & \quad \text{bool} \rightarrow \text{boollist} \rightarrow \text{boollist} \\
\text{head} : & \quad \text{boollist} \rightarrow \text{bool} \\
\text{tail} : & \quad \text{boollist} \rightarrow \text{boollist}
\end{align*}
\]

These 4 operations can be provided by a single program of the following record type

\[
\Pi(\text{empty : boollist}, \quad \text{cons : bool \rightarrow boollist \rightarrow boollist}, \quad \\
\text{head : boollist} \rightarrow \text{bool}, \quad \text{tail : boollist} \rightarrow \text{boollist})
\]

This record type gives the signature of an abstract datatype of boolean lists. For an implementation of this abstract datatype we have to choose a particular datatype \(\text{boollist}\) and a program of the type above implementing the operations on boolean lists. In a program \(M\) that uses this abstract datatype we simply assume the existence of a datatype \(\text{boollist}\) and a program of the type above. For this \(\Sigma\)-types can be used. The datatype-constructor \(F\) as follows

\[
F = \lambda \text{boollist}. *_s \Pi(\text{empty : boollist}, \quad \text{cons : bool} \rightarrow \text{boollist} \rightarrow \text{boollist}, \quad \\
\text{head : boollist} \rightarrow \text{bool}, \quad \text{tail : boollist} \rightarrow \text{boollist})
\]

This \(F\) gives the signature of our abstract datatype. The type

\[
\text{ADT} = (\Sigma \text{boollist} *_s, F \text{boollist}) *_s
\]

can now serve as the type of implementations of the abstract datatype of boolean lists. For an implementation of this abstract datatype we have to choose a datatype \(\tau\) and a program of type \(F\tau\). The inhabitants of \(\tau\) then represent lists of booleans, and the program of type \(F\tau\) provides the implementations of the operations on these (representations of) lists. The introduction rule for the datatype \(\text{ADT}\) is

\[
\frac{\Gamma \vdash \tau : *_s \quad \Gamma \vdash N : F \tau}{\Gamma \vdash (\text{in}_{\text{ADT}} \tau N) : \text{ADT}} \quad (\Sigma \text{intro})
\]
So, an inhabitant of ADT—i.e., an implementation of the abstract datatype of boolean lists—can be built using a datatype \( \tau \) and a program \( N \) of type \( F \tau \). Of course, there is no guarantee that this is indeed a correct implementation of lists, e.g., it may well be the case that \((N \cdot \text{cons} \cdot \text{nil}) \not= \text{nil} \). Later, in examples 4.43 and 4.45, specifications for ADT will be given.

To make a program using the abstract datatype of boolean lists, we simply assume the existence of a type \( \text{boolist} : * \), and a program \( N \) of type \( F \text{boolist} \). Of course, there is no guarantee that this is indeed a correct implementation of lists, e.g., it may well be the case that \((N \cdot \text{cons} \cdot \text{nil}) \not= \text{nil} \).

Later, in examples 4.43 and 4.45, specifications for ADT will be given.

To make a program using the abstract datatype of boolean lists, we simply assume the existence of a type \( \text{boolist} : * \), and a program \( N \) of type \( F \text{boolist} \). Of course, there is no guarantee that this is indeed a correct implementation of lists, e.g., it may well be the case that \((N \cdot \text{cons} \cdot \text{nil}) \not= \text{nil} \).

The crucial point is that in the "main" program \( M \) the variables \( \text{boolist} \) and \( x \) are visible, but not the bindings to \( \tau \) and \( N \). In other words, the interface of the abstract datatype is visible in \( M \), but the implementation is not.

When \( \Sigma \)-types are used in this way, then implementations of abstract datatypes become first-class citizens in the programming language, i.e., they can be manipulated just like any other data or program. For instance, they can be passed as parameters, and the choice between different implementations can then be made at during the execution of a program.

4 26 Notation. We write \((\text{abstype } \alpha \cdot \mathcal{K}, \text{ with } x : \sigma \text{ is imp in } M) \) for \( \nabla(\lambda \alpha : \mathcal{K} \cdot \lambda x : \sigma \cdot M) \text{ imp} \).

So the program given at the end of the example above is written as

\[
(\text{abstype } \text{boolist} : * \text{, with } \tau : F \text{boolist is } (\text{in}_{\text{ADT}} \tau \cdot N) \text{ in } M)
\]

With this notation the interface of the abstract datatype and the implementation are no longer separated by the main program \( M \).

\( \lambda \omega \tau \) does not only provide the abstract datatypes, but also abstract datatype-constructors.

4.27 Example. An abstract datatype-constructor consists of a datatype-creator and a collection of operations on the datatypes that can be built with it. As an example we consider an abstract datatype-creator for building lists over any datatype. It comprises a datatype-creator \( \text{hst} : * \mapsto * \), and operations for manipulating inhabitants of the datatypes \( \text{hst} \sigma \), for all datatypes \( \sigma \).

\[
\text{empty} : \text{hst} \sigma, \text{cons} : \sigma \rightarrow \text{hst} \sigma \rightarrow \text{hst} \sigma, \text{head} : \text{hst} \sigma \rightarrow \sigma, \text{tail} : \text{hst} \sigma \rightarrow \text{hst} \sigma.
\]
These operations can be provided by a single program of type

\[
\Pi \langle \text{empty} : \Pi \alpha \times \star \ A \text{list } \alpha, \ cons : A \alpha \times A \text{list } \alpha \rightarrow A \text{list } \alpha, \ head : A \alpha \times \text{list } \alpha \rightarrow \alpha, \ tail : A \alpha \times \text{list } \alpha \rightarrow \text{list } \alpha \rangle,
\]

or, alternatively, by a program of type

\[
\Pi \alpha \times \Pi \langle \text{empty} : \text{list } \alpha, \ cons : \alpha \rightarrow \text{list } \alpha \rightarrow \text{list } \alpha, \ head : \text{list } \alpha \rightarrow \alpha, \ tail : \text{list } \alpha \rightarrow \text{list } \alpha \rangle.
\]

We choose the second option, and define a datatype-constructor \( F \) as follows

\[
F = \lambda \text{list } \star \rightarrow \star. \ Pi \alpha \times \Pi \langle \text{empty} : \text{list } \alpha, \ cons : \alpha \rightarrow \text{list } \alpha \rightarrow \text{list } \alpha, \ head : \text{list } \alpha \rightarrow \alpha, \ tail : \text{list } \alpha \rightarrow \text{list } \alpha \rangle : (\star \rightarrow \star) \rightarrow \star.
\]

The datatype

\[
ADT = (\Sigma \text{list } \star \rightarrow \star. \ F \text{list }): \star
\]

is then the type of implementations of an abstract datatype-constructor for making lists. Its inhabitants are of the form \((m_{ADT} \tau N)\), with \(\tau \cdot \star \rightarrow \star\) and \(N : F \tau\). If

\[
F \vdash \forall (\lambda \text{list } \star \rightarrow \star. \ \lambda x: F \text{bool list } M) \cdot ADT \rightarrow \rho,
\]

then in the program \(M\) the operations

\[
\lambda \sigma \text{empty} : \text{list } \sigma \quad \lambda \sigma \cdot \text{cons} \quad \sigma \rightarrow \text{list } \sigma \rightarrow \text{list } \sigma \quad \lambda \sigma \cdot \text{head} \quad \text{list } \sigma \rightarrow \sigma \quad \lambda \sigma \cdot \text{tail} \quad \text{list } \sigma \rightarrow \text{list } \sigma
\]

can be used, for all datatypes \(\sigma\).

Properties of \(\lambda \omega_\star^+\) and \(\lambda \omega_{\star^+}\)

As for the system without \(+\), \(\times\) and \(\Sigma\), the context-free syntax of the pseudoterms can be refined, distinguishing the different levels:

4.28 Definition. For \(\lambda \omega_{\star^+}\), the sets of pseudoterms Cons and Prog defined in definition 3.2 are extended as follows:

\[
\begin{align*}
\text{Cons} &= | \text{Cons } \times \text{Cons} | \Pi (\Lambda \text{Cons}, \ldots, \Lambda \text{Cons}) | \Pi ()_\star, \\
& | \text{Cons } + \text{Cons} | \Sigma (\Lambda \text{Cons}, \ldots, \Lambda \text{Cons}) | \Sigma ()_\star, \\
& | (\Sigma \text{Var}\cdot \text{Kind. } \text{Cons}) \\
\text{Prog} := \ldots | (\text{Prog }, \text{Prog}) | (\Lambda \rightarrow \text{Prog}, \ldots, \Lambda \rightarrow \text{Prog}) | ()_\star, | \text{Prog } \Lambda \\
& | \text{in}_\text{Cons } \text{Cons } | \downarrow \text{Prog } | \downarrow \text{Prog}_\text{Cons} \\
& | \text{in}_\text{Cons } \text{Cons } \text{Prog}
\end{align*}
\]
4.2. EXTENSION OF THE PROGRAMMING LANGUAGE

The set Kind containing the kinds is not affected by the new type-constructors. The dependencies between Kind, Cons and Prog do not change: Cons still only depends on Kind, and Prog depends on Cons and Kind. As for \( \lambda w \), the kinds, datatype-constructors and programs are elements of Kind, Cons and Prog, respectively:

4.29 LEMMA (Classification for \( \lambda w^+ \))

1. If \( \Gamma \vdash K : \Box_e \) then \( K \in \text{Kind} \).
2. If \( \Gamma \vdash \sigma : K : \Box_e \) then \( \sigma \in \text{Cons} \).
3. If \( \Gamma \vdash M : \sigma : \Box_e \) then \( M \in \text{Prog} \).

PROOF In exactly the same way as lemma 3.5. \( \square \)

The usual encodings of \( + \), \( \times \) and \( \Sigma \) in \( \lambda w \) can be used to show that the extension of \( \lambda w \) and \( \lambda w^+ \) with \( + \), \( \times \) and \( \Sigma \) preserves the property of strong normalisation:

4.30 COROLLARY. The system \( \lambda w^+_e \) is \( \text{SN}_{\theta_e} \).

PROOF. This follows from the fact that \( \lambda w^+_e \) is \( \text{SN}_{\theta_e} \), because there exists a mapping \( \vdash \) which maps reduction sequences in \( \lambda w^+_e \) to longer reduction sequences in \( \lambda w^+_e \). This mapping translates \( + \), \( \times \) and \( \Sigma \)-type to their usual encodings, which were given in definition 3.11 as encodings of \( \lor, \land \) and \( \exists \). N-ary products and sums can be treated as repeated binary ones, i.e. \( \sigma_1 \times \sigma_2 \times \ldots \times \sigma_n \mid = \sigma_1 \times (\sigma_2 \times (\ldots \times \sigma_n)) \). Labelled products can be treated as unlabelled ones. We assume some ordering on the set of labels to fix a unique order of the fields, and then simply forget about the labels. \( \square \)
4.3 Extension of the Programming Logic

Extending $\lambda \omega_p$ with $+$, $\times$ and $\Sigma$ in the same way as $\lambda \omega$, produces the following system $\lambda \omega_p^+$:

4.31 Definition. $\lambda \omega_p^+ (\delta)$ is the (D)PTS with $+$, $\times$ and $\Sigma$ specified by

\[
\begin{align*}
S &= \{*, \square_p \} \\
A &= \{*, \square_p \} \\
R^H &= \{(\square_p, \square_p), (\square_p, *p), (*, *p)\} \\
R^E &= \{(\square_p, *p)\} \\
R^X &= R^+ = \{*p\}
\end{align*}
\]

In this system cartesian products are interpreted as conjunctions, disjoint sums as disjunctions, and dependent sums as existential quantifications. In $\lambda \omega_p$ we now also write $\wedge$ for $\times$, $\vee$ for $+$ and $\exists$ for $\Sigma$. The new propositions that can be formed are conjunctions $P_1 \wedge \ldots \wedge P_n$, and disjunctions $P_1 \vee \ldots \vee P_n$, and higher order existential quantifications ($\exists P : Q$). There is no real need for the labelled conjunctions $\forall (l_1 P_1, \ldots, l_n P_n)$ and labelled disjunctions $\exists (l_1 P_1, \ldots, l_n P_n)$. In the programming language labelled products and sums are needed for more readable programs. In the logic, on the other hand, we are not really concerned with the readability of proof terms. Indeed, for the logic there is no real need to have $\forall$, $\exists$ and $\square$ as primitives, because for the encodings given in definition 3.11 all the required properties can be proved.

Instead of defining propositions True and False in terms of higher order quantification as in definition 3.11, they can now also be defined as the empty conjunction and disjunction:

4.32 Definition (True and False) The context defining the propositions True and False is

\[
\begin{align*}
\text{True} &= \forall() \ast_p : \ast_p, \\
\text{False} &= \exists() \ast_p : \ast_p
\end{align*}
\]

Then for True and False we have the following inference rules:

\[
\begin{align*}
(\text{True intro}) & \quad \Gamma \vdash \ast_p : \text{True} \\
(\text{False elim}) & \quad \Gamma \vdash \forall_p : \text{False} \\
& \quad \Gamma \vdash P : \text{True} \\
& \quad \Gamma \vdash \square_p : \text{False} \\
& \quad \Gamma \vdash \rightarrow : P
\end{align*}
\]

The extension of $\lambda \omega_L$ with $+$, $\times$ and $\Sigma$, containing both $\lambda \omega_p^+$ and $\lambda \omega_p^+$, is the following system $\lambda \omega_L^+$:

4.33 Definition. $\lambda \omega_L^+ (\delta)$ is the (D)PTS with $+$, $\times$ and $\Sigma$ specified by

\[
\begin{align*}
S &= \{*, \square_p \ast_p, \square_p \} \\
A &= \{*, \square_p \ast_p, \square_p \}
\end{align*}
\]
4.3. EXTENSION OF THE PROGRAMMING LOGIC

\[ R^\Pi = \{ (\Box, \Box), (\Box, \star), (\star, \star), (\Box, \Box_p), (\star, \Box_p), (\Box_p, \star), (\star, \star_p), (\Box_p, \star_p), (\star, \star_p) \} \]

\[ R^\Sigma = \{ (\Box, \star), (\Box_p, \star), (\star, \star_p), (\Box_p, \star_p), (\star, \star_p) \} \]

\[ R^* = R^+ = \{ \star, \star_p \} \]

The specification of \( \lambda \omega^+ \) consists of those of \( \lambda \omega^+_\Pi \) and \( \lambda \omega^+_\Sigma \), with four more rules for \( \Pi \)-types and two more rules for \( \Sigma \)-types. The rules in \( R^\Sigma \) are those of \( \lambda \omega^+_\Sigma \) and \( \lambda \omega^+_\Pi \), plus \( (\Box, \star_p) \) and \( (\star, \star_p) \). These two rules enable existential quantification, over kinds \( K \) and over datatypes \( \sigma \), i.e., \( (\exists \sigma. \alpha \ P) \) and \( (\exists \alpha. \ K \ P) \). The rules added for \( \Pi \)-types but not for \( \Sigma \)-types are \( (\Box, \Box_p) \) and \( (\star, \star_p) \). There does not seem to be any use for \( \Sigma \)-types formed using these rules, nor any intuitive interpretation of them.

The context-free syntax given in definition 4.28 for \( \lambda \omega^+_L \) can be extended to the whole of \( \lambda \omega^+_L \).

4.34 Definition. For \( \lambda \omega^+_L \), the sets of pseudoterms \( \text{PCons} \) and \( \text{Proof} \) defined in definition 3.2 are extended as follows:

\[
\text{PCons} ::= \ldots \ | \text{PCons} \land \ldots \land \text{PCons} \ | \forall (\text{L} \cdot \text{PCons}, \ldots, \text{L} \cdot \text{PCons}) \ | \text{PCons} \lor \ldots \lor \text{PCons} \ | \exists (\text{L} \cdot \text{PCons}, \ldots, \text{L} \cdot \text{PCons}) \ | (\exists \text{Var}^\text{L} \cdot \text{Kind} \cdot \text{PCons}) \ | (\exists \text{Var}^\text{L} \cdot \text{PCons}) \ | (\exists \text{Var}^\text{L} \cdot \text{Pkind} \cdot \text{PCons})
\]

\[
\text{Proof} ::= \ldots \ | (\text{Proof}, \ldots, \text{Proof}) \ | (\text{L} \rightarrow \text{Proof}, \ldots, \text{L} \rightarrow \text{Proof}) \ | ()_p \ | \text{Proof} \cdot \text{L} \ | \text{inpCons} \cdot \text{PCons} \cdot \text{Proof} \ | \text{inpCons} \cdot \text{Prog} \cdot \text{Proof} \ | \text{inpCons} \cdot \text{PCons} \cdot \text{Proof}
\]

In exactly the same way lemma 3 17 was proved, it can be proved that:

4.35 Lemma (Classification for \( \lambda \omega^+_L \))

1. If \( \Gamma \vdash K : \Box \), then \( K \in \text{Kind} \)
2. If \( \Gamma \vdash \sigma : \Box \), then \( \sigma \in \text{Cons} \)
3. If \( \Gamma \vdash M : \sigma : \star \), then \( M \in \text{Prog} \)
4. If \( \Gamma \vdash P : \Box_p \), then \( P \in \text{Pkind} \)
5. If \( \Gamma \vdash P : \Box_p \), then \( P \in \text{PCons} \)
6. If \( \Gamma \vdash p : P : \star_p \), then \( p \in \text{Proof} \).
The encodings of $+, \times$ and $\Sigma$ can be used to show that $\lambda \omega^+_\Sigma$ and $\lambda \omega^+_\Sigma$ are strongly normalising:

4.36 COROLLARY The system $\lambda \omega^+_\Sigma$ is $\text{SN}_{\beta(\delta)}$.

PROOF. As corollary 4.30, now using $\text{SN}_{\beta(\delta)}$ of $\lambda \omega^+_\Sigma$ instead of $\lambda \omega^+_\Sigma$.

Because there are no rules of the form $(\cdot, \cdot)$ in $\mathbb{N}_1$ or $\mathbb{R}_1$, $\lambda \omega^+_\Sigma$ is a conservative extension of $\lambda \omega^+_\Sigma$.

4.37 THEOREM (Conservativity of $\lambda \omega^+_\Sigma$ over $\lambda \omega^+_\Sigma$).

Suppose $\Gamma \vdash a : A$ in $\lambda \omega^+_\Sigma$ and $a$ is a program, datatype-constructor or a kind (i.e. $a \in \text{Prog} \cup \text{Cons} \cup \text{Kind}$).

Then $\Gamma \vdash a : A$ in $\lambda \omega^+_\Sigma$.

PROOF Induction on the derivation of $\Gamma \vdash a : A$.

4.38 DISCUSSION. We now discuss possible generalisations of the elimination rules for $\Sigma$-types, and our reasons for excluding them. Similar generalisation exists for the elimination rules for $\Sigma$-types. These generalised rules are instances of the rules for so-called inductive types given in [CP90].

Suppose $\Gamma \vdash \sigma + \tau : *$. The elimination rule we have for this datatype is

$$\frac{\Gamma \vdash \sigma \rightarrow \rho \quad \Gamma \vdash \tau : \tau \rightarrow \rho \quad \Gamma \vdash \rho : *_\Sigma}{\Gamma \vdash \sigma + \tau : \tau \rightarrow \rho}$$

- One possible generalisation is to allow the range of $f \sigma g - \rho$ in the rule above to have another type than $*_{\Sigma}$, for instance

$$\frac{\Gamma \vdash P : \sigma \rightarrow *_{\Sigma} \quad \Gamma \vdash Q : \tau \rightarrow *_{\Sigma}}{\Gamma \vdash P \lor Q : \sigma + \tau \rightarrow *_{\Sigma}}$$

This inference rule allows a predicate on $\sigma + \tau$ to be defined using a case-distinction. Without rule (i), it is still possible to define a predicate on $\sigma + \tau$ in terms of predicates on $\sigma$ and $\tau$, for example as

$$R = \lambda z. \sigma + \tau \quad (\exists y. \sigma \quad z =_{\sigma + \tau} \text{in}_{\sigma + \tau} \, 1 \, \tau \land P \, \tau) \lor (\exists y. \tau \quad z =_{\sigma + \tau} \text{in}_{\sigma + \tau} \, 2 \, y \land Q \, y)$$

From an extensional point of view $P \lor Q$ and $R$ are the same. The only difference is in their reduction behaviour. The reduction rule for $\lor$ gives

$$(P \lor Q)(\text{in}_{\sigma + \tau} \, 1 \, x) \Rightarrow y \quad P \, x$$

i.e. $(P \lor Q)(\text{in}_{\sigma + \tau} \, 1 \, x)$ and $P \, x$ are convertible. On the other hand, $R(\text{in}_{\sigma + \tau} \, 1 \, x)$ and $P \, x$ are not convertible. Instead, we just have a proof $\rho$ such that

$$\rho \quad R(\text{in}_{\sigma + \tau} \, 1 \, x) \iff P \, x$$
4.3. EXTENSION OF THE PROGRAMMING LOGIC

- Another way to generalise the elimination rule for +-types is to allow \( f \prec g \) to have a \( \Pi \)-type, and not just an \(--\)-type:

\[
\frac{\Gamma \vdash p_1 : \forall x. \sigma. P (in_{\sigma + \tau} \cdot 1 \cdot x)}{\Gamma \vdash p_2 : \forall y. \tau. P (in_{\sigma + \tau} \cdot 2 \cdot y)} \quad \Gamma \vdash P :: \sigma + \tau \rightarrow * \cdot p
\]

This rule can be used to prove properties of inhabitants of \( \sigma + \tau \), e.g.

\[
\forall x : \sigma + \tau \ (\exists x. \sigma. z =_{\sigma + \tau} \text{in}_{\sigma + \tau} \cdot 1 \cdot x) \lor (\exists y. \tau. z =_{\sigma + \tau} \text{in}_{\sigma + \tau} \cdot 2 \cdot y)
\]

Instead of rule (ii), we can simply introduce an axiom

\[
\text{AX}_{\sigma + \tau} : \forall P : \sigma + \tau \rightarrow * \cdot p. \ (\forall x : \sigma. P (\text{in}_{\sigma + \tau} \cdot 1 \cdot x)) \Rightarrow (\forall y : \tau. P (\text{in}_{\sigma + \tau} \cdot 2 \cdot y)) \Rightarrow (\forall z : \sigma + \tau. P (z) \cdot p)
\]

Again, the only difference between having rule (ii) and having the axiom \( \text{AX}_{\sigma + \tau} \) is in the reduction behaviour. The proof \((p_1 \triangleright p_2)(\text{in}_{\sigma + \tau} \cdot 1 \cdot x)\) of the proposition \( P (\text{in}_{\sigma + \tau} \cdot 1 \cdot x) \) \( \beta \)-reduces to \((p_1 \cdot x)\), the proof \((\text{AX}_{\sigma + \tau} P p_1 p_2 (\text{in}_{\sigma + \tau} \cdot 1 \cdot x))\) of the same proposition does not. But, since we are not interested in the reduction behaviour of proofs, this difference does not matter.

So the rules (i) and (ii) are not strictly necessary, and only rule (i) has any advantages (viz. a more powerful intensional equality of propositions). We exclude them for two reasons.

First, if these rules are included, we can no longer use the fact that \( \lambda C_\delta \) is \( \beta \delta \)-strongly normalising to prove strong normalisation of the system. We do not want to have to pay attention to a strong normalisation proof here.

A more fundamental reason is that in chapter 5 the programming language will be extended with a fixpoint operator \( \top \). Types will then be interpreted as cpos, and the datatype \( \sigma + \tau \) will include an "undefined" element \( \bot_{\sigma + \tau} \). Rule (ii) is then no longer sound. The problem with rule (i) is that it does not follow from the reduction rules for \( \top \) whether the predicate \( P \top Q \) is true or false in \( \bot_{\sigma + \tau} \). To define a predicate on the cpo \( \sigma + \tau \) in terms of predicates on \( \sigma \) and \( \tau \), we now also have to choose a value for the predicate in \( \bot_{\sigma + \tau} \). (In the programming language this problem is solved by taking the function \( f \prec g \) to be strict, i.e. the value of \( f \prec g : \sigma + \tau \rightarrow \rho \) in \( \bot_{\sigma + \tau} \) will be \( \bot_\rho \).

As in \( \lambda \omega_L \), in \( \lambda \omega_L^\tau \) we want to use the axioms in AXIOM (definition 3.23) for classical logic and extensionality of functions in the programming language. To reason about the new datatypes some additional axioms are needed.

For \( x \)-types we want axioms stating that pairing is surjective, i.e. that all inhabitants of \( \Pi (l_1. \sigma_1 \ldots l_n. \sigma_n) \) are of the form \((l_1 \rightarrow N_1, \ldots, l_n \rightarrow N_n)\).

Similarly, for \(+\) and \( \Sigma \)-types we want axioms stating that all their inhabitants can be constructed using (one of) the injection(s).

Finally, we introduce an axiom stating that true and false are not equal. Using this axiom we can prove, for any \(+\)-type, that \( \text{in}_{\Pi(l_1. \sigma_1 \ldots l_n. \sigma_n)} \cdot l_i \cdot N_i \) and \( \text{in}_{\Sigma(l_1. \sigma_1 \ldots l_n. \sigma_n)} \cdot l_j \cdot N_j \) are not equal if \( l_i \neq l_j \). To do this, define a function \( f : \Sigma(l_1. \sigma_1 \ldots l_n. \sigma_n) \rightarrow \text{bool} \) such that \( f (l_i. N_i) \equiv \text{true} \) and \( f (l_j. N_j) \equiv \text{false} \); then by the definition of Leibniz' equality it follows from false \( \neq \) true that

\[
\text{in}_{\Sigma(l_1. \sigma_1 \ldots l_n. \sigma_n)} \cdot l_i \cdot N_i, \neq \text{in}_{\Sigma(l_1. \sigma_1 \ldots l_n. \sigma_n)} \cdot l_j \cdot N_j
\]
4.39 Definition. $AXIOM^+$ is the set of axioms containing

1. **Classic** : $\forall P \cdot \star, (\neg \neg P) \Rightarrow P$
2. **$p_{bool}$** : true $\not\equiv_{bool}$ false,
3. **$AX_{\alpha \rightarrow \tau}$** : $\forall f, g : \alpha \rightarrow \tau. (\forall x \alpha \cdot (f x) = (g x)) \Rightarrow f =_\alpha \tau g$
4. **$AX_{\Pi \alpha \cdot K \cdot \sigma}$** : $\forall f, g : (\Pi \alpha \cdot K \cdot \sigma), (\forall \alpha \cdot K \cdot (f \alpha) =_\sigma (g \alpha)) \Rightarrow f =_{\Pi \alpha \cdot K \cdot \sigma} g$
5. **$AX_{\Sigma \alpha \cdot K \cdot \sigma}$** : $\forall P : \Pi(l_1 : \sigma_1, \ldots, l_n : \sigma_n) \rightarrow \star$

\[ (\forall x_1 : \sigma_1, \ldots, x_n : \sigma_n, P(l_1 \mapsto x_1, \ldots, l_n \mapsto x_n)) \]
\[ \Rightarrow (\forall x : \Pi(l_1 : \sigma_1, \ldots, l_n : \sigma_n). P x) \]

\[ AX_{\Sigma \alpha \cdot K \cdot \sigma} \]
\[ \forall P : \Sigma(l_1 : \sigma_1, \ldots, l_n : \sigma_n) \rightarrow \star \]
\[ (\forall x : \Sigma(l_1 : \sigma_1, \ldots, l_n : \sigma_n) P(x)) \]
\[ \Rightarrow (\forall (\Sigma \alpha \cdot K \cdot \sigma). P x) \]

for all $\sigma =_\tau (\Pi \alpha \cdot K \cdot \sigma), \Pi(l_1 : \sigma_1, \ldots, l_n : \sigma_n), l_0 : \sigma_0), (\Sigma \alpha \cdot K \cdot \sigma) \in \text{Cons}$

Using axioms in $AXIOM^+$ we can, for example prove the propositions $(\forall x : \text{Empty False}), (\forall x : \text{Unit} x =_{\text{Unit unit}})$, and $(\forall x : \text{bool} . x =_{\text{bool true}} \lor x =_{\text{bool false}})$

The axioms in $AXIOM^+$ can be safely used in $\lambda \omega^+_L$.

4.40 Lemma (Consistency of $AXIOM^+$ in $\lambda \omega^+_L$)
False is not provable in a context containing only axioms from $AXIOM^+$

\[ \text{Proof.} \] See lemma 7.27.

4.4 Program and Proof Development

In chapter 3 we gave examples of coupled derivation rules in $\lambda \omega^+_L$, pairs of derivable rules consisting of a type inference rule and a corresponding proof rule for a certain program construction. $\lambda \omega^+_L$ offers many new ways for forming programs in addition to the lambda abstraction and application available in $\lambda \omega^+_S$. For these we can give proof rules to accompany the type inference rules. Some examples are give below

4.41 Lemma (Coupled derivation rule for if - then - else).

The following rules are derivable using axioms from $AXIOM^+$

\[ \Gamma \vdash b \cdot \text{bool} \]
\[ \Gamma \vdash \rho \cdot \star, \Gamma \vdash R : \rho \rightarrow \star_p \]
\[ \Gamma \vdash M : \rho \]
\[ \Gamma \vdash N : \rho \]
\[ \Gamma \vdash \text{if } b \text{ then } M \text{ else } N : \rho \]

\[ \Gamma \vdash R : \rho \rightarrow \star_p \]
\[ \Gamma, p : (b =_{\text{bool true}}) \vdash R M \]
\[ \Gamma, p : (b =_{\text{bool false}}) \vdash R N \]
\[ \Gamma \vdash \text{if } b \text{ then } M \text{ else } N \]
(When we present such coupled derivation rules as above, it is left implicit that the premisses of the type inference rule are also premisses of the proof rule. Repeating all these premisses would be tedious. In this particular case, just the premiss \( \Gamma \vdash \rho : * \) is needed for the proof rule to be derivable.)

**Proof.** Showing that the type inference rule (on the left) is derivable is trivial (as will be the case in the examples that follow). To show that the proof rule (on the right) is derivable, two axioms from \( AXIOM^+ \) are needed. Recall that \( \text{bool} \approx Unit + Unit \) and \( Unit \approx \Pi()_* \).

From \( AX_{\Pi()} \) and \( AX_{Unit+Unit} \) it follows that \( \forall b. \text{bool}. b := \text{bool} \ true \lor b : = \text{bool} \ false \) (i).

Then

\[
\begin{align*}
\rho : \sigma, M, N : \rho, b : \text{bool}, R : \rho \to *_p, \\
b = \text{bool} \ true \Rightarrow R M, \\
b = \text{bool} \ false \Rightarrow R N
\end{align*}
\]

\[
\begin{array}{ll}
1 & \rho : \sigma, M, N : \rho, b : \text{bool}, R : \rho \to *_p, \\
2 & b = \text{bool} \ true \\
3 & R M \\
4 & R (\text{if true then } M \text{ else } N) \\
5 & R (\text{if } b \text{ then } M \text{ else } N) \\
6 & b = \text{bool} \ true \Rightarrow R (\text{if } b \text{ then } M \text{ else } N) \\
7 & b = \text{bool} \ false \Rightarrow R (\text{if } b \text{ then } M \text{ else } N) \\
8 & (b = \text{bool} \ false \lor b = \text{bool} \ false) \Rightarrow R (\text{if } b \text{ then } M \text{ else } N) \\
9 & \forall b \in \text{bool}. R (\text{if } b \text{ then } M \text{ else } N)
\end{array}
\]

Similar coupled derivation rules can be given for all the \(+\)-types:

**4.42 Lemma.** (Coupled derivation rule for case)

The following rules are derivable using axioms from \( AXIOM^+ \):

\[
\begin{align*}
\Gamma \vdash \Sigma(l_1: \sigma_1, \ldots, l_n: \sigma_n) : *_p \\
\Gamma \vdash \rho : *_\sigma \\
\Gamma \vdash \Sigma(l_1: \sigma_1, \ldots, l_n: \sigma_n), \tau : \sigma_1 \vdash M_1 : \rho \text{ for } i = 0 \ldots n \\
\Gamma \vdash \text{(case } N \text{ of in } l_1 x_1 \mapsto M_1 | \ldots | \text{in } l_n x_n \mapsto M_n \text{)} \vdash \rho \\
\Gamma \vdash \text{R : } *_p \to *_p, \Gamma, p : \Sigma(l_1: \sigma_1, \ldots, l_n: \sigma_n), \text{in } l_i x_i \vdash R M_i \text{ for } i = 0 \ldots n \\
\Gamma \vdash \text{R (case } N \text{ of in } l_1 x_1 \mapsto M_1 | \ldots | \text{in } l_n x_n \mapsto M_n) \vdash \rho
\end{align*}
\]

Subscripts of in have been omitted here to keep things readable; it is clear from the context what they should be.

**Proof.** Analogous to lemma 4.41, now using \( AX_{\Sigma(l_1: \sigma_1, \ldots, l_n: \sigma_n)} \) to distinguish the cases \( N = \Sigma(l_1: \sigma_1, \ldots, l_n: \sigma_n) \) in \( l_i \; N_i \), where \( i = 1 \ldots n \).

The specification of an abstract datatype \( (\Sigma \sigma : *_\sigma \; \sigma) \) involves a polymorphic predicate \( P : (\Pi x : *_\sigma \; \sigma \to *_p) \). As an example we look at the abstract datatype of boolean lists introduced in example 4.25.
CHAPTER 4. SIMPLE EXTENSIONS

4.43 EXAMPLE. Recall that in example 4.25 the datatype-constructors \( ADT \) and \( F \) were defined as:

\[
F = \lambda \text{boollist} : *s. \begin{cases}
\text{empty} : \text{boolist}, \\
\text{cons} : \text{bool} \rightarrow \text{boollist} \rightarrow \text{boollist}, \\
\text{head} : \text{boolist} \rightarrow \text{bool}, \\
\text{tail} : \text{boolist} \rightarrow \text{boollist}
\end{cases} \rightarrow *s,
\]

\[
ADT = (\Sigma \text{boolist} : *s, F \text{boolist}) : *s
\]

To specify the abstract datatype \( ADT \) of boolean lists we can use the following polymorphic predicate \( P \),

\[
P = \lambda \text{boolist} : *s. \forall \text{boolist}.\ \\
\forall x. \text{tail} x \text{empty} = \text{boolist} \text{in } 2 \text{ unit} \land x.\text{head} x.\text{empty} = \text{bool} \text{in } 2 \text{ unit} \\
\land (\forall b \text{ bool, } x \text{ boolist}. x.\text{tail}(x.\text{cons} b ) = \text{boolist} \text{in } 1 \text{ unit} \land x.\text{head}(x.\text{cons} b) = \text{bool} \text{in } 1 \text{ unit})
\]

Again, subscripts of \( in \) have been omitted here to keep things readable.

An implementation (\( \text{in}_{ADT} \tau N \)) \( ADT \) of the abstract datatype is correct if we can give a proof of \( (P \tau N) \). For a program \( \forall \text{boolist} : *s, \lambda x \text{ boolist}. M \) : \( ADT \rightarrow \rho \) we can then prove correctness of \( M \) under the assumption that \( (P \text{boolist} \tau) \).

For the abstype-construction defined in 4.26 we can give the following proof rule:

4.44 LEMMA (Coupled derivation rule for abstype).

The following rules are derivable using axioms from \( AXIOM^+ \):

\[
\Gamma \vdash (\Sigma \alpha : *s. \sigma) : *s \\
\Gamma \vdash \rho : *s \\
\Gamma \vdash \tau : *s \\
\Gamma \vdash N : \sigma; \alpha = \tau \\
\Gamma, \alpha : \tau \vdash M : \rho \\
\Gamma \vdash (\text{abstype } \alpha : *s, \text{ with } \sigma \text{ is } (\text{in}_{\Sigma \alpha : *s. \tau N} ) \text{ in } M ) : \rho
\]

\[
\Gamma \vdash P : (\exists \alpha : \tau N, \sigma \rightarrow *p) \\
\Gamma \vdash R : \rho \rightarrow \tau N \\
\Gamma \vdash P \tau N \\
\Gamma, \alpha : \tau N, x.\sigma \vdash P \alpha x \vdash R M \\
\Gamma \vdash R (\text{abstype } \alpha : *s, \text{ with } x.\sigma \text{ is } (\text{in}_{\Sigma \alpha : *s. \tau N} ) \text{ in } M )
\]

PROOF. To prove that the proof rule is derivable, we have to show that

\[
(\forall x.\sigma, P \alpha x \Rightarrow R M ) \rightarrow R (\text{abstype } \alpha : *s, \text{ with } x.\sigma \text{ is } (\text{in}_{\Sigma \alpha : *s. \tau N} ) \text{ in } M )
\]

can be derived. This immediately follows from the fact that

\[
(\text{abstype } \alpha : *s, \text{ with } x.\sigma \text{ is } (\text{in}_{\Sigma \alpha : *s. \tau N} ) \text{ in } M ) \gg M[\alpha := \tau] \ll N
\]
4.4. PROGRAM AND PROOF DEVELOPMENT

The derivation rules above can be generalised for \((\Sigma \alpha K \sigma)\) with \(K\) an arbitrary kind, simply by taking \(P : (\Pi \alpha K \sigma \rightarrow *_{P})\). The coupled derivation rules for the abstype-construct can also be specialised, to take into account a representation invariant for the abstract datatype. As an example, we first reconsider the specification for \(ADT\):

4.45 EXAMPLE. The specification given for \(ADT\) in example 4.43 can be improved by requiring that there is a representation invariant \(I : \text{boolist} \rightarrow *_{P}\) which holds for \text{empty} and is preserved by \text{cons} and \text{tail}.

\[
P = \lambda \text{boolist} : *_{s}. \lambda I : \text{boolist} \rightarrow *_{s}. \lambda x : \text{boolist}.
I x. \text{empty} \land x. \text{tail} x. \text{empty} = \text{boolist in. 2 unit} \land x. \text{head} x. \text{empty} = \text{bool} \text{ in. 2 unit}
\land (\forall \text{bool}, l \text{ boolist})
(I l) \Rightarrow (x. \text{tail}(x. \text{cons} b l) = \text{boolist in. 1 l} \land x. \text{head}(x. \text{cons} b l) = \text{bool} \text{ in. 1 b}
\land I (x. \text{tail} l) \land I (x. \text{cons} b l))
: \Pi \text{boolist} : *_{s}. (\text{list} \rightarrow *_{P}) \rightarrow (\text{boolist} \rightarrow *_{P})
\]

Compared with the specification given in example 4.43, the conditions "\(x. \text{tail}(x. \text{cons} b l) = l\)" and "\(x. \text{head}(x. \text{cons} b l) = b\)" now only have to hold for lists \(l\) that satisfy the representation invariant \(I\). Now an implementation \((\text{in}_{ADT} \tau N)\) \(ADT\) is correct if we can give an invariant \(I \cdot \tau \rightarrow *_{P}\) for which there is a proof of \((P \tau I N)\)

Recall that in section 3.4.3 we discussed the annotation for datatype-constructors. The prop-constructor \(P\) annotates the datatype-construct \(F : *_{s} \rightarrow *_{s}\). Note that the type of \(P\) is indeed \(\text{type-of-lift}_{*_{s} \rightarrow *_{s}}(F)\) (as defined in definition 3.31). \(\square\)

For the abstype-construct another proof rule can now be given:

4.46 LEMMA (Coupled derivation rule for abstype).

The following rules are derivable using axioms from \(AXIOM^+\):

\[
\begin{align*}
\Gamma & \vdash (\Sigma \alpha *_{s} \sigma) \rightarrow *_{s} \\
\Gamma & \vdash \rho : *_{s} \\
\Gamma & \vdash \tau \rightarrow *_{s} \\
\Gamma & \vdash N : \sigma[\alpha := \tau] \\
\Gamma, \alpha *_{s}, x \sigma & \vdash M : \rho \\
\Gamma & \vdash \tau (\text{abstype } \alpha *_{s} \text{ with } x \sigma \text{ is } (\text{in}_{\Sigma \alpha *_{s} \sigma} \tau N) \text{ in } M) \cdot \rho \\
\Gamma & \vdash \sigma : *_{p}, \alpha \rightarrow *_{s} (\rightarrow \sigma \rightarrow *_{P}) \\
\Gamma & \vdash R : \rho \rightarrow *_{P} \\
\Gamma & \vdash I : \tau \rightarrow *_{P} \\
\Gamma & \vdash P \tau I N \\
\Gamma, \alpha *_{s}, I \alpha & \vdash *_{P}, x \sigma, p_{x} \text{ P } \alpha I x. \vdash R M \\
\Gamma & \vdash R (\text{abstype } \alpha *_{s} \text{ with } x \sigma \text{ is } (\text{in}_{\Sigma \alpha *_{s} \sigma} \tau N) \text{ in } M)
\end{align*}
\]

PROOF. Similar to lemma 4.44 \(\square\)

Again, these derivation rules can be generalised to \((\Sigma \alpha K \sigma)\) with \(K\) an arbitrary kind. Then we have to take \(P : (\Pi \alpha K \text{ type-of-lift}_{*_{P}}(\alpha) \rightarrow (\sigma \rightarrow *_{P}))\) and \(I \text{ type-of-lift}_{*_{P}}(\alpha)\).
CHAPTER 4  SIMPLE EXTENSIONS

The coupled derivation rules are all *compositional* rules, i.e. they deduce the type and the correctness of a program from the type and correctness of its component parts. To prove correctness of programs we may also want to use transformation rules, i.e. using equalities between programs to replace (sub)programs by equal ones. Using axioms from AXIOM+ many equalities can be derived in \( \lambda \omega^f_2 \).

4.47 Definition (composition). Composition for programs is defined by the following context \( \Gamma_{\text{composition}} \):

\[
\begin{align*}
\circ & = \lambda \alpha, \beta, \gamma \cdot \lambda g \beta \rightarrow \gamma. \lambda f \alpha \rightarrow \beta. \lambda x: \alpha. \, g \,(f \, x) \\
& = \Pi \alpha, \beta, \gamma \cdot \beta \rightarrow \gamma. \lambda \gamma: \alpha. \, (\beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma) .
\end{align*}
\]

\( \circ \) will be written *infix*, without its three type parameters. So we write \( g \circ f \) for \( (\circ \, \alpha \, \beta \, \gamma \rightarrow \beta \rightarrow \gamma \rightarrow \alpha \rightarrow \beta \rightarrow \gamma) \, \beta \rightarrow \gamma \rightarrow \alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma) \rightarrow g \, (f \, x) \).

It is not difficult to prove the transformation rule for distributing \( \circ \) over \( \vartriangleright \):

4.48 Lemma. The following proposition is provable using axioms from AXIOM+

\[ \forall \rho_1, \rho_2, \tau, \sigma \cdot s, \, f \, \rho_1 \rightarrow \sigma, \, g \, \rho_2 \rightarrow \sigma, \, h: \sigma \rightarrow \tau \quad h \circ (f \, \vartriangleright \, g) = \rho_1, \rho_2 \rightarrow \tau \, (h \circ f) \, \vartriangleright \, (h \circ g) \]

Proof:

\[
\begin{array}{l}
1. \quad \rho_1, \rho_2, \tau, \sigma \cdot s, f \, \rho_1 \rightarrow \sigma, g : \rho_2 \rightarrow \sigma, h : \sigma \rightarrow \tau \\
2. \quad x : \rho_1 \\
3. \quad (h \circ (f \, \vartriangleright \, g)) (m_{\rho_1, \rho_2} \, x) = \tau (h \circ f) \, \vartriangleright \, (h \circ g)) (m_{\rho_1, \rho_2} \, x) \quad \text{both sides \( \beta \)-reduce} \\
4. \quad \forall x : \rho_1. \, (h \circ (f \, \vartriangleright \, g)) (m_{\rho_1, \rho_2} \, x) = \tau (h \circ f) \, \vartriangleright \, (h \circ g)) (m_{\rho_1, \rho_2} \, x) \quad 3 \quad \text{to \( h \, (f \, x) \)-reduce} \\
5. \quad \forall y : \rho_2. \, (h \circ (f \, \vartriangleright \, g)) (m_{\rho_1, \rho_2} \, y) = \tau (h \circ f) \, \vartriangleright \, (h \circ g)) (m_{\rho_1, \rho_2} \, y) \quad 4, 5, \text{AX} \rho_1, \rho_2 \\
6. \quad \forall z : \rho_1 + \rho_2. \, (h \circ (f \, \vartriangleright \, g)) (m_{\rho_1, \rho_2} \, z) = \tau (h \circ f) \, \vartriangleright \, (h \circ g)) (m_{\rho_1, \rho_2} \, z) \quad 4, 5, \text{AX} \rho_1, \rho_2 \\
7. \quad h \circ (f \, \vartriangleright \, g) = \rho_1, \rho_2 \rightarrow \tau \, (h \circ f) \, \vartriangleright \, (h \circ g) \quad 6, \text{AX} \rho_1, \rho_2 \rightarrow \tau
\end{array}
\]

Many such transformation rules can be proved. For instance, for the distribution of composition over \( \vartriangleright \) (if then else):

4.49 Lemma. The following propositions are provable using axioms from AXIOM+

\[
\begin{align*}
1. \forall b : \text{bool}. \, \forall \rho, \sigma, \tau \cdot s. \forall f, g : \sigma \rightarrow \tau, \forall h : \rho \rightarrow \sigma. \quad (\text{if } b \text{ then } f \text{ else } g) \circ h = \rho \rightarrow \tau \quad \text{if } b \text{ then } h \circ f \text{ else } g \circ h \\
2. \forall b : \text{bool}. \, \forall \rho, \sigma, \tau \cdot s. \forall h : \rho \rightarrow \sigma. \forall f, g : \rho \rightarrow \sigma. \quad h \circ (\text{if } b \text{ then } f \text{ else } g) = \rho \rightarrow \tau \quad \text{if } b \text{ then } h \circ f \text{ else } h \circ g
\end{align*}
\]

By the definition of \( \text{bool} \) and (if then else), the second part of this lemma is an instantiation of the previous lemma.
Chapter 5

Recursion

Recursive datatypes and recursive programs are essential in any typed functional programming language. In this chapter the programming language is extended with recursion at both the level of datatypes and the level of programs. The new programming language $\lambda\omega_3^+$ is the extension of $\lambda\omega_3^+$ with two new primitives, namely a type constructor $\mu$ to form recursive datatypes and a fixpoint combinator $Y$ to form recursive programs.

The extension with unrestricted recursion drastically changes the nature of the programming language. It now offers the full power of the untyped lambda calculus. The price for this unrestricted recursion is that the programming language now includes non-terminating programs: programs of type $\sigma \rightarrow \tau$ are now partial functions from $\sigma$ to $\tau$. This affects the semantics of the programming language and (hence) the way we reason about programs in the programming logic.

In chapter 8 the semantics of the programming language with recursion is discussed. Datatypes can no longer be interpreted as sets. Instead, they will be interpreted as cpos. This means that domain theory can be used as the basis for reasoning about the new programming language. This is the conventional way of reasoning about non-termination and partial objects; the best known example of a programming logic based on domain theory is LCF [GMW79].

The programming logic $\lambda\omega_3^+$ will be extended to a system $\lambda\omega_3^c$. No new logical primitives are needed in $\lambda\omega_3^c$. Some domain-theoretic notions, such as the ordering $\sqsubseteq$ on programs, and their properties are needed, but these can all be expressed using the primitives of $\lambda\omega_3^c$.

It will be shown that all the domain theory that is needed can be formalized inside the system $\lambda\omega_3^c$. The higher-order nature of the logic turns out to be useful for this. In particular, it enables us to define the notion of admissibility (or chain-completeness) for predicates in the system. Consequently, the logic is more powerful than LCF, because there this notion has to live in the meta-theory.

The structure of this chapter is similar to the previous ones. In section 5.1 the programming language $\lambda\omega_3^c$ is defined. In section 5.2 the associated programming logic $\lambda\omega_3^c$ is defined, and a formalisation of domain theory in this system is given. Finally, in section 5.3 we give some examples of ways to prove correctness of programs in $\lambda\omega_3^c$. 
5.1 Extension of the Programming Language

In this section we define the program language \( \lambda \omega^\mu \), which extends the system \( \lambda \omega^+ \) defined in the previous chapter with recursive datatypes and recursive programs.

For recursive datatypes a new type constructor \( \mu \) is introduced, with which recursive types of the form \( (\mu \alpha \times \sigma) \) can be formed. A recursive type \( (\mu \alpha \times \sigma) \) is the solution of the recursive type equation

\[
\alpha \cong \sigma,
\]

where \( \alpha \in \text{Var}^\omega \) is a datatype-variable. In other words, the datatype \( (\mu \alpha \times \sigma) \) is isomorphic with its unfolding \( \alpha := (\mu \alpha \times \sigma) \). This isomorphism is given by two operations \( \text{unfold}_{\mu \alpha \times \sigma} \) and \( \text{fold}_{\mu \alpha \times \sigma} \), which map inhabitants of a recursive type to its unfolding and back. These operations come with the following reduction rules:

\[
\begin{align*}
\text{unfold}_{\mu \alpha \times \sigma} (\text{fold}_{\mu \alpha \times \sigma} M) & \xrightarrow{\mu} M \\
\text{fold}_{\mu \alpha \times \sigma} (\text{unfold}_{\mu \alpha \times \sigma} M) & \xrightarrow{\mu} M
\end{align*}
\]

It follows from these reduction rules that \( \text{fold}_{\mu \alpha \times \sigma} \) and \( \text{unfold}_{\mu \alpha \times \sigma} \) do indeed give an isomorphism.

An alternative to operations \( \text{fold}_{\mu \alpha \times \sigma} \) and \( \text{unfold}_{\mu \alpha \times \sigma} \) is to identify a recursive type and its unfolding. Later, in discussion 5.10, it is explained why we have chosen not to do this.

Recursion at program level is provided by a fixpoint-operator \( Y \),

\[
Y (\Pi \alpha \rightarrow (\alpha \rightarrow \alpha))
\]

with the reduction rule

\[
Y \sigma f \xrightarrow{\mu} f (Y \sigma f)
\]

In fact, there is no real need to add a fixpoint-operator as a primitive. Because we have solutions of all recursive type equations — including for instance a solution \( (\mu \alpha \times \sigma) \) of \( \alpha \cong \alpha \rightarrow \alpha \) — we have the full power of the untyped lambda calculus, and fixpoint-operators can be defined. An example of this is given later, in example 5.2. The reason for including a fixpoint-operator \( Y \) as a primitive is that is plays such an important role. Also, a direct implementation of \( Y \) will be more efficient than any definable fixpoint-operator.

The programming language \( \lambda \omega^\mu \) and its extension with definitions \( \lambda \omega^\mu_{\text{def}} \) are now defined as follows:

5.1 Definition \( (\lambda \omega^\mu_{\text{def}}) \)

The programming language \( \lambda \omega^\mu_{\text{def}} \) is the extension of \( \lambda \omega^+ \) with the pseudoterms, reduction rules and type inference given below. The set of pseudoterms is extended as follows

\[
T := \cdot \mid (\mu \alpha \times \sigma) T \mid \text{fold}_{\mu \alpha \times \sigma} T \mid \text{unfold}_{\mu \alpha \times \sigma} \sigma T \mid Y
\]

The following reduction rules are added

\[
\begin{align*}
\text{unfold}_{\mu \alpha \times \sigma} (\text{fold}_{\mu \alpha \times \sigma} M) & \xrightarrow{\mu} M \\
\text{fold}_{\mu \alpha \times \sigma} (\text{unfold}_{\mu \alpha \times \sigma} M) & \xrightarrow{\mu} M \\
Y \sigma f & \xrightarrow{\mu} f (Y \sigma f)
\end{align*}
\]
and the following type inference rules

\[
\begin{align*}
\text{(\(\mu\text{form}\))} & \quad \Gamma, \alpha: * \vdash \sigma : * \\
\text{(\(\mu\text{intro}\))} & \quad \Gamma \vdash M \quad \sigma[\alpha := (\mu\alpha:*\sigma)] \\
\text{(\(\mu\text{elim}\))} & \quad \Gamma \vdash M : (\mu\alpha:*\sigma) \\
\text{\(\eta\text{intro}\))} & \quad \epsilon \vdash \gamma : (\Pi\alpha:*\sigma, (\alpha \to \alpha) \to \alpha)
\end{align*}
\]

Unlike the reduction rules for +, \(\times\) and \(\Sigma\) introduced in the previous chapter, the new reduction rules are not included in the notion of \(\beta\)-reduction, but instead we have a separate notion of \(\mu\)-reduction. As a result, \(\beta\) and \(\beta\)-reduction are kept strongly normalising. At this point there is no reason for having separate reduction relations \(\triangleright_{\beta}\) and \(\triangleright_{\mu}\). But for the programming logic \(\text{\(\Lambda\omega_{T}^{\omega}\)}\) introduced in section 5.2 it will be important that \(\beta(\delta)\)-reduction is kept strongly normalising (or rather that \(\beta(\delta)\)-conversion is kept decidable). This will be explained in more detail in the next section in discussion 5.10. For the same reason we do not identify recursive types with their unfoldings. Then \(\beta\)-reduction would also not be strongly normalising and \(\beta\)-conversion would be undecidable.

The two reduction rules for \(\text{\(\text{fold}_{\mu\alpha:*\sigma}\)}\) and \(\text{\(\text{unfold}_{\mu\alpha:*\sigma}\)}\) can be seen as a \(\beta\)- and an \(\eta\)-reduction rule. It is the convention that the reduction of a term formed by an introduction construction applied to an elimination construction is called \(\beta\)-reduction, and that the reduction of a term formed by an elimination construction applied to an introduction construction is called \(\eta\)-reduction. For example, in the \(\beta\)-reduces \((\lambda x:A. b)\ a\) and \((a, b)\ 1\) elimination constructions - application and selection - are applied to introduction constructions – abstraction and pairing. In the \(\eta\)-reduces \((\lambda x:A. b\ x)\) and \((a, 1, a, 2)\) introduction constructions are applied to elimination constructions.

By this convention \(\text{\(\text{unfold}_{\mu\alpha:*\sigma}\)}\) \((\text{\(\text{fold}_{\mu\alpha:*\sigma}\)}\ M) \triangleright_{\mu} M\) is the \(\beta\)-reduction rule, and \(\text{\(\text{fold}_{\mu\alpha:*\sigma}\)}\ \text{\(\text{unfold}_{\mu\alpha:*\sigma}\)}\ M \triangleright_{\mu} M\) the \(\eta\)-reduction rule for \(\mu\)-types. Of the two reduction rules for \(\text{\(\text{fold}_{\mu\alpha:*\sigma}\)}\) and \(\text{\(\text{unfold}_{\mu\alpha:*\sigma}\)}\) it is this "\(\beta\)"-reduction rule that appears to be the crucial one. For instance, in example 5.2 below it is this reduction rule that is needed to produce an infinite reduction sequence. We do not know if there are infinite reduction sequences in which the "\(\eta\)"-rule \(\text{\(\text{fold}_{\mu\alpha:*\sigma}\)}\ \text{\(\text{unfold}_{\mu\alpha:*\sigma}\)}\ M \triangleright_{\mu} M\) is used, but the "\(\beta\)"-rule \(\text{\(\text{unfold}_{\mu\alpha:*\sigma}\)}\ \text{\(\text{fold}_{\mu\alpha:*\sigma}\)}\ M \triangleright_{\mu} M\) is not used.

\[5.2\text{ \ Example} \quad \text{An example of a fixpoint-operator for programs that is now typable is}
\]

\[
Y_{\text{Turing}} = \lambda \alpha:* \quad \tau = (\mu \beta:*\sigma, \beta : (\alpha \to \alpha) \to \alpha) : * \quad
\]

\[
\text{in } w = (\lambda t:T. \lambda f:(\alpha \to \alpha). f((\text{\(\text{unfold}_{\tau}\)} \ x) \times f)) \\
\quad : \tau \to (\alpha \to \alpha) \to \alpha
\]

\[
\text{in } w (\text{\(\text{fold}_{\tau}\)} w) \\
(\Pi \alpha:* \quad (\alpha \to \alpha) \to \alpha)
\]

This is a typed version of Turing's fixpoint combinator for the untyped lambda calculus, which we can get simply by erasing all the type information and the operations \(\text{\(\text{fold}_{\tau}\)}\) and \(\text{\(\text{unfold}_{\tau}\)}\).
It is easy to verify that $Y_{\text{ Turing }}$ is indeed a fixed-point operator:

\[
Y_{\text{ Turing }} \cdot f \triangleq \beta \delta \tau = \in \ w = \in w (\text{fold}_r w) f
\]

\[
\delta \gamma \tau = \in \ w = \in (\lambda y. f (\text{unfold}_r y) f) \text{ (fold}_r w f
\]

\[
\delta \gamma \mu \tau = \in \ w = \in f (\text{unfold}_r (\text{fold}_r w)) \text{ (fold}_r w f)
\]

\[
\delta \gamma \mu \tau = \in \ w = \in f (w (\text{fold}_r w) f)
\]

\[
\gamma \delta \in (Y_{\text{ Turing }} \cdot f)
\]

In contrast to the programming languages introduced earlier, all datatypes are now inhabited, as is shown below. In $\lambda \omega_s$ and $\lambda \omega^+_s$ there are no programs inhabiting the datatype $(\Pi \alpha \cdot \ast_s, \alpha)$, but in $\lambda \omega^+_s$ there are, as the following definition demonstrates.

5.3 Definition. The context $\Gamma_\perp$ is

\[
\perp = (\lambda \alpha \cdot \ast_s Y \alpha (\lambda f : \alpha. x)) : (\Pi \alpha \cdot \ast_s, \alpha)
\]

Consequently, any datatype $\sigma$ has at least one inhabitant, namely $(\perp \sigma)$. Given the reduction rule for $Y$, it is easy to see that this program does not have a normal form. The interpretation of $(\perp \sigma)$ in the cpo-model given in chapter 8 will of course be the bottom element of the cpo that is the interpretation of $\sigma$.

We will always assume that $\Gamma_\perp$ is part of the context. The type parameter of $\perp$ will be written as a subscript, i.e., we write $\perp_\sigma$ for $(\perp \sigma)$.

With the type constructor $\mu$ we can at last make "real" datatypes, such as a datatype for the natural numbers:

5.4 Example. The context $\Gamma_{\text{nat}}$ defining the datatype of natural numbers is

\[
\text{nat } = (\mu \alpha \cdot \ast_s \text{ Unit } + \alpha) : \ast
\]

\[
0 = \text{fold}_{\text{nat}} (\text{inl Unit } + \text{nat} : \text{nat}) : \text{nat}
\]

\[
S = \lambda n : \text{nat} \text{ fold}_{\text{nat}} (\text{inl Unit } + \text{nat} : 2 n) : \text{nat} \rightarrow \text{nat}
\]

\[
P = \lambda n : \text{nat} \downarrow (\lambda r \text{ Unit } 0, \lambda m : \text{nat } m) (\text{unfold}_{\text{nat}} m) : \text{nat} \rightarrow \text{nat}
\]

Of course, the price for having all recursive types and a fixed point combinator is that this datatype $\text{nat}$ not only has inhabitants $S^n 0$ with $n \in \mathbb{N}$, but also an inhabitant $\perp_\text{nat}$

Properties of $\lambda \omega^n_s$ and $\lambda \omega^n_x$

The type inference rule $(\mu \text{form})$ gives new datatypes, the other new type inference rules give new programs. The sets of pseudoterms $\text{Cons}$ and $\text{Prog}$ have to be extended accordingly:

5.5 Definition. The sets of pseudoterms $\text{Cons}$ and $\text{Prog}$ defined in definition 4.28 for $\lambda \omega^+_s$ are extended as follows

\[
\text{Cons } = \text{... } | (\mu \text{ Var }^\Gamma : \ast_s \text{ Cons})
\]

\[
\text{Prog } ::= \text{... } | \text{fold}_{\mu \alpha \ast_s} \sigma \text{ Prog } | \text{unfold}_{\mu \alpha \ast_s} \sigma \text{ Prog } | Y
\]
5.1 EXTENSION OF THE PROGRAMMING LANGUAGE

Then:

5.6 LEMMA (Classification for $\lambda \omega_\mu$).

1. If $\Gamma \vdash K : \Box$, then $K \in \text{Kind}$.
2. If $\Gamma \vdash \sigma \cdot K : \Box$, then $\sigma \in \text{Cons}$.
3. If $\Gamma \vdash M : \sigma : \ast$, then $M \in \text{Prog}$.

PROOF Exactly the same way as lemmas 3.5 and 4.29.

With the exception of strong normalisation, the systems $\lambda \omega_\mu$ and $\lambda \omega_\delta^\mu$ inherit all the properties of $\lambda \omega_\forall$ and $\lambda \omega_\delta$. And even though $\beta_\mu$- and $\beta_\mu \delta$-reduction are not strongly normalising, strong normalisation for $\beta$- and $\beta_\delta$-reduction is preserved.

Only programs can $\mu$-reduce, the kinds, datatypes and other datatype-constructors cannot. Because of this, types are not just unique up $\beta_\mu(\delta)$-conversion, but they are even unique up to $\beta(\delta)$-conversion.

5.7 THEOREM (Properties of $\lambda \omega_\mu^\ast$).

- $\text{CR}_{\beta_\mu}$: $\beta_\mu$-reduction is Church-Rosser
- $\text{SR}_{\beta_\mu \delta}$: if $\Gamma \vdash b : B$ and $b \succ \beta_\mu b'$ then $\Gamma \vdash b' : B$.
- $\text{UT}_\beta$: if $\Gamma \vdash b : B$ and $\Gamma \vdash b : B'$ then $B \simeq_\sigma B'$.
- $\text{SN}_\beta$: if $\Gamma \vdash b : B$ then $b$ and $B$ are $\beta$-strongly normalising

PROOF As for PTSs with $+$, $\times$ and $\Sigma$ (Lemma 4.13), Church-Rosser can be proved using the theory of Combinatory Reduction Systems (CRSs). The relation $\succ \beta_\mu$ is not an orthogonal CRS, because it has so-called overlapping redices of the form

$\text{fold}_{\mu \ast \ast} \circ (\underline{\text{unfold}}_{\mu \ast \ast} \circ \text{fold}_{\mu \ast \ast} \circ M) .

This term contains two overlapping redices, indicated by the over- and underlining. However, contracting either redex result in the same term, namely $(\text{fold}_{\mu \ast \ast} \circ M)$, so $\succ \beta_\mu$ is a weakly orthogonal CRS. Confluence for weakly orthogonal CRSs is proved in [Raa92].

$\text{SN}_\beta$ for $\lambda \omega_\mu^\ast$ follows from $\text{SN}_\beta$ for $\lambda \omega_\forall^\ast$. All the terms that are typable in $\lambda \omega_\mu^\ast$ are - with a slightly different syntax for the $\mu$-types and with extra parameters for $(\text{fold}_{\mu \ast \ast} \circ \sigma$ and $\underline{\text{fold}}_{\mu \ast \ast} \circ \sigma$ - also typable in $\lambda \omega_\forall^\ast$ in the following context.

$\ast$ : $(\ast, \ast) \rightarrow \ast,$

$\text{fold}$ : $\Pi F : \ast \rightarrow \ast . \ F (\mu F) \rightarrow \mu F$,

$\underline{\text{unfold}}$ : $\Pi F : \ast \rightarrow \ast . \ \mu F \rightarrow F (\mu F)$,

$\Upsilon : \Pi \sigma : \ast . \ (\sigma \rightarrow \sigma) \rightarrow \sigma$

It then follows from $\text{SN}_\beta$ for $\lambda \omega_\forall^\ast$ that all these terms are $\beta$-strongly normalising.

The properties SR and UT can be proved in the standard way, i.e. by the same inductions used in chapter 2 for PTSs (and in chapter 4 for PTSs with $+$, $\times$ and $\Sigma$).
5.8 Theorem (Properties of $\omega^\mu_\delta$).

- **CR$\_\delta\mu$:** $\delta\mu\delta$-reduction is Church-Rosser.
- **SR$\_\delta\mu$:** if $\Gamma \vdash b : B$ and $b \rightarrow_{\delta\mu\delta} b'$ then $\Gamma \vdash b' : B$.
- **UT$\_\delta\mu$:** if $\Gamma \vdash b : B$ and $\Gamma \vdash b' : B'$ then $B \simeq_{\delta\mu} B'$.
- **SN$\_\delta\mu$:** if $\Gamma \vdash b : B$ then $b$ and $B$ are $\delta\mu$-strongly normalising in $\Gamma$.
- **Elimination of definitions:** if $\Gamma \vdash a : A$ in $\omega^\mu_\delta$ then $\text{dnf}(\Gamma) \vdash \text{dnf}(\delta\mu\delta) \cdot \text{dnf}(A)$ in $\omega^\mu_\delta$.

**Proof.** SN$\_\delta\mu$ can be proved in the same way as SN$\_\delta$ for $\omega^\mu_\delta$ in the previous theorem. All the other properties can be proved in exactly the same way as in chapter 2 for DPTSs and in chapter 4 for DPTSs with $+, \times$ and $\Sigma$. □
5.2 Extension of the Programming Logic

In this section the programming logic \( \lambda \omega^\mu_L \) is defined, in which we can reason about the programming language \( \lambda \omega^\mu_L \).

As we mentioned earlier, domain theory is used as the basis for reasoning about \( \lambda \omega^\mu_L \). However, no notions or axioms from domain theory - such as the cpo ordering \( \sqsubseteq \) and its properties - have to be included as primitives in the system \( \lambda \omega^\mu_L \). Instead, all the domain theory that is needed will be formalised in the system, i.e., we will give a context declaring and defining all the domain-theoretic notions and axioms that are needed. No new logical primitives other than the ones already offered by \( \lambda \omega^\mu_L \) are needed for this, so as the system \( \lambda \omega^\mu_L \) we can simply take the system \( \lambda \omega^\mu_L \) with its \( \lambda \omega^\mu_L \)-subsystem extended to \( \lambda \omega^\mu_L \):

5.9 Definition (\( \lambda \omega^\mu_L(\delta) \))

The programming logic \( \lambda \omega^\mu_L(\delta) \) is the extension of the system \( \lambda \omega^\mu_L(\delta) \) with the pseudoterms, reduction and type inference rules given in definition 5.1.

5.10 Discussion (\( \beta(\delta) \)-conversion vs \( \mu \)-conversion of types).

In \( \lambda \omega^\mu_L \) there is an inference rule to \( \beta \)-convert types, namely the rule

\[
(\beta\text{conv}) \quad \Gamma \vdash b : B \quad \Gamma \vdash B : s \quad B \cong_\beta B' \quad \therefore \Gamma \vdash b : B'
\]

which allows a type to be replaced by a \( \beta \)-convertible one. In \( \lambda \omega^\mu_L \) we have the more powerful conversion rule \( (\beta\delta\text{conv}) \), which allows the \( \beta\delta \)-conversion of types. With this rule, the following inference rule is derivable.

\[
(\delta\text{conv}) \quad \Gamma \vdash b : B \quad \Gamma \vdash B : s \quad \Gamma \vdash B \cong_\delta B' \quad \therefore \Gamma \vdash b : B'
\]

It is easy to see that, because of these rules, type checking involves testing convertibility of types. For example, to check if \( r : A \vdash x : A' \) is derivable in \( \lambda \omega^\mu_L(\delta) \) we have to check among other things - if \( A \) and \( A' \) are \( \beta(\delta) \)-convertible. Because \( \beta(\delta) \)-reduction is Church-Rosser and strongly normalising, \( \beta(\delta) \)-conversion is decidable.

The type inference rules of \( \lambda \omega^\mu_L \) do not include a \( \mu \)-conversion rule

\[
(\mu\text{conv}) \quad \Gamma \vdash b : B \quad \Gamma \vdash B : s \quad B \cong_\mu B' \quad \therefore \Gamma \vdash b : B'
\]

which allows a type to be replaced by a \( \mu \)-convertible one. In the programming language \( \lambda \omega^\mu_L \) there is no use for this rule, because in \( \lambda \omega^\mu_L \) there are no types that can be \( \mu \)-reduced (only programs can be \( \mu \)-reduced). But in \( \lambda \omega^\mu_L \) there are types that \( \mu \)-reduce, because programs can occur as subexpressions of propositions. For example, if \( P : \sigma \rightarrow *_p \) then \( P (Y \sigma f) \) is a proposition that \( \mu \)-reduces to \( P (f (Y \sigma f)) \). The rule \( (\mu\text{conv}) \) could be used to deduce \( \Gamma \vdash p : P (Y \sigma f) \) from \( \Gamma \vdash p : P (f (Y \sigma f)) \) and vice versa, and hence it could be used to prove \( (Y \sigma f) =_\sigma f (Y \sigma f) \).

The reason for excluding the rule \( (\mu\text{conv}) \) is that it would make type inference undecidable, because \( \mu \)-conversion is undecidable. To be precise, it would make type inference for proof terms undecidable, i.e., it would no longer be decidable if \( \Gamma \vdash p : P \) for proof terms \( p \in \text{Proof} \) and propositions \( P \in \text{PCons} \).
For the same reason, we do not identify a recursive type and its unfolding. This would make the operations \( \text{fold}_{\mu^*}, \sigma \) and \( \text{unfold}_{\mu^*}, \sigma \) redundant, but it would also make type inference undecidable, because \( \beta \)-conversion is then no longer decidable.

The rules \( (\beta \text{conv}) \) and \( (\delta \text{conv}) \) can be used to prove that all \( \beta \delta \)-convertible programs are Leibniz' equal (see page 41, where the notion of Leibniz' equality of programs is introduced). Because we do not have the rule \( (\mu \text{conv}) \), we cannot prove Leibniz' equality of \( \mu \)-convertible programs in the same way. The properties \( \text{fold}_{\mu^*}, \sigma \) (\( \text{unfold}_{\mu^*}, \sigma \) \( M \)) \( =_{\mu^*} \sigma \) \( M \), \( \text{unfold}_{\mu^*}, \sigma \) (\( \text{fold}_{\mu^*}, \sigma \) \( N \)) \( =_{\mu^*} \sigma \) \( \sigma [\alpha =_{\mu^*} \sigma] N \), and \( (Y \sigma f) =_{\sigma} f (Y \sigma f) \) will have to be introduced as axioms (see definition 5.17).

So, unlike \( \beta \) and \( \delta \)-conversions, any \( \mu \)-conversions that are done in a proof leave a trace in the proof term that represents that proof. Proof terms for the properties mentioned above effectively record all the \( \mu \)-conversions that are done in a proof.

**Properties of \( \lambda \omega^\mu_\beta \) and \( \lambda \omega^\mu_\delta \)**

In the system \( \lambda \omega^\mu_\beta \) we have the same inference rules for prop-kinds, prop-constructors and proofs as in \( \lambda \omega^\mu_\delta \). This means that the context-free syntax for these levels remains unchanged, i.e. for \( \lambda \omega^\mu_\beta \) the sets Pkind, PCons and Proof can be defined by the same context-free grammar given in definition 4.34 for \( \lambda \omega^\mu_\delta \).

The systems \( \lambda \omega^\mu_\beta \) and \( \lambda \omega^\mu_\delta \) inherit all the properties of \( \lambda \omega^\mu_\delta \) and \( \lambda \omega^\mu_\delta \). The Church-Rosser properties for \( \beta \mu \) and \( \beta \mu \delta \) which do not depend on the typing relation have already been proved for \( \lambda \omega^\mu_\mu \) and \( \lambda \omega^\mu_\delta \) in the previous section. Strong normalisation of \( \beta(\delta) \)-reduction for \( \lambda \omega^\mu_\delta \) can be proved in the same way as for \( \lambda \omega^\mu_\delta \). The remaining properties can all be proved by the same inductions used to prove these properties for the previous systems.

5.11 Theorem (Properties of \( \lambda \omega^\mu_\delta \)).

- **CR\( _{\beta \mu} \)**: \( \beta \mu \)-reduction is Church-Rosser.
  - **SR\( _{\beta \mu} \)**: if \( \Gamma \vdash b : B \) and \( \beta \mu \vdash \beta \mu \) \( b' \) then \( \Gamma \vdash b' : B \).
  - **UT\( _{\beta \delta} \)**: if \( \Gamma \vdash b : B \) and \( \Gamma \vdash b : B' \) then \( B \cong_{\delta} B' \).
  - **SN\( _{\beta} \)**: if \( \Gamma \vdash b : B \) then \( b \) and \( B \) are \( \beta \)-strongly normalising.
  - **Conservativity of \( \lambda \omega^\mu_\delta \) over \( \lambda \omega^\mu_\mu \)**
    - if \( \Gamma \vdash a : A \) in \( \lambda \omega^\mu_\delta \) and \( a \in \text{Prog} \cup \text{Cons} \cup \text{Kind} \) then \( \Gamma^{\text{Core}} \vdash a : A \) in \( \lambda \omega^\mu_\mu \).

5.12 Theorem (Properties of \( \lambda \omega^\mu_\delta \)).

- **CR\( _{\beta \mu \delta} \)**: \( \beta \mu \delta \)-reduction is Church-Rosser.
  - **SR\( _{\beta \mu \delta} \)**: if \( \Gamma \vdash b : B \) and \( \beta \mu \delta \vdash \beta \mu \delta \) \( b' \) then \( \Gamma \vdash b' : B \).
  - **UT\( _{\beta \delta \delta} \)**: if \( \Gamma \vdash b : B \) and \( \Gamma \vdash b : B' \) then \( B \cong_{\delta \delta} B' \).
  - **SN\( _{\beta \delta} \)**: if \( \Gamma \vdash b : B \) then \( b \) and \( B \) are \( \beta \delta \)-strongly normalising in \( \Gamma \).
  - **Elimination of definitions**:
    - if \( \Gamma \vdash a : A \) in \( \lambda \omega^\mu_\delta \) then \( \delta \text{nf}(\Gamma) \vdash \delta \text{nf}_f(a) =_{\delta \text{nf}} (A) \) in \( \lambda \omega^\mu_\delta \).
5.2 EXTENSION OF THE PROGRAMMING LOGIC

Formalisation of Domain Theory in $\lambda\omega^n_L$

To reason about recursive programs in $\lambda\omega^n_L$, a context $\Gamma_{\text{CPO}}$ will be defined, which declares the cpo ordering $\sqsubseteq$ and all the properties of $\sqsubseteq$ and of $\bot$. In this context Scott's rule for computational induction - also known as fixpoint induction - will be provable. The model given in chapter 8 gives the justification for the axioms in $\Gamma_{\text{CPO}}$.

First we list the notions from the theory of cpos that have to be formalised.

5.13 DEFINITION (chain, cpo, monotonic, continuous).

Let $A$ be a set, partially ordered by $\sqsubseteq_A$, i.e. $\sqsubseteq_A$ is reflexive, transitive and antisymmetric.

1. a subset $C$ of $A$ is called a chain if it is not empty and if for all $x, y \in C$, $x \sqsubseteq_A y$ or $y \sqsubseteq_A x$.

2. $A$ is called a cpo if every chain $C$ in $A$ has a least upper bound - or limit $\bigvee C$, and it has a least element $\bot_A$ (which is the least upper bound of the empty set in $A$).

Suppose the sets $A$ and $B$, partially ordered by $\sqsubseteq_A$ and $\sqsubseteq_B$, respectively, are cpos.

3. a function $f$ from $A$ to $B$ is called monotonic if for all $x, y \in A$, if $x \sqsubseteq_A y$ then $f(x) \sqsubseteq_B f(y)$.

4. a function $f$ from $A$ to $B$ is called continuous if $f(\bigvee C) = \bigvee \{f(x) \mid x \in C\}$ for every chain $C$ in $A$.

If $A$ be a cpo and $f$ a continuous function from $A$ to $A$, then $f$ has a least fixed point $Y(f)$. This means that $Y(f) = f(Y(f))$, and if $f(x) = x$ then $Y(f) \sqsubseteq_A x$. This least fixed point of $Y(f)$ is the least upper bound of $\{\bot_A, f(\bot_A), f^2(\bot_A), \ldots\}$. The least fixpoint of $f$ is also the least prefixpoint of $f$, so if $f(x) \sqsubseteq_A x$ then $Y(f) \sqsubseteq_A x$.

Scott's fixpoint induction rule - given in lemma 5.15 below - provides a way to reason about least fixpoints. It requires the following definition.

5.14 DEFINITION A predicate $P$ on a set $A$ is called admissible if for every chain $C$ in $A$ for which all elements satisfy $P$ the limit of $C$ also satisfies $P$.

5.15 LEMMA (Fixpoint Induction). Let $A$ be a cpo, $f$ a continuous function from $A$ to $A$, and $P$ an admissible predicate on $A$. If

- $P(\bot_A)$
- for all $x \in A$, if $P(x)$ then $P(f(x))$

then $P(Y(f))$.

A $\lambda\omega^n_L$-context $\Gamma_{\text{CPO}}$ will be defined, which declares an ordering $\sqsubseteq$ on datatypes, and axioms for $\sqsubseteq$ and $\bot$, from which it follows that all datatypes are cpos, that all programs of some type $\sigma \rightarrow \tau$ are continuous (and hence monotonic), and that $\bot$ produces least fixed points. Before this context is defined we first discuss the ingredients one by one.
The most important notion needed is the cpo-ordering \( \sqsubseteq \) on programs. Like Leibniz' equality of programs, introduced in definition 3.21, this is a polymorphic predicate of type \((\Pi \alpha \cdot \lambda \to \alpha \to \alpha)\), i.e.

\[
\sqsubseteq : \Pi \alpha \cdot \lambda \to \alpha \to \alpha
\]

For \( \sqsubseteq \) the same notational conventions are used as for \( = \), i.e. \( \sqsubseteq \) is written infix with its first argument as a subscript. So for instance we write \((M \sqsubseteq \sigma N)\) for \((\sqsubseteq \sigma M \sqsubseteq \sigma N)\).

It is easy to give axioms stating that \( \sqsubseteq \) is reflexive, transitive and antisymmetric, and that all functions are monotonic:

\[
\begin{align*}
\text{refl} & : \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \\
\text{trans} & \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \\
\text{antisym} & \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \\
\text{monotonicity} & \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha
\end{align*}
\]

We also need some properties of the fixpoint-operator \( Y \) provided by the programming language, namely that \((Y \sigma f)\) is the least fixed-point of \( f \) for all \( \sigma \to \sigma \). The axioms below state that \((Y \sigma f)\) is a fixpoint of \( f \) and that it is smaller than any other fixpoint:

\[
\begin{align*}
\text{fix} & \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \\
\text{leastfix} & \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha \quad \forall \alpha \cdot \lambda \to \alpha \to \alpha
\end{align*}
\]

It immediately follows from the axiom leastfix that \((\forall \sigma \cdot \forall \alpha \cdot \bot \sqsubseteq \alpha)\), with \( \bot \) as defined in definition 5.3. So every datatyped \( \alpha \) has a least element, namely the program \( \bot \).

We still need the property that all chains have least upper bounds, and that all functions are continuous. Expressing these properties in \( \lambda \omega \eta \) requires a bit more work.

First of all, the notion of (least) upper bound of a subset \( \{M_1, \ldots, M_n\} \) of a datatyped \( \sigma \) is needed. Predicates on datatypes will be used to characterise such subsets. The following terms \( UB \) and \( LUB \) express the notions of upper bound and least upper bound of a predicate on a datatype, respectively.

\[
\begin{align*}
\text{UB} & \quad \lambda \alpha \cdot \lambda \sigma \cdot \lambda \xi \cdot \lambda \gamma \cdot \lambda x \cdot \lambda y \cdot \lambda r \cdot \lambda \alpha \cdot \lambda \sigma \cdot \lambda \xi \cdot \lambda \gamma \cdot \lambda x \cdot \lambda y \cdot \lambda r \\
\text{LUB} & \quad \lambda \alpha \cdot \lambda \sigma \cdot \lambda \xi \cdot \lambda \gamma \cdot \lambda x \cdot \lambda y \cdot \lambda r \cdot \lambda \alpha \cdot \lambda \sigma \cdot \lambda \xi \cdot \lambda \gamma \cdot \lambda x \cdot \lambda y \cdot \lambda r
\end{align*}
\]

If \( P : \sigma \to \sigma \), then the proposition \((UB \sigma P x)\) states that \( x \) is an upper bound of the set characterised by \( P \) and \((LUB \sigma P x)\) states that \( x \) is a least upper bound or limit of this set.

The following term defines what is means for a predicate on a datatype to be a chain:

\[
\text{cham} = \lambda \alpha \cdot \lambda \sigma \cdot \lambda C \cdot \alpha \to \sigma \\
(\exists x \in \alpha \cdot C x) \wedge (\forall x \in \alpha \cdot C x \land C y) \Rightarrow x \in \alpha \land y \in \alpha
\]

If \( C \) is predicated on a datatype \( \alpha \), then \((cham \alpha C) \cdot \sigma \) is the proposition "\( C \) is a chain".

Using predicates to characterise sets, and using \( LUB \) and \( cham \) defined above, we then get the following axiom for continuity of all functions:

\[
\begin{align*}
\text{continuity} & \quad \forall \sigma \cdot \forall \tau \cdot \forall y \cdot \sigma \to \tau \cdot \forall C \cdot \sigma \to \tau \cdot \forall \text{lub} \sigma \cdot \forall \text{lub} \tau \\
C' = (\lambda y \cdot \lambda \tau \cdot \exists x \cdot y = x \land C x) \quad \tau \to \sigma \quad \text{in}
(\text{cham} \sigma C) \Rightarrow (LUB \sigma C \text{lub}) \Rightarrow (LUB \tau C' \text{lub}') \Rightarrow \text{g lub} \equiv \text{lub}'
\end{align*}
\]
Here $C' : \tau \to \ast_p$ is the image of $C$ under $g$.

We can now give the last property of $\subseteq$, namely that all chains have a least upper bound:

$$\text{complete} \equiv \forall \alpha \ast_p. \forall C \alpha \to \ast_p. \text{chain } \alpha C \implies (\exists \text{lub } \alpha. \text{LUB } \alpha C \text { lub})$$

Recall that from leastfix, it followed that all datatypes have a least element, So, from leastfix and complete together it follows that all datatypes are cpos.

Note that we cannot hope to define or even to declare a function

$$\bigcup : (\Pi \alpha \ast_p. (\alpha \to \ast_p) \to \alpha)$$

that maps predicates to their limits, because this type cannot be formed in $\lambda \omega^p_L$. A term $(\bigcup \sigma P)$ would be an inhabitant of the datatype $\sigma$ depending on a predicate $P$. So it is a term in the programming language depending on a term in the logic. This is exactly one of the dependencies we have chosen to exclude in $\lambda \omega_L$ and its extensions.

A set $P$ is called admissible or chain-complete if any chain in $P$ has a limit in $P$. A predicate $P : \alpha \to \ast_p$ is called admissible if the set it characterises is, i.e. if for any chain $C$ for which all elements satisfy $P$ the limit also satisfies $P$. So we define

$$\text{admissible} = \lambda \alpha \ast_s. \lambda P \alpha \to \ast_p$$

$$\forall C \alpha \to \ast_p. \forall \text{lub } \alpha$$

$$(\text{chain } \alpha C) \implies (\text{LUB } \alpha C \text { lub}) \implies (\forall \tau. \alpha \tau x \Rightarrow P x) \Rightarrow (\exists \text{lub } P \text { lub})$$

$$: \Pi \alpha \ast_s. (\alpha \to \ast_p) \to \ast_p$$

The fact the notion of admissibility can be expressed and that admissibility of programs can be proved in the system means that the logic we have is stronger than LCF ([Pau87]). There the condition of the admissibility of $P$ in fixpoint induction is strengthened to a syntactic check on the shape of $P$. Even though the notion of admissibility is definable, such a syntactic check can still be useful, because proving admissibility of a predicate can be quite complicated.

All declarations and definitions in $\Gamma_{CPO}$ have now been discussed, with the exception of the (self-explanatory) definition of strict.

5.16 Definition. $\Gamma_{CPO}$ is the $\lambda \omega^p_L$-context

$$\subseteq : \Pi \alpha \ast_s. \alpha \to \alpha \to \ast_p$$

$$\text{refl} : \forall \alpha \ast_s. \forall \alpha. \forall x. x \sqsubseteq_\alpha x$$

$$\text{trans} : \forall \alpha \ast_s. \forall x, y, \tau. \forall x \sqsubseteq_\alpha y \Rightarrow y \sqsubseteq_\alpha z \Rightarrow x \sqsubseteq_\alpha z$$

$$\text{antisym} : \forall \alpha \ast_s. \forall x, y. x \sqsubseteq_\alpha y \Rightarrow y \sqsubseteq_\alpha x \Rightarrow x =_\alpha y$$

$$\text{monotonicity} : \forall \alpha, \beta \ast_s. \forall x. \forall \alpha \beta. \forall x \sqsubseteq_\alpha y \Rightarrow x \sqsubseteq_\beta f y$$

$$\text{fix} : \forall \alpha \ast_s. \forall f. \forall \alpha f \to \alpha \Rightarrow \forall \alpha f =_\alpha f (Y \alpha f)$$

$$\text{leastfix} : \forall \alpha \ast_s. \forall f. \forall \alpha f \to \alpha. \forall \alpha. f x \sqsubseteq_\alpha x \Rightarrow \forall \alpha f \sqsubseteq_\alpha x$$

$$\text{UB} : \lambda \alpha \ast_s. \lambda P \alpha \to \ast_p. \lambda x. \forall \alpha. \forall y. \forall \alpha. P y \Rightarrow \forall x. y \sqsubseteq_\alpha x$$

$$: \Pi \alpha \ast_s. (\alpha \to \ast_p) \to \alpha \to \ast_p$$
CHAPTER 5. RECURSION

\[ \text{LUB} = \lambda \alpha \cdot \lambda P \alpha \rightarrow \ast_p. \lambda x. (UB \alpha P x) \land (\forall y. UB \alpha P y \Rightarrow \tau \subseteq y) \]
\[ \text{chain} = \lambda \alpha \cdot \lambda C \cdot \alpha \rightarrow \ast_p. \]
\[ (\exists x. \alpha \cdot C x) \land (\forall x, y. \alpha \cdot C x \land C y \Rightarrow x \subseteq y \lor y \subseteq x) \]
\[ \text{complete} = \lambda \alpha \cdot \lambda C \cdot \alpha \rightarrow \ast_p. \text{chain} \cdot C \Rightarrow (\exists \text{lub} \alpha. \text{LUB} \alpha C \cdot \text{lub}) \]
\[ \text{admissible} = \lambda \alpha \cdot \lambda P \alpha \rightarrow \ast_p. \forall \alpha \cdot \alpha \rightarrow \ast_p. \text{chain} \cdot \alpha \Rightarrow (\exists \text{lub} \alpha. \text{LUB} \alpha C \cdot \text{lub}) \]
\[ \text{strict} = \lambda \sigma, \tau \cdot \ast_p. \lambda f. \sigma \rightarrow \tau. \downarrow \sigma = \tau \Downarrow \tau \]
\[ \text{continuity} = \forall \sigma, \tau, \ast_p. \forall g. \sigma \rightarrow \tau. \forall C. \sigma \rightarrow \ast_p. \forall \text{lub} : \sigma. \forall \text{lub} : \tau. \]
\[ C' = (\lambda y. \tau. \exists x. \sigma. g x = \tau \land C x) : \tau \rightarrow \ast_p \text{ in} \]
\[ \text{chain} \sigma C \Rightarrow (\text{LUB} \sigma C \cdot \text{lub}) \Rightarrow (\text{LUB} \tau C' \cdot \text{lub}') \Rightarrow \text{g lub} = \tau \cdot \text{lub}' \]

More axioms are needed than just the ones in \( \Gamma_{\text{CPO}} \). We want to use axioms similar to the ones in \( \text{AXIOM}^+ \) (definition 4.39), e.g., axioms for classical logic, axioms for extensionality of \( \rightarrow \) and \( \Pi \)-types, and axioms for structural induction on \( +, \times \), and \( \Sigma \)-types. Below a set of axioms \( \text{AXIOM}^\mu \) is defined that can be safely used in \( \lambda \omega^\mu \). That these axioms are sound is shown in chapter 8, using the cpo-model.

Compared with the axioms in \( \text{AXIOM}^+ \) there are a few differences. First of all, we want axioms relating the cpo-ordering on the different datatypes. For the \( \rightarrow \), \( \Pi \)-, and \( \times \)-datatypes we want to be able to prove

\[ f \subseteq_{\sigma \rightarrow \tau} g \iff (\forall x. \sigma. f x \subseteq_{\tau} g x) \]
\[ f \subseteq_{\Pi \alpha \cdot K \cdot \sigma} g \iff (\forall x. \Pi K \cdot f x \subseteq_{\sigma} g x) \]
\[ M \subseteq_{\Pi i_{1}, \ldots, i_{n}, x_{0}} N \iff N \in_{\sigma_{1}} M l_{1} \land \ldots \land N l_{n} \in_{\sigma_{n}} M l_{n} \]

All the implications from left to right can be proved using monotonicity. For example, if \( f \subseteq_{\Pi \alpha \cdot K \cdot \sigma} g \), then by monotonicity

\[ (\lambda x. (\Pi x \cdot K \cdot \sigma) \cdot x) \cdot f \subseteq_{\sigma} (\lambda x. (\Pi x \cdot K \cdot \sigma) \cdot x) \cdot g \],

and hence \( f \subseteq_{\sigma} g \).

For (i) and (ii), the implications from right to left are included as axioms in \( \text{AXIOM}^\mu \). They can replace the axioms for extensionality of \( \rightarrow \) and \( \Pi \)-types that were included in \( \text{AXIOM} \) and \( \text{AXIOM}^+ \), because these follow from (i) and (ii) by the antisymmetry of \( \subseteq \).

For (iii), the implication from right to left does not have to be included as an axiom, because it follows from monotonicity of the function \( \text{tuple} \cdot \sigma_{1} \rightarrow \rightarrow \sigma_{n} \rightarrow \Pi (l_{1}, \sigma_{1} \ldots l_{n}, \sigma_{n}) \)

with \( \text{tuple} \cdot N_{1} \ldots N_{n} \sim \alpha \) (\( l_{i} \mapsto N_{i}, l_{i} \mapsto N_{n} \))
No properties of the ordering \( \subseteq \) on \(+\)-types and \( \Sigma \)-types have to be included as axioms. For instance, we can already prove that

\[
N \subseteq \sigma_1 \iff \text{in}_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} N \subseteq \text{in}_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} \iff N' \ \\text{for } \, l_i \neq l_j.
\]

The implication from left to right follows from the fact that \((\lambda x. \sigma_i. \text{in}_{\Sigma(l_i \sigma_1 \ldots l_n \sigma_n)} l_i x)\) is monotonic. The implication from right to left can be proved by defining a program \( f \) of type \( \Sigma(l_1 \sigma_1 \ldots l_n \sigma_n) \to \sigma_i \) such that \( f(\text{in}_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} l_i x) \gg \gg \sigma_i x \), and using the fact that this function \( f \) is monotonic.

We can also prove, for any \( l_i \neq l_j \), that

\[
\text{in}_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} l_i N_i \subseteq \text{in}_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} l_j N_j = \text{true} = \text{false}.
\]

To do this, define functions \( f, g \) \( \Sigma(l_1 \sigma_1 \ldots l_n \sigma_n) \to \text{bool} \) such that \( f(\text{in}_{l_i} x) \gg \text{true} \), \( f(\text{in}_{l_j} x) \gg \text{false} \), and \( f(\text{in}_{l_j} x) \gg \text{true} \). Then by monotonicity of \( f \) and \( g \) and antisymmetry of \( \subseteq \) it follows that

\[
\text{in}_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} l_i N_i = \text{in}_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} l_j N_j = \text{true} = \text{false}.
\]

The axioms \( AX_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} = AX_{\Sigma_{\alpha \mathbb{K} \sigma}} \) in \( AX_{\mathbb{M}^{+}} \) for structural induction on \(+\)- and \( \Sigma \)-types have to change. A type \( \Sigma(l_1 \sigma_1 \ldots l_n \sigma_n) \) not only contains elements of the form \( \text{in}_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} l_i M_i \), but it now also contains a bottom element \( \bot \Sigma(l_1 \sigma_1 \ldots l_n \sigma_n) \). For example, for the datatype \( \Sigma(1, 2, \sigma_2) \), i.e. \( \sigma_1 + \sigma_2 \), we now get

\[
AX_{\sigma_1 + \sigma_2} : \forall P. \sigma_1 + \sigma_2 \rightarrow *P. \left( \forall i. \text{in}_{\sigma_1 + \sigma_2} P(\text{in}_{\sigma_1} \text{in}_{\sigma_2} 1 x_1) \rightarrow (\forall z. \text{in}_{\sigma_1} P(\text{in}_{\sigma_1} z z)) \rightarrow P \bot \sigma_1 + \sigma_2 \rightarrow (\forall z. \text{in}_{\sigma_1} + \sigma_2. P z) \right).
\]

Datatypes \( (\Sigma_{\alpha \mathbb{K} \sigma} \sigma) \) also contain bottom elements, so for these the axioms \( AX_{\Sigma_{\mathbb{K} \sigma}} \) are changed in the same way.

For \(+\) or \( \Sigma \)-types we also have to include axioms that state that all functions constructed using the elimination construction \( \nabla \) are strict.

Finally, for the \( \mu \)-types we have to include axioms \( AX_{\mu_{\alpha \mathbb{K} \sigma}} \) that state that fold, unfold, \( \sigma \) are isomorphisms.

5.17 DEFINITION \( AX_{\mathbb{M}^{+}} \) is the set of axioms containing

\[
\begin{align*}
\text{classic} : & \quad \forall P. *P. (\neg P) \Rightarrow P, \\
\text{p} & \quad \text{true} \neq \text{false}, \\
AX_{\sigma_1 + \sigma_2} & \quad \forall f, g : \sigma \rightarrow \tau \quad (\forall x. \sigma \rightarrow \tau \quad f \tau \gg g x) \Rightarrow f \subseteq \sigma \rightarrow g, \\
AX_{\Pi_{\alpha \mathbb{K} \sigma}} & \quad \forall f, g \quad (\forall \alpha. \mathbb{K} \alpha \sigma \rightarrow \text{in}_{\mathbb{K} \sigma} g) \Rightarrow f \subseteq (\alpha \mathbb{K} \sigma \rightarrow \text{in}_{\mathbb{K} \sigma} g), \\
AX_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} & \quad \forall P. \Sigma(l_1 \sigma_1 \ldots l_n \sigma_n) \rightarrow *P. \\
& \quad (\forall x. \Sigma(l_1 \sigma_1 \ldots l_n \sigma_n) P(l_1 \rightarrow x_1, \ldots l_n \rightarrow x_n) \rightarrow (\forall x. \Sigma(l_1 \sigma_1 \ldots l_n \sigma_n) P z), \\
AX_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} & \quad \forall P. \Sigma(l_1 \sigma_1 \ldots l_n \sigma_n) \rightarrow *P. \\
& \quad (\forall x. \Sigma(l_1 \sigma_1 \ldots l_n \sigma_n) P(\text{in}_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} l_1 x)) \rightarrow P.
\end{align*}
\]
\[ (\forall x_n. P(\text{in}_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)}, l_n x_n)) \]

\[ \Rightarrow P \perp_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} \]

\[ \Rightarrow (\forall z : \Sigma(l_1 \sigma_1 \ldots l_n \sigma_n). P z) \]

**AX\Sigma K \sigma** :

\[ \forall P. (\Sigma \alpha. K. \sigma) \rightarrow \ast P. \]

\[ (\forall \alpha. K. \forall x. P(\text{in}_{\Sigma \alpha. K. \sigma} \alpha x)) \]

\[ \Rightarrow P \perp_{\Sigma \alpha. K. \sigma} \]

\[ \Rightarrow (\forall z : (\Sigma \alpha. K. \sigma). P z) \]

**AX\mu \alpha \ast \sigma** :

\[ (\forall z. (\mu \alpha \ast \sigma \sigma)) : \text{fold}_{\mu \alpha \ast \sigma} \sigma (\text{unfold}_{\mu \alpha \ast \sigma} \sigma z) = \mu \alpha \ast \sigma \sigma z \]

\[ \wedge (\forall z. \sigma[\alpha := (\mu \alpha \ast \sigma \sigma)] : \text{unfold}_{\mu \alpha \ast \sigma} \sigma (\text{fold}_{\mu \alpha \ast \sigma} \sigma z) = \sigma[\alpha := (\mu \alpha \ast \sigma \sigma)] z) \]

**STRICT\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)** :

\[ \forall \rho \ast : \forall f : (l_1 \sigma_1 \rightarrow \rho, \ldots, l_n \sigma_n \rightarrow \rho). \bigwedge f \perp_{\Sigma(l_1 \sigma_1 \ldots l_n \sigma_n)} \Rightarrow \rho \perp \rho \]

**STRICT\Sigma K \sigma** :

\[ \forall \rho \ast : \forall f : (\Pi \alpha. K. \sigma \rightarrow \rho). \bigwedge f \perp_{\Sigma \alpha. K. \sigma} = \rho \perp \rho \]

for all \( \sigma \rightarrow \tau, (\Pi \alpha. K. \sigma) : \Pi(l_1 \sigma_1 \ldots l_n \sigma_n), \Sigma(l_1 \sigma_1 \ldots l_n \sigma_n) = (\Sigma \alpha. K. \sigma), (\mu \alpha \ast \sigma) \in \text{Cons} \).

Of course, we want to know if the axioms in \( \Gamma_{\text{CPO}} \) and \( AXIOM^\mu \) are consistent. This can be proved using the model given in chapter 8

5.18 Lemma (Consistency of \( \Gamma_{\text{CPO}} \) and \( AXIOM^\mu \) in \( \lambda \omega_L \)).

False is not provable in the context \( \Gamma_{\text{CPO}} \) extended with axioms from \( AXIOM^\mu \).

**Proof** See lemma 8.33. \( \square \)
5.3 Program and Proof Development

As in the previous programming logics, in $\lambda \omega^k$ we can prove propositions that can be used to deduce a property of a program from certain properties of its subprograms, and we can prove propositions that state equalities between programs, which can be used as transformation rules.

First we consider the problem of proving properties of recursive programs, i.e. programs constructed with the fixpoint combinator $Y$. The following lemma is crucial for this:

5.19 **Lemma (Fixpoint Induction).**

In the context $\Gamma_{CPO}$ the following proposition is provable:

$$\forall \alpha. * \alpha, \forall f : \alpha \to \alpha, \forall P : \alpha \to * P \Rightarrow \alpha \Rightarrow (\forall x. P x \Rightarrow P (f x)) \Rightarrow P (Y \alpha f)$$

**Proof.** Let $\Gamma \vdash \alpha : * \alpha, \Gamma \vdash P : \alpha \to * P$ and $\Gamma \vdash f : \alpha \to \alpha$, and suppose that $\Gamma \vdash \alpha : (\text{admissible } \alpha P), \Gamma \vdash P \perp \alpha$ and $\Gamma \vdash : (\forall x. \alpha. P x \Rightarrow P (f x))$. To prove: $P (Y \alpha f)$.

The plan of the proof is as follows: If $P \perp \alpha$ and $(\forall x. \alpha. P x \Rightarrow P (f x))$, then all elements in the chain

$$\perp \alpha \subseteq \perp \alpha \subseteq f \perp \alpha \subseteq f^2 \perp \alpha \subseteq \ldots$$

satisfy $P$. Since $P$ is admissible it then follows that the least upper bound of this chain also satisfies $P$. So to prove $P (Y \alpha f)$, we have to show that $\{ \perp \alpha, f \perp \alpha, f^2 \perp \alpha, \ldots \}$ is indeed a chain and that $(Y \alpha f)$ is its least upper bound.

The predicate on $\alpha$ that characterises the chain $\{ \perp \alpha, f \perp \alpha, f^2 \perp \alpha, \ldots \}$ is defined as follows:

$$C = \lambda x. \alpha. (\forall Q : \alpha. Q \perp \alpha \Rightarrow (\forall y. \alpha. Q y \Rightarrow Q (f y)) \Rightarrow Q x)$$

$$: \alpha \to * P$$

It is easy to verify that $C : \alpha \to * P$ is true in $\perp \alpha$ and closed under $f$, and for any predicate $Q : \alpha \to * P$ that is also true in $\perp \alpha$ and closed under $f$ we have $(\forall x. \alpha. C x \Rightarrow Q x)$. So $C : \alpha \to * P$ is the smallest predicate that is true in $\perp \alpha$ and closed under $f$.

We have to prove that $C$ is a chain and that $(Y \alpha f)$ is the least upper bound of $C$. Proving of (chain $\alpha C$) is not difficult: define

$$Q = \lambda x. \alpha. (\forall z. \alpha. C z \Rightarrow (z \subseteq \alpha x \lor x \subseteq z))$$

$$: \alpha \to * P$$

and prove that this predicate is true in $\perp \alpha$ and closed under $f$. A fairly detailed proof of $(\text{LUB } \alpha C (Y \alpha f))$ is given in figure 5.1 on page 100. It is essentially a conventional proof of the fact that the least fixpoint of a continuous function $f$ is the least upper bound of the chain $\perp \alpha \subseteq f \perp \alpha \subseteq f^2 \perp \alpha \subseteq \ldots$. The type parameter of $\subseteq$ is omitted in figure 5.1.

This lemma gives the following proof rule to accompany the type inference rule for $Y$:

5.20 **Corollary (Coupled derivation rule for $Y$).** In the context $\Gamma_{CPO}$ the following rules are derivable:

$$\frac{\Gamma \vdash \alpha : * \alpha, \Gamma \vdash P : \alpha \to * P, \Gamma \vdash \alpha : (\text{admissible } \alpha P)}{\Gamma \vdash Y \alpha f : \alpha}$$

$$\frac{\Gamma \vdash Y \alpha f : \alpha, \Gamma \vdash P \perp \alpha, \Gamma \vdash : (\forall x. \alpha. P x \Rightarrow P (f x))}{\Gamma \vdash P (Y \alpha f)}$$

□
1. \( \text{chain } \sigma C \) easy
2. \( \exists \text{lub}: (\text{LUB } \sigma C \text{ lub}) \) 1, complete
3. \( \text{lub } : \sigma, (\text{LUB } \sigma C \text{ lub}) \)
4. \( C' = (\lambda y. (\exists x. C x \land f x = y)) : \sigma \rightarrow \ast_p \)
5. \( \text{chain } \sigma C' \) easy
6. \( \exists \text{lub}' : (\text{LUB } \sigma C' \text{ lub'}) \) 5, complete
7. \( \text{lub}' = \sigma f \text{ lub} \)
8. \( \text{LUB } \sigma C' (f \text{ lub}) \) 3,7, continuity, def \( C' \)
9. \( \forall x : \sigma. C' x \Rightarrow C x \) def \( C, C' \)
10. \( \text{UB } \sigma C' \text{ lub} \) 6,9, (\( \forall \text{intro} \)), (\( \exists \text{elim} \))
11. \( f \text{ lub } \subseteq \text{lub} \) 10,12, def LUB
12. \( \text{Y } \sigma f \subseteq \text{lub} \) 13, leastfix
13. \( \exists x : \sigma, x \subseteq \text{Y } \sigma f \) easy
14. \( f x \subseteq f (\text{Y } \sigma f) \) 16, monotonicity
15. \( f x \subseteq \text{Y } \sigma f \) 17, fix
16. \( \forall x : \sigma. \tau \subseteq \text{Y } \sigma f \Rightarrow f \tau \subseteq \text{Y } \sigma f \) 18, (\( \forall \text{intro} \)), (\( \Rightarrow \text{intro} \))
17. \( \forall x : \sigma. C x \Rightarrow f \tau \subseteq \text{Y } \sigma f \) 15,19, def \( C \)
18. \( \text{UB } \sigma C (\text{Y } \sigma f) \) 20, def UB
19. \( \text{lub } \subseteq \text{Y } \sigma f \) 21, 3, def LUB
20. \( \text{lub } = \sigma \text{Y } \sigma f \) 14,22, antisymp
21. \( \text{LUB } \sigma C (\text{Y } \sigma f) \) 3,23
22. \( \text{LUB } \sigma C (\text{Y } \sigma f) \) 2,24, (\( \forall \text{intro} \)), (\( \exists \text{elim} \))

Figure 5.1: proof of lemma 5.19
Lemma 5.19 and its corollary are of course useless if we cannot prove admissibility of predicates. Large classes of predicates can be shown to be admissible, see for instance [ZNV72] [Fau87]. To prove that a predicate is admissible, it is useful to prove admissibility for all predicates of a certain form, as in lemma 5.21 below, and to prove that a certain construction preserve admissibility, as in lemma 5.22 below. These two lemmas indicate a well-known class of admissible predicates.

5.21 Lemma. In context $\Gamma_{CP0}$ the following proposition is provable.

$$\forall \alpha, \beta \cdot \forall g, h \cdot \alpha \rightarrow \beta. \text{ admissible } \alpha (\lambda x: \alpha. g x \sqsubseteq \beta h x).$$

Proof. Suppose $\alpha, \beta : \ast$, and $g, h : \alpha \rightarrow \beta$. Define $P = (\lambda x: \alpha. g x \sqsubseteq \beta h x) : \alpha \rightarrow \ast_p$.

To prove admissible $\alpha P$ we have to prove

$$\forall C : \alpha \rightarrow \ast_p, \text{lub } \alpha. \quad (\text{chain } \alpha C) \Rightarrow (\text{LUB } \alpha C \text{lub}) \Rightarrow (\forall x : \alpha. C x \Rightarrow P x) \Rightarrow (P \text{lub}).$$

Suppose $C : \alpha \rightarrow \ast_p, \text{lub } \alpha, (\text{chain } \alpha C), (\text{LUB } \alpha C \text{lub})$, and $(\forall x : \alpha. C x \Rightarrow P x)$. So $C$ is a chain with least upper bound lub and all elements in $C$ satisfy $P$.

To prove: $(P \text{lub})$, i.e. $g \text{lub} \sqsubseteq h \text{lub}$.

Define predicates $C_g$ and $C_h$ as follows:

$$C_g = (\lambda y : \tau. \exists x : \sigma. P x \land y =_\tau g x) \quad \tau \rightarrow \ast_p$$

$$C_h = (\lambda y : \tau. \exists x : \sigma. P x \land y =_\tau h x) \quad \tau \rightarrow \ast_p$$

By continuity $(g \text{lub})$ is the limit of $C_g$, and $(h \text{lub})$ is the limit of $C_h$, i.e. $(\text{LUB } \tau C_g (g \text{lub}))$ and $(\text{LUB } \tau C_h (h \text{lub}))$. It follows from $(\forall x : \alpha. C x \Rightarrow P x)$ - which is $\delta$-convertible with $(\forall x : \alpha. C x \Rightarrow g x \sqsubseteq \beta h x)$ - than for every element of $C_g$ there is a larger element of $C_h$, i.e.

$$\forall y : \tau. C_g y \Rightarrow (\exists z : \tau. C_h z \land y \sqsubseteq z).$$

Then $(h \text{lub})$ - the least upper bound of $C_h$ - is also an upper bound of $C_g$. But $(g \text{lub})$ is the least upper bound of $C_g$ and so $g \text{lub} \sqsubseteq h \text{lub}$.

It is well-known that conjunction "preserves" admissibility.

5.22 Lemma. In context $\Gamma_{CP0}$ the following proposition is provable.

$$\forall \alpha : \ast, \forall P, Q : \alpha \rightarrow \ast, \quad \text{admissible } \alpha P \Rightarrow \text{admissible } \alpha Q \Rightarrow \text{admissible } \alpha (\lambda x : \alpha. P x \land Q x).$$

Proof. Easy.

Using the last two lemmas admissibility for a large class of predicates can be proved. For example, by the antisymmetry of $\sqsubseteq$ it immediately follows from these lemmas that all predicates of the form $(\lambda x : \sigma. g x \Rightarrow h x) : \sigma \rightarrow \ast_p$ are admissible.

Fixpoint induction can not only be used to prove properties of individual recursive programs, but can also be used to prove many transformation rules for recursive programs. An example is given in the next lemma.
1 \sigma : \ast_0

2 f, g : \sigma \rightarrow \sigma

3 f \perp = g \perp, f \circ g = g \circ f

4 \text{admissible } (\lambda x: \sigma \ x \in Y \ g)

5 \perp \in Y \ g

6 x : \sigma, \ x \in Y \ g

7 f x \in f (Y \ g)

8 \text{admissible } (\lambda y : \sigma \ f y \in Y \ g)

9 g \perp \in Y \ g

10 f \perp \in Y \ g

11 \text{y : } \sigma, \ f y \in Y \ g

12 g (f y) \in g (Y \ g)

13 f (g y) \in g (Y \ g)

14 f (g y) \in Y \ g

15 \forall y : \sigma, \ f y \in Y \ g \Rightarrow f (g y) \in Y \ g

16 f (Y \ g) \in Y \ g

17 f \ r \in Y \ g

18 \forall x : \sigma \ r \in Y \ g \Rightarrow f \ r \in Y \ g

19 Y f \in Y \ g

20 \forall f, g : \sigma \rightarrow \sigma \ f \perp = g \perp \Rightarrow f \circ g = g \circ f \Rightarrow Y \ f \in Y \ g

21 f, g : \sigma \rightarrow \sigma, \ f \perp = g \perp, \ f \circ g = g \circ f

22 Y f = Y \ g

23 \forall f, g : \sigma \rightarrow \sigma \ f \perp = g \perp \Rightarrow f \circ g = g \circ f \Rightarrow Y \ f = Y \ g

\text{lemma 5.21}

\text{easy}

6, \text{ monotonicity}

\text{lemma 5.21}

(5, \text{ monotonicity, fix})

3, 9

11, \text{ monotonicity}

3, 12

13, \text{ fix}

14, \text{ (vintro)}

8, 9, 15

7, 16, \text{ trans}

17, \text{ (vintro)}

4, 5, 18, \text{ lemma 5.19}

20, 21 \text{ antisym}

22, \text{ (vintro)}, (\Rightarrow \text{ intro})

\text{Figure 5.2 proof of lemma 5.23}
5.3 PROGRAM AND PROOF DEVELOPMENT

5.23 LEMMA. In the context \( \Gamma_{CPD} \) the following proposition is provable:

\[
\forall \sigma. \forall f, g. \sigma \rightarrow f. \Downarrow \sigma = \sigma g. \Downarrow \sigma \Rightarrow f o g = \sigma \rightarrow g o f \Rightarrow \forall \sigma. f = \sigma \forall \sigma. g
\]

PROOF. This proof, given in figure 5.2 on page 102, is still small enough to be given in full in natural deduction format. The type parameters of \( \bot, \forall, =, \subseteq \) and admissible – which are nearly always \( \sigma \) – are omitted in this proof. \( \square \)

In lemma 4.48 we gave an example of a transformation rule in \( \lambda \omega \), namely for the distribution of composition over \( \nabla \). Because \(+\)-types now include bottom elements, in \( \lambda \omega \) this rule requires an extra condition:

5.24 LEMMA. In the context \( \Gamma_{CPD} \) the following proposition is provable using axioms from \( AXIOM^\mu \):

\[
\forall \rho_1, \rho_2, \tau, \sigma. \forall f : \rho_1 \rightarrow \sigma, g : \rho_2 \rightarrow \sigma, h : \sigma \rightarrow \tau
\]

\[
(\text{strict } \sigma \tau h) \Rightarrow h o (f \nabla g) = \rho_1 + \rho_2 \rightarrow (h o f) \nabla (h o g)
\]

PROOF

1. \[
\begin{array}{c}
\rho_1, \rho_2, \tau, \sigma: \star, f : \rho_1 \rightarrow \sigma, g : \rho_2 \rightarrow \sigma, h : \sigma \rightarrow \tau \\
\text{strict } \sigma \tau h
\end{array}
\]

2. \[
\begin{array}{c}
\rho_1
\end{array}
\]

3. \[
\begin{array}{c}
\tau : \rho_1
\end{array}
\]

4. \[
\begin{array}{c}
h o (f \nabla g)(\in \rho_1 + \rho_2, 1 \pi) = \tau (h o f) \nabla (h o g)(\in \rho_1 + \rho_2, 1 \pi)
\end{array}
\]

both sides

5. \[
\begin{array}{c}
\forall x : \rho_1 (h o (f \nabla g))(\in \rho_1 + \rho_2, 1 \tau) = \tau ((h o f) \nabla (h o g))(\in \rho_1 + \rho_2, 1 \tau)
\end{array}
\]

6. \[
\begin{array}{c}
\forall y : \rho_2 (h o (f \nabla g))(\in \rho_1 + \rho_2, 2 \tau) = \tau ((h o f) \nabla (h o g))(\in \rho_1 + \rho_2, 2 \tau)
\end{array}
\]

both sides

7. \[
\begin{array}{c}
((h o f) \nabla (h o g)) \Downarrow \rho_1 + \rho_2 = \tau \Downarrow \tau
\end{array}
\]

8. \[
\begin{array}{c}
(f \nabla g) \Downarrow \rho_1 + \rho_2 = \sigma \Downarrow \sigma
\end{array}
\]

9. \[
\begin{array}{c}
(h o (f \nabla g)) \Downarrow \rho_1 + \rho_2 = \tau \Downarrow \tau
\end{array}
\]

10. \[
\begin{array}{c}
((h o f) \nabla (h o g)) \Downarrow \rho_1 + \rho_2 = \tau \Downarrow \tau
\end{array}
\]

11. \[
\begin{array}{c}
\forall z : \rho_1 + \rho_2, \sigma. (h o (f \nabla g)) z = \tau ((h o f) \nabla (h o g)) z
\end{array}
\]

12. \[
\begin{array}{c}
h o (f \nabla g) = \rho_1 + \rho_2 \rightarrow (h o f) \nabla (h o g)
\end{array}
\]

both sides

\( \Rightarrow \rho_5 h (f x) \)

4.

similarly

STRICT \( \rho_1 + \rho_2 \)

STRICT \( \rho_1 + \rho_2 \)

2.8

7.9

4, 5, 10, AXIOM \( \rho_1 + \rho_2 \)

11, AXIOM \( \rho_1 + \rho_2 \)

\( \square \)

In lemma 4.49 we gave two distribution rules for composition over (if then else) in \( \lambda \omega \).

In \( \lambda \omega \) the second of these requires an extra condition.

5.25 LEMMA. In the context \( \Gamma_{CPD} \) the following proposition is provable using axioms from \( AXIOM^\mu \):

1. \( \forall b : \text{bool}, \forall \sigma. \forall g : \sigma \rightarrow \tau. \forall h : \sigma \rightarrow \sigma. \)

   \( (\text{if } b \text{ then } f \text{ else } g) h = \rho \rightarrow \tau \text{ if } b \text{ then } f h \text{ else } g h \)
2. \( \forall \forall b : \text{bool}. \forall \rho, \sigma, \tau. \forall h : \tau. \forall f, g : \rho \rightarrow \sigma. \)

\[
\text{strict } \sigma \rightarrow \tau \Rightarrow h_0(\text{if } b \text{ then } f \text{ else } g) =_{\rho \rightarrow \tau} \text{ if } b \text{ then } h_0 f \text{ else } h_0 g \]

By the definition of bool and (if then else), the second part of this lemma is an instantiation of the previous lemma.

It is awkward to have to use the cpo-ordering \( \sqsubseteq \) every time we want to prove termination of a recursive program. Some standard recursion patterns will be used often in recursive programs, such as primitive recursion, or recursion on the natural numbers or lists with all recursive calls on smaller natural numbers or shorter lists. For these common recursion patterns we would like to prove termination once and for all. Also, we would want to derive induction rules tailored to those recursion patterns, which can be used from then on to prove properties of programs that use one of these recursion patterns.
Part II

Semantics
Chapter 6

The Basic System

This chapter treats the semantics of the basic system \( \lambda \omega_L \) introduced in chapter 3. The semantics gives a sound interpretation of the system. It provides a denotational semantics for the programming language and a truth-table semantics for the logic, which shows that the logic is free from inconsistencies. The model provides the justification (and possibly also the inspiration) for extensions of the basic system. This can be extensions of the programming language, e.g., new datatypes, datatype-constructors and associated primitive operations, as will be considered in subsequent chapters. It can also be extensions of the logic, typically axioms expressing properties of programs or datatypes. Some examples of such axioms have already been given in chapter 3.

The structure of this chapter closely follows that of chapter 3. We begin by considering the two subsystems of \( \lambda \omega_L : \lambda \omega_s \) and \( \lambda \omega_p \). Although syntactically these two systems are identical - they are copies of \( \lambda \omega \) - we want different interpretations for them. This is because in \( \lambda \omega_s \) our main interest concerns the interpretation of the terms (programs), whereas in \( \lambda \omega_p \), our main interest concerns the interpretation of the types (propositions). Also, the models will have to accommodate extensions of the systems, and \( \lambda \omega_s \) and \( \lambda \omega_p \) will be extended in different directions.

Still, the global structure of the models for \( \lambda \omega_s \) and \( \lambda \omega_p \) is the same. In section 6.1 we describe the general structure of a model for \( \lambda \omega \), the higher order lambda calculus. This is a straightforward extension of the environment models defined in [BMM90] for the second order lambda calculus.

In section 6.2 we give a model for \( \lambda \omega_s \) by showing that the PER-model, which is the best known model for the second and higher order lambda calculus, is indeed an instantiation of this general model definition.

In section 6.3 it is shown how the general model definition can be instantiated to produce a model for \( \lambda \omega_p \). The model for \( \lambda \omega_p \) is much simpler than the one for \( \lambda \omega_s \). It uses the classical interpretation of propositions as truth values. It identifies all proof terms, which is why it is called a proof-irrelevance model. This simple model suffices to prove consistency of the logic.

In section 6.4 we consider the semantics of the whole of \( \lambda \omega_L \). It is shown how the proof-irrelevance for \( \lambda \omega_p \) can be combined with any model for \( \lambda \omega_s \) to produce a model for \( \lambda \omega_L \). In \( \lambda \omega_L \) there are more predicates, propositions, and proofs than in \( \lambda \omega_p \), but the truth-value interpretation of \( \lambda \omega_p \) can easily be extended to include the additional constructs of \( \lambda \omega_L \). This model proves consistency of the logic, and consistency of the axioms in \( AXIOM \).
In defining the semantics of $\lambda \omega$ and its subsystems, the distinction between the different levels plays an important role. In the definition of a PTS there is just one collection of (pseudo)terms. But for the particular PTSs we consider a more refined context-free syntax has been introduced in definitions 3.4 and 3.10, where the different sets of pseudoterms Kind, Cons, Prog, Pkind, Pcons and Proof are defined. The interpretation of terms in the different models will be based on this context-free syntax.

As far as the semantics is concerned, only PTSs, and not DPTSs, have to be considered. By theorem 2.3.6 any model for a PTS also models the associated DPTS. As the interpretation of a DPTS-term $A$ in context $\Gamma$ we can take the interpretation of its $\delta$-normal form, the DPTS-term $\delta n f \Gamma (A)$. This means the interpretation of DPTS-terms is given in two steps: first take the $\delta$-normal form, and then take the interpretation of the resulting PTS-term. Defining the interpretation of DPTS-terms directly would only obscure the model definitions without any added value, because it would simply amount to composing the function $\delta n f \Gamma (\_)$ and the interpretation function for PTS-terms.

### 6.1 General Model Definition for $\lambda \omega$

In this section we give the general definition of the notion of environment model for the system $\lambda \omega$. This describes the overall structure of an environment model for $\lambda \omega$, and - because $\lambda \omega$, and $\lambda \omega_p$ are copies of $\lambda \omega$ - also of environment models for $\lambda \omega$, and $\lambda \omega_p$.

In [BMM90] the notion of environment model for the second order lambda calculus is defined. It is based on the notion of environment model for the untyped lambda calculus, as given in [Mey82]. The general model definition for $\lambda \omega$ - the higher order lambda calculus - is a simple extension of the one for the second order lambda calculus.

The aim of such a general model definition is to separate the general characteristics of a $\lambda \omega$-model from those that are particular to specific models. Some properties can be proven with respect to this general model definition, which saves us from having to prove them for each $\lambda \omega$-model individually. In particular, soundness of type assignment, i.e.

$$\Gamma \vdash a : A \Rightarrow [a] \in [A],$$

and soundness of conversion, i.e.

$$a \equiv \beta b \Rightarrow [a] = [b],$$

will be proven for the general model definition.

Because the general model definition specifies exactly what constitutes a model for $\lambda \omega$, it can also help the design of a specific model. This will be the case in chapter 8, where a model is constructed by solving the domain equations that are part of the general model definition.

The general model definition is explained using the copy $\lambda \omega$, of $\lambda \omega$. Recall that in $\lambda \omega$, three levels were distinguished: kinds, datatype-constructors and programs. The two top layers of $\lambda \omega$, the datatype-constructors and their kinds, do not depend on the bottom layer, the programs. This means the interpretation of the kinds and datatype-constructors can be considered separately, before we turn to the interpretation of the programs.
6.1. GENERAL MODEL DEFINITION FOR $\lambda\omega$

The semantics of the kinds and datatype-constructors

The datatype-constructors with their kinds form a simply typed lambda calculus with a single type constant $*$, and term constants $\to,*,*\to*$ and $\Pi: (K \to *) \to *$ for all kinds $K$. So a model for the datatype-constructors and their kinds is a model for the simply typed lambda calculus. Before we give a formal definition of what constitutes a model for the kinds and datatype-constructors, we discuss the different ingredients.

The kinds are generated by

$$K := * \mid K \to K,$$

so all kinds are closed expressions. For the interpretation of kinds we simply have a set $\text{Kind}_K$ for every kind $K$.

The datatype-constructors of type $K$ are interpreted as elements of the set $\text{Kind}_K$. So if $\Gamma \vdash \sigma : K$, then

$$[\Gamma \vdash \sigma : K] \eta \in \text{Kind}_K;$$

$[\Gamma \vdash \sigma : K] \eta$ is the meaning of the datatype-constructor $\sigma$ in the environment $\eta$. This environment $\eta$ is a function which gives the meaning of the free variables of $\sigma$.

By lemma 3.5 the datatype-constructors are of the form

$$\sigma := \alpha \mid (\lambda \alpha : K. \sigma) \mid \sigma \sigma \mid \sigma \to \sigma \mid (\Pi \alpha : K. \sigma)$$

where $\alpha \in \text{Var}^D$ and $K$ ranges over kinds. To define the meaning of abstractions and applications in datatype-constructors (i.e. $(\lambda \alpha : K. \sigma)$ and $\sigma_1 \sigma_2$), the sets $\text{Kind}_K$ have to solve the domain equations

$$\text{Kind}_{K_1 \to K_2} \cong [\text{Kind}_{K_1} \to \text{Kind}_{K_2}]$$

where the square brackets denote some subset of the function space. The associated isomorphisms are the element-to-function mappings, well-known from models of the type-free lambda calculus.

In fact, $\text{Kind}_{K_1 \to K_2}$ and $\text{Kind}_{K_1} \to \text{Kind}_{K_2}$ can be taken equal and not just isomorphic. We maintain the isomorphisms here to emphasize the similarity with the definition of the semantics of programs that will be given later.

Solving the domain equations above takes care of the interpretation of abstraction and application in datatype-constructors. This leaves only the datatypes of the form $\sigma \to \tau$ and $(\Pi \alpha : K. \sigma)$ to be dealt with.

The meaning of $\sigma \to \tau$ (in $\text{Kind}_*$) is defined in terms of the meanings of $\sigma$ and $\tau$ (both in $\text{Kind}_*$). For this a function $\leftarrow$ is needed, with

$$\leftarrow \in \text{Kind}_* \to \text{Kind}_* \to \text{Kind}_*.$$

The meaning of $(\Pi \alpha : K. \sigma)$ (in $\text{Kind}_*$) is defined in terms of the function that maps all possible interpretations of $\alpha$ (in $\text{Kind}_*$) to the resulting meanings of $\sigma$ (in $\text{Kind}_*$). So $[\Gamma \vdash (\Pi \alpha : K. \sigma) \to *] \eta$ is defined in terms of the function which maps $\alpha \in \text{Kind}_K$ to $[\Gamma, \alpha : K \vdash \sigma : *] \eta[\alpha := a] \in \text{Kind}_*$. For this a function $\prod$ is needed, with

$$\prod \in \prod_{\alpha \in K} (\text{Kind}_K \to \text{Kind}_*) \to \text{Kind}_*.$$

So $\leftarrow$ provides the interpretation of $\to$, and $\prod$ provides the interpretation of $\Pi$. We have now introduced everything that is needed for a model for the $\lambda\omega$-datatype-constructors.
6.1 DEFINITION. An environment frame for the datatype-constructors of $\lambda\omega$, is a 4-tuple $(\text{Kind}, \Phi_{\text{Kind}}, \rightarrow, \Pi)$, where

- $\text{Kind} = \{ \text{Kind}_K | K$ is a kind \}$ is a family of sets, indexed by kinds.
- $\Phi_{\text{Kind}} = \{ \Phi_{K_1, K_2} | K_1 \rightarrow K_2$ is a kind \}$ is a family of bijections with
  $$
  \Phi_{K_1, K_2} \in \text{Kind}_{K_1 \rightarrow K_2} \rightarrow [\text{Kind}_{K_1} \rightarrow \text{Kind}_{K_2}]
  $$
  where the square brackets denote some subset of the function space.
- $\rightarrow \in \text{Kind}_{*} \rightarrow \text{Kind}_{*} \rightarrow \text{Kind}_{*}$.
- $\Pi \in \prod_{K \in \text{Kind}} (\text{Kind}_K \rightarrow \text{Kind}_{*}) \rightarrow \text{Kind}_{*}$.

The meaning of a datatype-constructor $\sigma$ depends on an environment giving the meaning of its free variables. The meanings assigned to the free variables of $\sigma$ by this environment have to match the kinds assigned to them in the context. The free variables of a datatype-constructor are all datatype-constructor variables, i.e., if $\Gamma \vdash \sigma : K$, then the free variables of $\sigma$ are declared in $\Gamma^{\|\sigma}$.

6.2 DEFINITION. Let $\Gamma$ be a $\lambda\omega$-context. An environment $\eta$ satisfies $\Gamma^{\|\sigma}$, written $\eta \models \Gamma^{\|\sigma}$, if $\eta(\alpha) \in \text{Kind}_K$ for all $\alpha : K$ in $\Gamma^{\|\sigma}$.

The meaning of datatype-constructor $\sigma$ is defined by induction on its type derivation rather than by induction on its structure. This is done because the definition involves (type) information which cannot be found in the datatype-constructors, but which can be found in their type derivations. For example, the meaning of $\sigma \tau$ depends on $\Phi_{K_1, K_2}$, where $K_1 \rightarrow K_2$ is the type of $\sigma$. The meaning of programs will later also be defined by induction on type derivations.

A type derivation for a term follows the structure of that term fairly closely, so there is not much difference between the two forms of induction. However, there is a difference. It is caused by the inference rules (weaken) and ($\beta\text{conv}$), which can be applied at many points in a derivation.

By Lemma 2.15 we can restrict the places where the rule (weaken) is used, namely only to derive $\Gamma \vdash \sigma : K'$ where $\sigma$ is a variable. In these cases the interpretation of $\sigma$ is immediately given by the environment.

This leaves ($\beta\text{conv}$) as the only inference rule whose use is not directed by the syntax. So the only way to produce different type derivations for the same term is by different applications of the rule ($\beta\text{conv}$). Whenever we define the meaning of terms by induction on their type derivation, the first thing to do is of course prove that different type derivation do not result in different meanings of the same term.

6.3 DEFINITION (Semantics of $\lambda\omega$-datatype-constructor). For datatype-constructors $\sigma$ we define $\| \Gamma \vdash \sigma : K \| \eta$ for all $\Gamma \vdash \sigma : K$ and $\eta \models \Gamma^{\|\sigma}$, by
induction on the derivation of \( \Gamma \vdash \sigma : K \), as follows

\[
\begin{align*}
\Gamma, \alpha \vdash K, \Gamma' \vdash \alpha : K & \quad \mathsf{\eta} \equiv \eta(\alpha) \\
\Gamma \vdash \sigma : K & \quad \mathsf{\eta} \equiv \begin{cases} 
\Gamma \vdash \sigma : K' & \text{if } \Gamma \vdash \sigma : K \text{ follows from } \Gamma \vdash \sigma : K' \text{ by } (\beta\text{conv}). 
\end{cases} \\
\Gamma \vdash \sigma : K_2 & \quad \mathsf{\eta} \equiv (\forall K_1. K_2 \to K_2 \eta) [\Gamma \vdash \sigma : K_1] \eta \\
\Gamma \vdash (\lambda \alpha : K_1 \cdot \sigma) : K_1 \to K_2 & \quad \mathsf{\eta} \equiv \Phi^{-1}_{K_1, K_2} (\forall a \in \text{Kind}_{K_1}. [\Gamma, \alpha : K_1 \vdash \sigma : K_2] \eta[\alpha := a]) \\
\Gamma \vdash \sigma : \ast_\eta & \quad \mathsf{\eta} \equiv [\Gamma \vdash \sigma : \ast_\eta] \eta [\Gamma \vdash \tau : \ast_\eta] \eta \\
\Gamma \vdash (\Pi \alpha : K \cdot \sigma) : \ast_\eta & \quad \mathsf{\eta} \equiv \Pi K (\forall a \in \text{Kind}_{K}. [\Gamma, \alpha : K \vdash \sigma : \ast_\eta] \eta[\alpha := a])
\end{align*}
\]

The rule \((\beta\text{conv})\) is not really needed in type derivations for datatype-constructors. The type of a datatype-constructor is a kind and because all kinds are in normal form, this type is unique, not just unique up to \(\delta\)-conversion. This means that \(K \equiv K'\) in all applications of \((\beta\text{conv})\). An immediate consequence is that \([\Gamma \vdash \sigma : K] \eta\) does not depend on which particular type derivation we consider.

\(\square\)

The subscript \(K\) of \(\Pi K\) will usually be omitted.

By lemma 3.5 the clauses in the definition above cover all possible type derivations for datatype-constructors. Still, \([\Gamma \vdash \sigma : K] \eta\) is not well-defined for all \(\Gamma \vdash \sigma : K\) and \(\eta \models \Gamma^\sigma\), for every environment frame. The problem is that

\[
\lambda a \in \text{Kind}_{K_1}. [\Gamma, \alpha : K_1 \vdash \sigma : K_2] \eta[\alpha := a]
\]

is possibly not in the subset \([\text{Kind}_{K_1} \rightarrow \text{Kind}_{K_2}]\) of \(\text{Kind}_{K_1} \rightarrow \text{Kind}_{K_2}\), i.e. the range of the \(\Phi_{K_1, K_2}\).

6.4 DEFINITION. An environment model for the datatype-constructors of \(\lambda \omega\) is an environment frame for the datatype-constructors for which \([\Gamma \vdash \sigma : K] \eta\) is defined for all \(\Gamma \vdash \sigma : K\) and \(\eta \models \Gamma^\sigma\).

\(\square\)

In the actual models that we consider this will never be a problem, as the range \(\text{Kind}_{K_1} \rightarrow \text{Kind}_{K_2}\) of \(\Phi_{K_1, K_2}\) will always be the whole function space \(\text{Kind}_{K_1} \rightarrow \text{Kind}_{K_2}\).

For any environment model for the datatype-constructors we have the following properties:

6.5 THEOREM (Soundness of type assignment for datatype-constructors).
If \(\Gamma \vdash \sigma : K\) then \([\Gamma \vdash \sigma : K] \eta \notin \text{Kind}_{K}\) for all \(\eta \models \Gamma^\sigma\).

\(\square\)

6.6 LEMMA (Soundness of \(\beta\)-reduction for datatype-constructors).
Suppose \(\sigma \Downarrow \sigma'\), \(\Gamma \vdash \sigma' : K\) \(\square\), and \(\Gamma \vdash \sigma : K : \square\).

Then \([\Gamma \vdash \sigma : K] \eta = [\Gamma \vdash \sigma' : K] \eta\) for all \(\eta \models \Gamma^\sigma\).

\(\square\)
6.7 LEMMA (Substitution in datatype-constructors).
Suppose \( \Gamma, y : B, \Gamma' \vdash \sigma : \mathcal{K} \) and \( \Gamma \vdash b : B \). Then

\[
\eta \left[ \Gamma, \Gamma'[y := b] \vdash \sigma[y := b] : \mathcal{K} \right] = \left[ \Gamma, y : B, \Gamma' \vdash \sigma \quad \mathcal{K} \right] \eta[y := \left[ \Gamma \vdash b \quad B \right] \eta],
\]

for all \( \eta = (\Gamma, \Gamma'[y := b])^\Omega \), and \( \eta[y] = \left[ \Gamma \vdash b : B \quad \eta \right] = (\Gamma, y : B, \Gamma')^\Omega \).

PROOF. Induction on the structure of \( \sigma \). \( \square \)

6.8 THEOREM (Soundness of \( \beta \)-conversion for datatype-constructors).
Suppose \( \sigma \equiv_\beta \sigma', \Gamma \vdash \sigma : \mathcal{K} : \Omega \), and \( \Gamma \vdash \sigma' : \mathcal{K} : \Omega \).

Then \( \left[ \Gamma \vdash \sigma : \mathcal{K} \right] \eta = \left[ \Gamma \vdash \sigma' : \mathcal{K} \right] \eta \) for all \( \eta = \Gamma^\Omega \).

PROOF. This follows from soundness of \( \beta \)-reduction, \( \text{SR}_\beta \) and \( \text{CR}_\beta \). By \( \text{CR}_\beta \) \( \sigma \) and \( \sigma' \) have a common reduct \( \sigma'' \). By \( \text{SR}_\beta \) all terms on the reduction path from \( \sigma \) or \( \sigma' \) to \( \sigma'' \) have type \( \mathcal{K} \). By soundness of \( \beta \)-reduction, all these terms have the same meaning. \( \square \)

The semantics of programs

The definition of the semantics of programs is similar to the definition of the semantics of datatype-constructors. Instead of having a family of sets \( \text{Kind} \) indexed by kinds, we now have a family of sets \( \text{Dom} \) indexed by \( \text{Kind}_\sigma \), i.e. indexed by the interpretations of datatypes. The meaning of a program of type \( \sigma \) is an element of the set that \( \text{Dom} \) associated to the meaning of \( \sigma \). So if \( \Gamma \vdash M : \sigma \), then

\[
\left[ \Gamma \vdash M : \sigma \right] \eta \subseteq \text{Dom}_M^\eta.
\]

By lemma 3.5 programs are of the form

\[
M = x | (\lambda x. M) | MM | (\lambda \alpha.K.M) | M \sigma,
\]

where \( \sigma \) ranges over datatype-constructors, \( \mathcal{K} \) over kinds, \( x \in \text{Var}^* \) and \( \alpha \in \text{Var}^{\Omega \alpha} \). Defining the semantics of programs requires mappings similar to the element-to-function mappings \( \Phi_{\mathcal{K}_1, \mathcal{K}_2} \) needed to define the semantics of datatype-constructors. However, because there are two kinds of abstraction in programs, over a datatype and over a kind, things are slightly more complicated.

Suppose \( \Gamma \vdash M : \sigma \rightarrow \tau \). Then for all \( \Gamma \vdash N : \sigma \) we have \( \Gamma \vdash MN : \tau \), so we should be able to define the meaning of \( MN \) (\( \in \text{Dom}_{\Gamma[1_{\tau \rightarrow \tau}, \ast]} \)) in terms of the meanings of \( M \) \( \in \text{Dom}_{\Gamma[1_{\tau \rightarrow \tau}, \ast]_\Omega} \) and \( N \in \text{Dom}_{\Gamma[1_{\tau \rightarrow \tau}, \ast]} \). This means the meaning of \( M \) has to be considered as a mapping from \( \text{Dom}_{\Gamma[1_{\tau \rightarrow \tau}, \ast]_\Omega} \) to \( \text{Dom}_{\Gamma[1_{\tau \rightarrow \tau}, \ast]_\Omega} \). This requires

\[
\text{Dom}_{\Gamma[1_{\tau \rightarrow \tau}, \ast]_\Omega} \cong \left[ \text{Dom}_{\Gamma[1_{\tau \rightarrow \tau}, \ast]} \rightarrow \text{Dom}_{\Gamma[1_{\tau \rightarrow \tau}, \ast]} \right], \quad (i)
\]

where the square brackets denote some subset of the function space. The associated isomorphism

\[
\Phi_{\Gamma[1_{\tau \rightarrow \tau}, \ast]_\Omega} \in \text{Dom}_{\Gamma[1_{\tau \rightarrow \tau}, \ast]_\Omega} \rightarrow \left[ \text{Dom}_{\Gamma[1_{\tau \rightarrow \tau}, \ast]} \rightarrow \text{Dom}_{\Gamma[1_{\tau \rightarrow \tau}, \ast]} \right]
\]

is the element-to-function mapping needed to define the meaning of term abstraction and application.
Suppose \( \Gamma \vdash M : (\Pi \alpha : \mathcal{K} . \sigma) \). Then \( \Gamma \vdash M \tau . \sigma[\alpha := \tau] \) for all \( \Gamma \vdash \tau : \mathcal{K} \). So for all \( \tau \) we have to define the meaning of \( M \tau . \sigma[\alpha := \tau] \) in terms of the meanings of \( M (\in \text{Dom}(\Gamma \vdash \Pi \alpha : \mathcal{K} . \sigma[\alpha := \tau]|\eta)) \) and \( \tau (\in \text{Kind}_{\mathcal{K}}) \). This requires

\[
\text{Dom}(\Gamma \vdash (\Pi \alpha : \mathcal{K} . \sigma)[\alpha := \tau]|\eta) \cong \left[ \prod_{\alpha \in \text{Kind}_{\mathcal{K}}} \text{Dom}(\Gamma \vdash \Pi \alpha : \mathcal{K} . \sigma[\alpha := \tau]|\eta)[\alpha = a] \right],
\]

where the square brackets denote some subset of the generalised Cartesian product. The associated isomorphism

\[
\Phi(\Gamma \vdash (\Pi \alpha : \mathcal{K} . \sigma)[\alpha := \tau]|\eta) \in \text{Dom}(\Gamma \vdash (\Pi \alpha : \mathcal{K} . \sigma)[\alpha := \tau]|\eta) \rightarrow \prod_{\alpha \in \text{Kind}_{\mathcal{K}}} \text{Dom}(\Gamma \vdash \Pi \alpha : \mathcal{K} . \sigma[\alpha := \tau]|\eta)[\alpha = a]
\]

is used to define the meaning of kind abstraction and application.

So for a model for \( \lambda \omega \), we need a family of sets \( \text{Dom} \) such that

\[
\text{Dom}_{a \sqcup b} \cong [\text{Dom}_a \rightarrow \text{Dom}_b]
\]

\[
\text{Dom}_{\prod F} \cong \left[ \prod_{a \in \text{Kind}_{\mathcal{K}}} \text{Dom}_F(a) \right]
\]

for all \( a, b \in \text{Kind}_\ast \) and all \( F \in \text{Kind}_{\mathcal{K} \rightarrow \mathcal{K}_\ast} \).

6.9 Definition. An environment frame for \( \lambda \omega \) is a 4-tuple \( \langle \text{Kind}, \text{Dom}, \Phi^-, \Phi^\Pi \rangle \), where

- \( \text{KIND} = \langle \text{Kind}, \Phi_{\text{Kind}}[\square] \rangle \) is an environment model for the datatype-constructors.
- \( \text{Dom} = \{\text{Dom}_a | a \in \text{Kind}_\ast\} \) is a family of sets, indexed by \( \text{Kind}_\ast \).
- \( \Phi^- = \{\Phi^- a \mid a, b \in \text{Kind}_\ast\} \) and \( \Phi^\Pi = \{\Phi^\Pi F \mid \square : \mathcal{K} \rightarrow \text{Kind}_\ast\} \) are families of bijections with

\[
\Phi^- a b \in \text{Dom}_a [\square] b \rightarrow [\text{Dom}_a \rightarrow \text{Dom}_b],
\]

\[
\Phi^\Pi F \in \text{Dom}_{\prod F} \rightarrow \left[ \prod_{a \in \text{Kind}_{\mathcal{K}}} \text{Dom}_F(a) \right],
\]

where the square brackets denote some subset of the function space and the product, respectively.

The meaning of a program depends on an environment that gives the meaning of its free variables. The meanings assigned to the free variables have to match the types assigned to them in the context.

6.10 Definition. Let \( \Gamma \) be a \( \lambda \omega \)-context. An environment \( \eta \) satisfies \( \Gamma \vartriangleleft \eta \) — written \( \eta \models \Gamma \vartriangleleft \eta \) — if

- \( \eta \models \Gamma \vartriangleleft \), i.e. \( \eta(\alpha) \in \text{Kind}_{\mathcal{K}} \) for all \( \alpha : \mathcal{K} \) in \( \Gamma \vartriangleleft \), and
- \( \eta(\tau) \in \text{Dom}(\Gamma \vdash \sigma[\alpha := \tau]|\eta) \) for all \( \tau : \sigma \) in \( \Gamma \vartriangleleft \).
6.11 Definition (Semantics of programs).

For programs \( M \) we define \([ \Gamma \vdash M : \sigma ]\eta \) for all \( \Gamma \vdash M : \sigma \) and \( \eta \models \Gamma^\omega \), by induction on the derivation of \( \Gamma \vdash M : \sigma \), as follows:

\[
[\Gamma, x : \sigma, \Gamma' \vdash x : \sigma] \eta \equiv \eta(x)
\]

\[
[\Gamma \vdash M : \sigma] \eta \equiv [\Gamma \vdash M : \sigma'] \eta
\]

if \( \Gamma \vdash M : \sigma \) follows from \( \Gamma \vdash M : \sigma' \) by \((\beta_{\text{conv}})\).

\[
[\Gamma \vdash MN : \tau] \eta \equiv (\Phi_1[\Gamma \vdash M : \sigma \rightarrow \tau] \eta)[\Gamma \vdash N : \sigma] \eta
\]

\[
[\Gamma \vdash (\lambda x. M) : \sigma \rightarrow \tau] \eta \equiv \Phi^{-1}_1(\lambda x \in \text{Dom}[I \vdash \sigma \ast_1]) \eta \]

\[
[\Gamma \vdash M\alpha : \tau\alpha = \sigma] \eta \equiv (\Phi_2[\Gamma \vdash M (\Pi \alpha K. \tau)] \eta)[\Gamma \vdash \sigma - K] \eta
\]

\[
[\Gamma \vdash (\lambda \alpha K. M) : (\Pi \alpha K. \tau)] \eta \equiv \Phi^{-1}_2(\lambda a \in \text{Kind}_K) \eta \]

\[
[\Gamma \vdash M : \tau[\alpha = \sigma]] \eta \equiv \Phi_2(\lambda a \in \text{Kind}_K) \eta[\alpha = a]
\]

where \( \Phi_1 = \Phi[I \vdash \sigma \ast_1] \eta \) and \( \Phi_2 = \Phi[I \vdash K \ast_1] \eta \).

By lemma 3.5 the clauses in this definition cover all possible type derivations for programs. However, not for every environment frame is \([ \Gamma \vdash M : \sigma ]\eta \) well-defined for all \( \Gamma \vdash M : \sigma \) and \( \eta \models \Gamma^\omega \). In order for the meaning of an abstraction \((\lambda x. M)\) or \((\lambda \alpha K. M)\) to be defined, the ranges of the \( \Phi_1 \) and \( \Phi_2 \) above have to be large enough.

6.12 Definition. A \( \lambda \omega \)-environment model is a \( \lambda \omega \)-environment frame for which \([ \Gamma \vdash M : K ] \eta \) is defined for all \( \Gamma \vdash M : K \) and \( \eta \models \Gamma^\omega \).

Of course we want to show that the meaning of a program does not depend on the particular type derivation we consider. Unlike for datatype-constructors, for a program there can be many type derivations, in which the rule \((\beta_{\text{conv}})\) is used in different places, and different (but \( \beta \)-convertible) types are derived for subexpressions of the program. To show that this does not influence the interpretation of the program, we need the fact that these \( \beta \)-convertible types have the same interpretation. This has already been proved in theorem 6.8, soundness of \( \beta \)-conversion for the datatype-constructors.

6.13 Lemma. Let \( d\tau_1 \) and \( d\tau_2 \) be derivations of \( \Gamma \vdash M : \sigma \) and \( \Gamma \vdash M : \sigma' \), respectively. Then

\[
[\Gamma \vdash M : \sigma] \eta = [\Gamma \vdash M : \sigma'] \eta
\]

where the meanings are defined using \( d\tau_1 \) and \( d\tau_2 \) respectively.

Proof. Induction on the structure of \( M \) using \( UT_\beta \) and the soundness of \( \beta \)-conversion for datatype-constructors (theorem 6.8).

6.14 Theorem (Soundness of type assignment for programs).

If \( \Gamma \vdash M : \sigma \) then \([ \Gamma \vdash M : \sigma ] \eta \in \text{Dom}[I \vdash \sigma \ast_1] \eta \) for all \( \eta \models \Gamma^\omega \).

Proof. Induction on the derivation of \( \Gamma \vdash M : \sigma \), using soundness of type assignment for datatype-constructors (theorem 6.5).
6.1. GENERAL MODEL DEFINITION FOR $\lambda\omega$

6.15 LEMMA (Soundness of $\beta$-reduction for programs).
Suppose $M \beta M'$, $\Gamma \vdash M : \sigma$ and $\Gamma \vdash M' : \sigma'$.
Then $[\Gamma \vdash M : \sigma] \eta = [\Gamma \vdash M' : \sigma'] \eta$ for all $\eta \models \Gamma^\varphi$.

PROOF. Induction on the structure of $M$.
Datatype-constructors can be subterms of programs, so the reduction in $M$ can be a reduction in a datatype-constructor in $M$. Hence we need soundness of $\beta$-reduction for the datatype-constructors (lemma 6.6).

The interesting case is the case that $M$ is a redex, where we use the substitution lemma for programs given below. \hfill \Box

6.16 LEMMA (Substitution in programs).
Suppose $\Gamma, y : B, \Gamma' \vdash M : \sigma$ and $\Gamma \vdash b : B$. Then
$$[[\Gamma', y := b \vdash M[y := b] : \sigma[y := b]] \eta = [[\Gamma, y : B, \Gamma' \vdash M : \sigma] \eta[y := [\Gamma \vdash b : B] \eta],
$$
for all $\eta \models (\Gamma, \Gamma'[y := b])^\varphi$, and $\eta[y := [\Gamma \vdash b : B] \eta] \models (\Gamma, y : B, \Gamma')^\varphi$.

PROOF. Induction on the structure of $M$, using the substitution lemma for the datatype-constructors (lemma 6.7). We treat just one case, the case that $M$ is an abstraction, i.e. $M \equiv (\lambda x \rho. N)$. Its type is then a function type, i.e. $\sigma \equiv \rho \rightarrow \tau$.

First some abbreviations: $\overline{A}$ is $A[y := b]$ for $\lambda\omega$-terms $A$, and
$$\Delta \equiv \Gamma, \Gamma'[y := b]
\quad \Delta \equiv \Gamma, y : B, \Gamma'
\quad \overline{\eta} \equiv \eta[y := [\Gamma \vdash b : B] \eta]$$
So $\Delta \vdash b : B$ and $\Delta \vdash (\lambda x \rho. N) : \rho \rightarrow \tau$.

Suppose $\eta \models \Delta, \Gamma'[y := b]$ and $\eta[y := [\Gamma \vdash b : B] \eta] \models \Delta, y : B, \Gamma'$, i.e. $\eta \models \Delta$, and $\overline{\eta} \models \Delta$.

To prove
$$[[\Delta \vdash (\lambda x \rho. N) \rho \rightarrow \tau \overline{\eta}] = [[\overline{\Delta} \vdash \overline{(\lambda x \rho. N) : \rho \rightarrow \tau \eta}]]$$
(i)

By the definition of $[ \ldots ]$:
$$[[\Delta \vdash (\lambda x \rho. N) : \rho \rightarrow \tau \overline{\eta}] = \Phi_{[\Delta \vdash \rho \rightarrow \tau \eta]}(A, x \in \text{Dom}_{[\Delta \vdash \rho \rightarrow \tau \eta]} \bullet [\Delta \vdash \rho \rightarrow \tau \eta] [\Delta, \Gamma \vdash N : \tau] \overline{x} = \xi)]$$
$$[[\overline{\Delta} \vdash \overline{(\lambda x \rho. N) : \rho \rightarrow \tau \eta}]\eta = \Phi_{[\overline{\Delta} \vdash \rho \rightarrow \tau \eta]}(A, x \in \text{Dom}_{[\overline{\Delta} \vdash \rho \rightarrow \tau \eta]} \bullet [\overline{\Delta}, \overline{\Gamma} \vdash N : \tau] \overline{x} = \xi)]$$
By the substitution lemma for datatype-constructors
$$[[\Delta \vdash \rho \rightarrow \tau \bullet] \eta] = [[\overline{\Delta} \vdash \overline{\rho} \rightarrow \overline{\tau} \bullet] \eta]$$
$$[[\Delta \vdash \rho \rightarrow \tau \bullet] \eta] = [[\overline{\Delta} \vdash \overline{\rho} \rightarrow \overline{\tau} \bullet] \eta]$$
and by the IH
$$[[\Delta, \Gamma \vdash N : \tau] \overline{x} = \xi] = [[\overline{\Delta}, \overline{\Gamma} \vdash \overline{N} : \overline{\tau}] \overline{x} = \xi],$$
and so (i). Note that the IH only applies if $\eta[r = \xi] \models (\Delta, x : \rho)$ and $\overline{\eta}[x = \xi] \models (\Delta, x : \rho)$. This follows from $\eta \models \overline{\Delta}, \overline{\eta} \models \overline{\Delta}$ and
$$\xi \in \text{Dom}_{[\overline{\Delta} \vdash \overline{\rho} \rightarrow \overline{\tau} \bullet]} \overline{\eta} = \text{Dom}_{[[\overline{\Delta} \vdash \overline{\rho} \rightarrow \overline{\tau} \bullet] \overline{\eta}]}$$
\hfill \Box
6.17 THEOREM (Soundness of \( \beta \)-conversion for programs).
Suppose \( M \simeq_{\beta} M' \), \( \Gamma \vdash M : \sigma \), and \( \Gamma \vdash M' : \sigma' \).
Then \( \{ \Gamma \vdash M : \sigma \} \eta = \{ \Gamma \vdash M' : \sigma' \} \eta \) for all \( \eta \models \Gamma^{\sim} \).

PROOF. This follows from soundness of \( \beta \)-reduction, \( SR_\eta \) and \( CR_\eta \).

In fact, the environment models for \( \lambda \omega \), respect not only \( \beta \)- but also \( \eta \)-equality. This follows immediately from the fact that the \( \Phi_{R_1}, R_2, \Phi_{\lambda \beta}, \) and \( \Phi_{\Pi} \) are all bijections.
6.2 PER-Model for $\lambda_\omega$}

The best-known models for the second and higher-order lambda calculus are the so-called PER-models, first given in [Gir72]. In these models datatypes are interpreted as partial equivalence relations over some partial combinatory algebra, and programs as equivalence classes. In this section it is shown that the PER-model given in [Gir72], called $HEO^\alpha$, can easily be fitted in the general model definition for $\lambda_\omega$.

6.18 Definition. 1. $(\mathbb{N}, )$ is Kleene's applicative structure. This means we have some enumeration of the partial recursive functions, and $n m$ is the result of applying the $n^{th}$ partial recursive function to $m$.

2. PER is the set of all partial equivalence relations on $\mathbb{N}$.

3. if $R \in$ PER and $n \in \mathbb{N}$, then $[n]_R$ is the equivalence class of $R$ that contains $n$, i.e. $[n]_R = \{ m \in \mathbb{N} \mid (n, m) \in R \}$.

For the model for the datatype-constructors sets $Kind_{\mathbb{K}}$ are needed, and functions $\rightarrow$ and $\prod$:

6.19 Definition

1. For all kinds $\mathbb{K}$ the set $Kind_{\mathbb{K}}$ is defined as follows

$$
\begin{align*}
Kind_{\mathbb{K}} & \triangleq \text{PER} \\
Kind_{\mathbb{K}_1 \rightarrow \mathbb{K}_2} & \triangleq \text{Kind}_{\mathbb{K}_1} \rightarrow \text{Kind}_{\mathbb{K}_2}
\end{align*}
$$

Here $Kind_{\mathbb{K}_1 \rightarrow \mathbb{K}_2}$ is the set of all functions from $Kind_{\mathbb{K}_1}$ to $Kind_{\mathbb{K}_2}$

2. The functions $\rightarrow : \text{PER} \rightarrow \text{PER} \rightarrow \text{PER}$ and $\prod : \prod_{\mathbb{K} \in \mathbb{K}_1} (\text{Kind}_{\mathbb{K}} \rightarrow \text{PER}) \rightarrow \text{PER}$ are defined by

$$
\begin{align*}
S \rightarrow T & \triangleq \{ (n, n') \in \mathbb{N}^2 \mid (n, m', m') \in T \text{ for all } (m, m') \in S \} \\
\prod F & \triangleq \bigcap_{a \in \text{Kind}_{\mathbb{K}}} F(a)
\end{align*}
$$

6.20 Lemma. $KIND_{HEO} = (Kind, \Phi_{Kind}, \rightarrow, \prod)$, where all the bijections in $\Phi_{Kind}$ are identities, is an environment model for the datatype-constructors.

Proof. Trivial, because all $\Phi_{\mathbb{K}_1, \mathbb{K}_2}$ are identities.

To complete the model for $\lambda_\omega$ we need a family of sets $\text{Dom}$ and associated families of bijections $\Phi_{\rightarrow}$ and $\Phi_{\prod}$.

6.21 Definition Let $R, S, T \in$ PER and $F \in Kind_{\mathbb{K}} \rightarrow$ PER for some kind $\mathbb{K}$ Then

1. $\text{Dom}_R \triangleq \{ [n]_R \mid (n, n) \in R \}$. 


2 \( \Phi^-_{ST} \in \text{Dom}_S \rightarrow \text{Dom}_T \) is defined by
\[
\Phi^-_{ST} [m]_S [n]_T \equiv [m \cdot n]_T
\]

3 \( \Phi^\Pi \in \text{Dom}_F \rightarrow \prod_{a \in \text{Kind}_F} \text{Dom}_{F(a)} \) is defined by
\[
\Phi^\Pi [m]_F a \equiv [m]_{F(a)}.
\]

The definitions of \( \Phi^-_{ST} \) and \( \Phi^\Pi \) are given in terms of representatives of equivalence classes. Checking that they are well-defined as functions on equivalence classes is straightforward. For \( \Phi^-_{ST} \) we have to verify that \((m, n, m' \cdot n') \in T \) if \((m, m') \in S \) and \((n, n') \in S \) (i.e., that \([m \cdot n]_T = [m' \cdot n']_T \) if \([m]_S [n]_T = [m']_S [n']_T \) and \([n]_S = [n']_S \) ). For \( \Phi^\Pi \) we have to verify that \((m, m') \in F(a) \) if \((m, m') \in [\Pi] F \) These properties immediately follow from the definitions of \( - \) and \( \Pi \).

6.22 Lemma. \( \langle \text{KIND}_{HEG}, \text{Dom}, \Phi^-, \Phi^\Pi \rangle \) is an environment frame for \( \lambda \omega_1 \).

Proof. We only have to show that
\[
\Phi^-_{ST} \in \text{Dom}_S \rightarrow \text{Dom}_T \quad \Phi^\Pi \in \text{Dom}_F \rightarrow \prod_{a \in \text{Kind}_F} \text{Dom}_{F(a)}
\]
are bijections, for certain subsets \([\text{Dom}_S \rightarrow \text{Dom}_T] \) of \([\text{Dom}_S \rightarrow \text{Dom}_T] \), and certain subsets \([\prod_{a \in \text{Kind}_F} \text{Dom}_{F(a)}] \) of \([\prod_{a \in \text{Kind}_F} \text{Dom}_{F(a)}] \). As these subsets we take the ranges of \( \Phi^-_{ST} \) and \( \Phi^\Pi \).

6.23 Lemma. \( \langle \text{KIND}_{HEG}, \text{Dom}, \Phi^-, \Phi^\Pi \rangle \) is an environment model for \( \lambda \omega_1 \).

Proof. We have to prove that \( \Gamma \vdash M : \sigma \) \( \eta \) is defined for all \( \Gamma \vdash M \) \( \sigma \) and \( \eta \equiv \Gamma^{- \sigma} \). To prove this we proceed by induction on the structure of \( M \) that if \( I \vdash M : \sigma \) with \( \Gamma^{- \sigma} \equiv x_1 : \rho_1, \ldots, x_m : \rho_m \), then there is a partial recursive function \( f \in \mathbb{N}^m \rightarrow \mathbb{N} \) such that for all \( \eta \equiv \Gamma^{- \sigma} \) with \([n]_F^{\rho_1, \ldots, \rho_m} \eta \equiv \eta(x_i)\)
\[
[f(n_1, \ldots, n_m)]_{[I \vdash \sigma \cdot \eta]} \equiv [\Gamma \vdash M : \sigma] \eta
\]
In other words, given representatives \( n \) of the equivalence classes \( \eta \), \( f \) returns a representative of the equivalence class \([f \Gamma \vdash M : \sigma] \eta \).

The crucial case in this induction is the case that \( M \) is an abstraction, for which we need Kleene's s-m-n theorem (see e.g. \( \text{Kleene's s-m-n theorem} \)).
6.3 Proof-irrelevance Model for $\lambda\omega_p$

In this section the general model definition given in 6.1 is instantiated to produce a model for the logic $\lambda\omega_p$. The model for $\lambda\omega_p$ can be much simpler than that for $\lambda\omega_s$, because our main concern is the interpretation of the types (propositions), and not the interpretation of the terms (proofs). Propositions are interpreted as truth values in this model, and all proof terms are identified, which is why the model is called a proof-irrelevance model. This simple model is all that is needed to prove consistency of $\lambda\omega_p$, and to check the consistency of any additional axioms.

To stress that this model is meant as a model for $\lambda\omega_p$ and not for $\lambda\omega_s$, we use $P\text{Kind}$, $P\text{Dom}$, $\exists$ and $\forall$ instead of $\text{Kind}$, $\text{Dom}$, $\Pi$ and $\Sigma$, respectively. Indeed, the model is useless as a model for the programming language $\lambda\omega_s$, because it would identify all programs. As we shall see, some of the technical machinery needed for an environment model can be avoided for this particular model, because it is so simple.

A proposition is interpreted as either the empty set 0 (representing "false") or as a singleton set 1 (representing "true").

6.24 Definition For all propkinds $\mathcal{P}$ the set $P\text{Kind}_{\mathcal{P}}$ is defined as

$$P\text{Kind}_{\mathcal{P}} = \{0, 1\}$$

Here $P\text{Kind}_{\mathcal{P}_1} \rightarrow P\text{Kind}_{\mathcal{P}_2}$ is the set of all functions from $P\text{Kind}_{\mathcal{P}_1}$ to $P\text{Kind}_{\mathcal{P}_2}$. □

For the interpretation of propositions that are formed using implication or universal quantification we define:

6.25 Definition. The functions $\exists \in P\text{Kind}_{\mathcal{P}} \rightarrow P\text{Kind}_{\mathcal{P}}$ and $\forall \in \Pi_{\mathcal{P} \in \mathcal{P}}(P\text{Kind}_{\mathcal{P}} \rightarrow P\text{Kind}_{\mathcal{P}})$ are defined as follows

$$P(\exists X) Q \equiv \begin{cases} 1 & \text{if } P = 0 \text{ or } Q = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$\forall X P \rightarrow Q \equiv \bigcap_{X \in P\text{Kind}_{\mathcal{P}}} F(X)$$

So $\forall X P \rightarrow Q = 1$ iff $F(X) = 1$ for all $X \in P\text{Kind}_{\mathcal{P}}$. □

6.26 Lemma. $P\text{Kind} = \langle P\text{Kind}, \Phi_{P\text{Kind}}, \exists, \forall \rangle$, where all the bijections in $\Phi_{P\text{Kind}}$ are identities, is an environment model for the $\lambda\omega_p$ prop-constructors.

Proof. Trivial, because all $\Phi_{\mathcal{P}_1, \mathcal{P}_2}$ are identities. □

6.27 Example. For the propositional constants and logical connectives defined in definition 3.11 we get

\[
\begin{align*}
[\text{False : } & \ast_{\mathcal{P}}] = 0 \\
[\text{True : } & \ast_{\mathcal{P}}] = 1 \\
[\neg : & \ast_{\mathcal{P}} \rightarrow \ast_{\mathcal{P}}] = \lambda X \in \{0, 1\}. \begin{cases} 1 \text{ if } X = 0 \\ 0 \text{ if } X = 1 \end{cases} \\
[\land : & \ast_{\mathcal{P}} \rightarrow \ast_{\mathcal{P}} \rightarrow \ast_{\mathcal{P}}] = \lambda X, Y \in \{0, 1\}. X \land Y \\
[\lor : & \ast_{\mathcal{P}} \rightarrow \ast_{\mathcal{P}} \rightarrow \ast_{\mathcal{P}}] = \lambda X, Y \in \{0, 1\}. X \lor Y \\
[\exists : & (\mathcal{P} \rightarrow \ast_{\mathcal{P}}) \rightarrow \ast_{\mathcal{P}}] = \lambda F \in P\text{Kind}_{\mathcal{P}} \rightarrow \{0, 1\} . \cup_{X \in P\text{Kind}_{\mathcal{P}}} F(X) \\
\end{align*}
\]
As the family of sets $P\text{Dom}$ that maps each element $P$ of $P\text{Kind}_{\ast}$ to a set $P\text{Dom}_\mu$ we can simply take the identity:

6.28 DEFINITION. $P\text{Dom}_1 = 1$ and $P\text{Dom}_0 = 0$. □

Then the domain equations

$$ P\text{Dom}_\mu \xrightarrow{\rightarrow} Q \equiv P\text{Dom}_\mu \longrightarrow P\text{Dom}_Q $$

$$ P\text{Dom}_\mu \bigvee_{\mu \cdot F} \equiv \prod_{X \in P\text{Kind}_{\mu}} P\text{Dom}_{\mu(X)} $$

become

$$ P \xrightarrow{\rightarrow} Q \equiv P \longrightarrow Q $$

$$ \bigvee_{\mu \cdot F} \equiv \prod_{X \in P\text{Kind}_{\mu}} F(X) $$

By the definition of $\xrightarrow{\rightarrow}$ and $\bigvee$, either both sides are the empty set or both sides are singleton sets. So the domain equations for $P\text{Dom}$ are solved. Moreover, all the associated isomorphisms are unique, since the isomorphisms are either between two one-element sets or between two empty sets. If we let $\Phi_X$ and $\Phi_Y$ be the isomorphisms solving the domain equations above, then

6.29 LEMMA. $(P\text{Kind}, P\text{Dom}, \Phi_X, \Phi_Y)$ is an environment model for $\lambda \omega_\mu$.

PROOF. Easy, because $P \xrightarrow{\rightarrow} Q$ and $\bigvee_{\mu \cdot F}$ are isomorphic with the whole function space $P \longrightarrow Q$ and the whole product $\prod_{X \in P\text{Kind}_{\mu}} F(X)$, respectively. □

If $\Gamma \vdash \mu : P : \ast_\mu$ and $\eta \models I \rightarrow \ast_\mu$ then by soundness of type assignment

$$ [\Gamma \vdash \mu : P] \eta \in [\Gamma \vdash \mu : \ast_\mu] \eta \in \{0, 1\} $$

But this is only possible if $[\Gamma \vdash \mu : \ast_\mu] \eta = 1$, and then $[\Gamma \vdash \mu : P] \eta \in 1$. This means that all proofs are identified in this model, they are all interpreted as the element of 1. Instead of defining the interpretation of a proof by induction on its type derivation it could simply be defined as the element of 1.

It also follows immediately from soundness of type assignment that:

6.30 COROLLARY $P$ is not provable in context $\Gamma$ if $[\Gamma \vdash \mu : \ast_\mu] \eta = 0$ for some $\eta \models I \rightarrow \ast_\mu$. □

This can be used to prove consistency (of contexts) in $\lambda \omega_\mu$, for example

6.31 COROLLARY (Consistency)

1. False is not provable in the empty context.

2. False is not provable in the context containing just the assumption $\text{classic} \cdot \forall \mu \cdot \ast_\mu \to (\to \mu) \iff \mu$.


6.3. PROOF-IRRELEVANCE MODEL FOR $\lambda\omega P$

PROOF. 1. follows immediately from the fact that $[[\text{False} : *_p]] = 0$. For 2. we also have to show that there is an environment $\eta$ that satisfies the context $\text{classic} : \forall P : *_p. (\neg\neg P) \Rightarrow P$.

The only possible choice for $\eta$ is the environment that maps $\text{classic}$ to the element of 1. That this environment satisfies the context follows from $[[\forall P : *_p. (\neg\neg P) \Rightarrow P : *_p]] = 1$.

This proof-irrelevance model can be seen as a degenerated PER-model, namely the PER-model where partial equivalence relations over 1 instead of $\mathbb{N}$ are used, and the only possible function in $1^2 \rightarrow 1$ is used instead of the Kleene application $\in \mathbb{N}^2 \rightarrow \mathbb{N}$.
6.4 Model for $\lambda \omega_L$

We now turn to the semantics of the whole system $\lambda \omega_L$. Recall that $\lambda \omega_L$ consists of three parts:

- the programming language $\lambda \omega_s$,
- the purely logical part $\lambda \omega_p$,
- four more PTS-rules that allow the formation of proofs and propositions that depend on programs and datatypes

This means that a model for $\lambda \omega_L$ will contain a submodel for $\lambda \omega_s$ and a submodel for $\lambda \omega_p$. We will in fact produce a model for $\lambda \omega_L$ by combining a model for $\lambda \omega_s$ and a model for $\lambda \omega_p$. To be precise, an arbitrary model for $\lambda \omega_s$ and the proof-irrelevance model for $\lambda \omega_p$ will be combined.

$\lambda \omega_L$ has the same programs and datatypes as $\lambda \omega_s$, so any model for $\lambda \omega_s$ can be used to interpret the programs and datatypes of $\lambda \omega_L$. This means we do not have to fix a particular interpretation for $\lambda \omega_s$ yet. A model for $\lambda \omega_p$ can be given with respect to an arbitrary model for the $\lambda \omega_s$-part.

On the other hand, $\lambda \omega_L$ does have more proofs and propositions than $\lambda \omega_p$. We fix a particular interpretation for the $\lambda \omega_p$-part, namely the proof-irrelevance model defined in the previous section. This proof-irrelevance model can easily be extended to interpret these additional constructs in the logic-part of $\lambda \omega_L$.

Recall that in $\lambda \omega_L$ six syntactic categories were distinguished, namely

1. kinds, which are elements of Kind,
2. datatype-constructors, which are elements of Cons,
3. programs, which are elements of Prog,
4. propkinds, which are elements of Pkind,
5. prop-constructors, which are elements of PCons,
6. proofs, which are elements of Proof

Each of these depends only on (some of) the ones that precede it in the order given above. This layered structure is a result of the fact that some $(s_1, s_2)$ combinations are excluded as PTS-rules in the definition of $\lambda \omega_L$. Here the layered structure pays off. It can be exploited by giving the semantics of each of the levels separately.

Let

$$M = (KIND, Dom, \Phi, \Phi^1)$$

be any environment model for $\lambda \omega_s$, with

$$KIND = (\text{Kind}, \Phi_{\text{Kind}}, \rightarrow, \Pi)$$

In the rest of this section a $\lambda \omega_L$-model will be defined in which this model $M$ is the $\lambda \omega_s$-submodel.
6.4. MODEL FOR $\lambda \omega_L$

The semantics of datatype-constructors and programs

$\lambda \omega_L$ has the same kinds, datatype-constructors and programs as $\lambda \omega_s$, their interpretation is simply given by $M$:

6.32 Definition. 1. $\eta \models \Gamma^{\circ}$ and $\eta \models \Gamma^{\circ*}$ are defined for $\lambda \omega_L$-contexts $\Gamma$ as for $\lambda \omega_s$-contexts (definitions 6.2 and 6.10).

2. $[\Gamma \vdash \sigma : K] \eta$ is defined for all $\Gamma \vdash \sigma : K$ and $\eta \models \Gamma^{\circ}$ as in definition 6.3.

3. $[\Gamma \vdash \nu : \sigma] \eta$ is defined for all $\Gamma \vdash \nu : \sigma$ and $\eta \models \Gamma^{\circ*}$ as in definition 6.11.

Because $M$ is an environment model of $\lambda \omega_s$, this interpretation has all the properties we have for environment models for $\lambda \omega_s$, e.g. soundness of type assignment and conversion.

The semantics of prop-kinds

By lemma 3.17 the prop-kinds are of the form

$$\mathcal{P} ::= \ast_p \mid \mathcal{P} \rightarrow \mathcal{P} \mid \sigma \rightarrow \mathcal{P} \mid (\Pi \alpha : K, \mathcal{P})$$

where $K$ ranges over kinds, $\sigma$ over datatype-constructors, and $\alpha \in \text{Var}^{\mathcal{P}}$. So prop-kinds can contain free variables. For example, in $\alpha : \ast \vdash \alpha \rightarrow \ast : \square_p$, the prop-kind $\alpha \rightarrow \ast$ contains a free variable $\alpha$. This means that the interpretation of a prop-kind depends on an environment that gives the interpretation of its free variables.

6.33 Definition (Semantics of prop-kinds)

For $\lambda \omega_L$-propkinds $\mathcal{P}$ we define $[\Gamma \vdash \mathcal{P} : \square_p] \eta$ for all $\Gamma \vdash \mathcal{P} : \square_p$ and $\eta \models \Gamma^{\circ}$, by induction on the derivation of $\Gamma \vdash \mathcal{P} : \square_p$, as follows

$$[\Gamma \vdash \ast_p : \square_p] \eta \equiv (0, 1)$$

$$[\Gamma \vdash \mathcal{P}_1 \rightarrow \mathcal{P}_2 : \square_p] \eta \equiv [\Gamma \vdash \mathcal{P}_1 : \square_p] \eta \rightarrow [\Gamma \vdash \mathcal{P}_2 : \square_p] \eta$$

$$[\Gamma \vdash \sigma \rightarrow \mathcal{P} : \square_p] \eta \equiv \text{Dom}_{[\Gamma \vdash \sigma : \square_p]} \rightarrow [\Gamma \vdash \mathcal{P} : \square_p] \eta$$

$$[\Gamma \vdash (\Pi \alpha : K, \mathcal{P}) : \square_p] \eta \equiv \prod_{\alpha \in \text{Var}^{\mathcal{P}}} [\Gamma, \alpha : K, \vdash \mathcal{P} : \square_p] \eta[\alpha := a]$$

Here in the right hand sides, $A \rightarrow B$ is the set of all functions from $A$ to $B$, and $\prod_{\alpha \in A} B(\alpha)$ is the set of all functions that map an $\alpha \in A$ to an element of $B(\alpha)$. By lemma 3.17 the clauses above define $[\Gamma \vdash \mathcal{P} : \square_p] \eta$ for all propkinds $\mathcal{P}$.

$[\Gamma \vdash \mathcal{P} : \square_p] \eta$ is just the same as $\mathcal{PKind}_\mathcal{P}$ as defined in the previous section for the propkinds that are typable in $\lambda \omega_s$.

6.34 Lemma (Soundness of $\beta$-reduction for prop-kinds).

Suppose $\mathcal{P} \triangleright_\beta \mathcal{P}'$, $\Gamma \vdash \mathcal{P} : \square_p$ and $\Gamma \vdash \mathcal{P}' : \square_p$.

Then $[\Gamma \vdash \mathcal{P} : \square_p] \eta = [\Gamma \vdash \mathcal{P}' : \square_p] \eta$ for all $\eta \models \Gamma^{\circ}$.

Proof. Induction on the structure of $\mathcal{P}$, using soundness of $\beta$-reduction for the datatype-constructors (lemma 6.6).
The substitution lemma for propkinds is not needed to prove soundness of $\beta$-reduction for propkinds, because all reductions in a propkind occur in subexpressions that are datatype-constructors. We will need the substitution lemma later.

6.35 Lemma (Substitution in propkinds).

Suppose $\Gamma, y : B, \Gamma' \vdash P \square p$ and $\Gamma \vdash b : B$. Then

$$[[\Gamma, \Gamma'[y := b] \vdash P[y := b] \square p] \eta] = [[\Gamma, y : B, \Gamma' \vdash P \square p] \eta[y := [\Gamma \vdash b : B] \eta]],$$

for all $\eta : (\Gamma, \Gamma'[y := b] \square p)$. and $\eta[y := [\Gamma \vdash b : B] \eta] = (\Gamma, y : B, \Gamma') \square p$.

Proof: Induction on the structure of $P$, using the substitution lemma for the datatype-constructors (lemma 6.7).

6.36 Theorem (Soundness of $\beta$-conversion for propkinds).

Suppose $P \equiv_\beta P'$, $\Gamma \vdash P \square p$ and $\Gamma \vdash B' : \square_p$.

Then $[[\Gamma \vdash P \square p] \eta] = [[\Gamma \vdash P' \square p] \eta]$ for all $\eta : \Gamma \square p$.

Proof: This follows SR$_3$, CR$_3$, and from soundness of $\beta$-reduction for propkinds (lemma 6.34).

The semantics of prop-constructors

By lemma 3.17 the prop-constructors are of the form

$$P : = x | (\lambda y : A. P) | Pa | (\forall y : A. P) | P \Rightarrow P,$$

where $A$ ranges over the kinds, datatype-constructors and prop-kinds, $\alpha$ over the datatype-constructors, programs and prop-constructors, and $x \in \text{Var}_{\square p}$.

The interpretation of a prop-constructor $P : \square p$ will be an element of the interpretation of $\square p$, i.e. if $\Gamma \vdash P : \square p$, then $[[\Gamma \vdash P \square p] \eta] = \{ \eta(P) \in [[\Gamma \vdash \square p] \eta] : \forall P \vdash \square p \in \Gamma \square p \}$. For example predicates on a datatype $\sigma$ are interpreted as characteristic functions of subsets of $\text{Dom}_{\Gamma \vdash \sigma \square p}$.

6.37 Definition. Let $\Gamma$ be a $\lambda \omega_t$-context. An environment $\eta$ satisfies $\Gamma \square \sigma \square p$ written $\eta \models \Gamma \square \sigma \square p$ if $\eta \models \Gamma \square \sigma \square p$ and $\eta(P) \in [[\Gamma \vdash \square p] \eta]$ for all $P : \square p \in \Gamma \square p$.

Given the definition of $[\Gamma \vdash \square p] \eta$, the interpretation of application and abstraction in prop-constructors is straightforward. For the interpretation of products in propositions we use intersections, as in the model for $\lambda \omega_p$.

6.38 Definition (Semantics of prop-constructors).

For $\lambda \omega_t$-propconstructors $P$ we define $[[\Gamma \vdash P \square p] \eta]$ for all $\Gamma \vdash P \square p$ and $\eta : \Gamma \square \sigma \square p$, by induction on the derivation of $\Gamma \vdash P \square p$, as follows

$$[[\Gamma, \Gamma' \vdash P, \Delta \vdash r \square p] \eta] = \eta(\tau),$$

$$[[\Gamma \vdash P \square p] \eta] = [[\Gamma \vdash P \square p] \eta],$$

if $\tau \vdash P \square p \square p$ follows from $\Gamma \vdash P \square p \square p$ by ($\beta\text{Conv}$)

$$[[\Gamma \vdash Pa : \square p[x := a]] \eta] = [[\Gamma \vdash P : (\Pi x.A \square p)] \eta[[\Gamma \vdash a : A] \eta],$$

$$[[\Gamma \vdash (\lambda x.A.P) (\Pi x.A \square p)] \eta] = \begin{cases} \lambda \xi \in A & \{ [[\Gamma, x : A \vdash P : \square p] \eta[x := \xi]] \}
\end{cases},$$

$$[[\Gamma \vdash (\forall x : A. P) : \square p] \eta] = \bigcap_{x : A} [[\Gamma, x : A \vdash P : \square p] \eta[x := \xi]]$$
6.39 **Lemma.** Let $d_1$ and $d_2$ be derivations of $\Gamma \vdash P : P'$ and $\Gamma \vdash P : P''$, respectively. Then

$$\llbracket \Gamma \vdash P : P' \rrbracket \eta = \llbracket \Gamma \vdash P : P'' \rrbracket \eta,$$

where the meanings are defined using $d_1$ and $d_2$ respectively.

**Proof.** Induction on the structure of $P$.

6.40 **Theorem.** (Soundness of type assignment for prop-constructors)

If $\Gamma \vdash P : P' : P_p$, then $\llbracket \Gamma \vdash P : P' \rrbracket \eta \in \llbracket \Gamma \vdash P : P_p \rrbracket \eta$ for all $\eta \models \Gamma \sigma^* \sigma_p$.

**Proof.** Induction on the derivation of $\Gamma \vdash P : P'$, using soundness of type assignment for datatype Constructors and programs (Theorems 6.5 and 6.14).

6.41 **Lemma.** (Soundness of $\beta$-reduction for prop-constructors)

Suppose $P \beta P'$, $\Gamma \vdash P : P'$ and $\Gamma \vdash P' : P''$.

Then $\llbracket \Gamma \vdash P : P' \rrbracket \eta = \llbracket \Gamma \vdash P' : P'' \rrbracket \eta$ for all $\eta \models \Gamma \sigma^* \sigma_p$.

**Proof.** Induction on the structure of $P$. Datatype-constructors, programs and propkinds can be subterms of prop-constructors, so soundness of $\beta$-reduction for these expressions is needed (lemmas 6.6, 6.15 and 6.34).

As usual, for the case that $M$ is the Redex we use the substitution lemma given below.

6.42 **Lemma.** (Substitution in prop-constructors)

Suppose $\Gamma, y : B, \Gamma' \vdash P : P'$ and $\Gamma \vdash b : B$. Then

$$\llbracket \Gamma, \Gamma'[y := b] \vdash P[y := b] : P' \rrbracket \eta = \llbracket \Gamma, y : B, \Gamma' \vdash P : P' \rrbracket \eta[y := \llbracket \Gamma \vdash b : B \rrbracket \eta],$$

for all $\eta \models (\Gamma, \Gamma'[y := b]) \sigma^* \sigma_p$ and $\eta[y := \llbracket \Gamma \vdash b : B \rrbracket \eta] = (\Gamma, y : B, \Gamma') \sigma^* \sigma_p$.

**Proof.** Induction on the structure of $P$, using the substitution lemmas for the datatype constructors, programs and propkinds (lemmas 6.7, 6.16 and 6.35).

6.43 **Theorem.** (Soundness of $\beta$-conversion for prop-constructors)

Suppose $P \beta P'$, $\Gamma \vdash P : P'$ and $\Gamma \vdash P' : P''$.

Then $\llbracket \Gamma \vdash P : P' \rrbracket \eta = \llbracket \Gamma \vdash P' : P'' \rrbracket \eta$ for all $\eta \models \Gamma \sigma^* \sigma_p$.

**Proof.** This follows from soundness of $\beta$-reduction for prop-constructors, $SR_\beta$ and $CR_\beta$.
The semantics of proofs

6.44 DEFINITION. Let \( \Gamma \) be a \( \lambda \omega_L \)-context. An environment \( \eta \) satisfies \( \Gamma \) written \( \eta \models \Gamma \) if \( \eta \models \Gamma^\xi \cdot \xi^\tau \) and \( \eta(x) \in [\Gamma \vdash P : \ast_P] \eta \) for all \( x : P \) in \( \Gamma^\tau \).

So \( \eta \models \Gamma \) iff

- \( \eta(x) \in \text{Kind} \mathcal{K} \) for all \( x : \mathcal{K} \) in \( \Gamma^\xi \), and
- \( \eta(x) \in \text{Dom}_{[I \vdash \sigma \ast \cdot \ast]} \) for all \( x : \sigma \) in \( \Gamma^\tau \), and
- \( \eta(x) \in \{ \Gamma \vdash P : \ast_P \} \eta \) for all \( x : P \) in \( \Gamma^\xi \), and
- \( \eta(x) \in \{ [\Gamma \vdash P : \ast_P] \eta \) for all \( x : P \) in \( \Gamma^\tau \).

Because \( \{ \Gamma \vdash P : \ast_P \} \eta \in \{ 0, 1 \} \), \( \eta(x) \in \{ \Gamma \vdash P : \ast_P \} \eta \) is only possible if \( \{ \Gamma \vdash P : \ast_P \} \eta \) is a.

6.45 DEFINITION (Semantics of proofs)

For \( \lambda \omega_L \)-proofs \( p \) we define \( [\Gamma \vdash p : P] \eta \) for all \( \Gamma \vdash p : P \) and \( \eta \models \Gamma \) as the element of 1.

6.46 THEOREM (Soundness of type assignment for proofs)

If \( \Gamma \vdash p : P \) then \( [\Gamma \vdash p : P] \eta \in \{ [\Gamma \vdash P : \ast_P] \eta \) for all \( \eta \models \Gamma \) iff \( \{ [\Gamma \vdash P : \ast_P] \eta \).

PROOF We prove that, for proofs \( p \),

if \( \Gamma \vdash p : P \) then \( [\Gamma \vdash p : P] \eta \) is only possible if \( [\Gamma \vdash p : P] \eta \) is a.

by induction on the derivation of \( \Gamma \vdash p : P \), using soundness of type assignment for datatypes, programs and procedure constructors (theorems 6.5, 6.14 and 6.40).

As for the proof-irrelevance model for \( \lambda \omega_p \), it follows immediately from soundness of type assignment that:

6.47 COROLLARY \( P \) is not provable in context \( \Gamma \) if \( \{ [\Gamma \vdash P : \ast_P] \eta \) is not 0 for some \( \eta \models \Gamma \).

This can be used to prove consistency (of contexts) in \( \lambda \omega_L \), as for instance in corollary 6.49.

6.48 EXAMPLE. As an example of the interpretation of a \( \lambda \omega_L \)-procedure constructor, we consider Leibniz' equality, which was defined in definition 3.21 by

\[
=_{L} = \lambda \alpha : \sigma, \lambda \tau, y : \alpha \to \ast \gamma, (P \alpha) \to (P y)
\]

\[
\Pi \alpha : \sigma \to \alpha \to \ast \gamma
\]

This will turn out to be interpreted as equality in the \( \lambda \omega_p \)-model.

Suppose \( M \) and \( N \) are programs with \( \Gamma \vdash M, N \) \( \sigma \) and \( \eta \models \Gamma \). Then

\[
\{ [\Gamma \vdash M =_{L} N : \ast_p] \eta \} = \{ [\Gamma \vdash \forall \sigma \to \ast_p, (P M) \to (P N) : \ast_p] \eta \} = \{ \Gamma, \text{P} : \sigma \to \ast_p, (P M) \to (P N) : \ast_p] \eta \} = \{ \xi \in \text{Dom}\{ \Gamma \vdash \sigma \to \ast \cdot \ast \}, \to \{ 0, 1 \} \}
\]

\[
\xi \in \text{Dom}\{ \Gamma \vdash \sigma \to \ast \cdot \ast \}, \to \{ 0, 1 \}
\]
For $\xi \in \text{Dom}(\Gamma \vdash \sigma, * \eta) \rightarrow \{0, 1\}$ it follows by the definition of $[ ]$ that
\[
\Gamma, P : \sigma \vdash *_p \Gamma (P M) \Rightarrow (P N) : *_p \eta[P := \xi]
\]
\[
\text{because } [P M] \Rightarrow (P N) = [P M] = [P N]
\]
and that
\[
\Gamma, P : \sigma \vdash *_p \Gamma (P M) \Rightarrow (P N) : *_p \eta[P := \xi]
\]
\[
\text{because } [P M] = [P M] \Rightarrow (P N) = [P M] = [P N]
\]
So for $\Gamma \vdash M =_\sigma N : *_p \eta$ we get:
\[
\Gamma \vdash M =_\sigma N : *_p \eta
\]
\[
\Gamma \vdash \forall P : \sigma \rightarrow *_p \Gamma (P M) \Rightarrow (P N) : *_p \eta
\]
\[
\xi \in \text{Dom}(\Gamma \vdash \sigma, * \eta) \rightarrow \{0, 1\}
\]
This can be simplified further if we distinguish two possibilities for $[\Gamma \vdash M : \sigma] \eta$ and $[\Gamma \vdash N : \sigma] \eta$:

(i) Suppose $[\Gamma \vdash M : \sigma] \eta = [\Gamma \vdash N : \sigma] \eta$

Then $\xi([\Gamma \vdash M : \sigma] \eta) = \xi([\Gamma \vdash N : \sigma] \eta)$ for all functions $\xi$. Since $0 \Rightarrow 0 = 1$ and $1 \Rightarrow 1 = 1$, this means that $\xi([\Gamma \vdash M : \sigma] \eta) \Rightarrow \xi([\Gamma \vdash N : \sigma] \eta) = 1$ for all $\xi \in \text{Dom}(\Gamma \vdash \sigma, * \eta) \rightarrow \{0, 1\}$.

(ii) Suppose $[\Gamma \vdash M : \sigma] \eta \neq [\Gamma \vdash N : \sigma] \eta$

Then there is a function $\xi \in \text{Dom}(\Gamma \vdash \sigma, * \eta) \rightarrow \{0, 1\}$ such that $\xi([\Gamma \vdash M : \sigma] \eta) = 1$ and $\xi([\Gamma \vdash N : \sigma] \eta) = 0$. Then $\xi([\Gamma \vdash M : \sigma] \eta) \Rightarrow \xi([\Gamma \vdash N : \sigma] \eta) = 0$ for this function $\xi$.

So
\[
[\Gamma \vdash M =_\sigma N : *_p \eta]
\]
\[
\xi \in \text{Dom}(\Gamma \vdash \sigma, * \eta) \rightarrow \{0, 1\}
\]
\[
= \left\{ \begin{array}{ll}
1 & \text{if } [\Gamma \vdash M : \sigma] \eta = [\Gamma \vdash N : \sigma] \eta \text{ (by (i))} \\
0 & \text{if } [\Gamma \vdash M : \sigma] \eta \neq [\Gamma \vdash N : \sigma] \eta \text{ (by (ii))}
\end{array} \right.
\]

This means that $[\Gamma \vdash N =_p M : *_p \eta] = 1 \iff [\Gamma \vdash N : \sigma] \eta = [\Gamma \vdash M : \sigma] \eta$ - the interpretation of Leibniz' equal of programs is 1 iff their interpretations in the $\lambda\omega_L$-model are equal - and that
\[
\begin{array}{ll}
[ =_L \Pi \alpha * * \alpha \rightarrow \alpha * \eta = \lambda \alpha \in K_{\omega L}. \lambda X, Y \in \text{Dom} \alpha \{ & 1, \text{if } X = Y \\
& 0, \text{if } X \neq Y
\end{array}
\]
So Leibniz' equality, as defined in definition 3.21, is interpreted as equality in the $\lambda\omega_2$-submodel, irrespective of the $\lambda\omega_2$-model we choose. This means that axioms for Leibniz' equality of programs can be safely added on the basis of equalities that hold in the $\lambda\omega_2$-model. For example, because equality of programs in any $\lambda\omega_2$-environment model is extensional, it can be assumed that Leibniz' equality is extensional. This is stated in the corollary below.

6.49 Corollary (Consistency of AXIOM - classical logic and extensionality in $\lambda\omega_2$).
False is not provable in a context containing only axioms from AXIOM.

Proof. $\llbracket \text{False} : \ast_n \rrbracket = 0$, so by corollary 6.47 we only have to show that there is an environment $\eta$ that satisfies this context. The only possible value that an environment can assign to the variables classic, $\text{EXT}$ and $\text{EXT}_\eta$ is the element of 1. That this environment satisfies the context above follows from the fact that all the propositions assumed in this context are interpreted as 1. \qed
Chapter 7

Simple Extensions

This chapter treats the semantics of the systems introduced in chapter 4, i.e. of the programming language $\lambda \omega^+$ and of the associated programming logic $\lambda \omega^+$. It builds on the model definitions given in the previous chapter for the programming language $\lambda \omega$ and the programming logic $\lambda \omega_\Sigma$. These models will be extended to provide interpretations for the $+, \times$ and $\Sigma$-types and their inhabitants.

As in the previous chapter, only the systems without the definition mechanism have to be considered. Any model for a PTSs with $+, \times$ and $\Sigma$ also provides a model for the corresponding DPTSs with $+, \times$ and $\Sigma$, because, by theorem 4.20 - elimination of definitions for DPTSs with $+, \times$, and $\Sigma$, a term in a system with definitions can be interpreted by first eliminating all definitions, and then interpreting the resulting term in the system without definitions.

The structure of this chapter closely follows that of chapter 6.

In section 7.1 we give a general model definition for $\lambda \omega^+$, which is an extension of the one for $\lambda \omega$, given in the section 6.1. It is not difficult to incorporate the datatype-constructors $+$ and $\times$ in the general model definition for $\lambda \omega$. The datatype-constructor $\Sigma$ turns out to be slightly more complicated.

In section 7.2 it is shown that the PER-model for $\lambda \omega^+$, which is an extension of the PER-model for $\lambda \omega$, given in section 6.2, is an instantiation of this general model definition.

In section 7.3 it is shown how the proof-irrelevance model for $\lambda \omega_\Sigma$ given in section 6.4 can be extended to provide a model for $\lambda \omega^+_\Sigma$. This model proves consistency of $\lambda \omega^+_\Sigma$ and consistency of the axioms in $\text{AXIOM}^+$. 

7.1 General Model Definition for $\lambda \omega^+_\Sigma$

The general model definition for $\lambda \omega_\Sigma$ given in section 6.1 will be extended to provide a general model definition for $\lambda \omega^+_\Sigma$. As in $\lambda \omega_\Sigma$, in $\lambda \omega^+_\Sigma$ we can first consider the semantics of kinds, then the semantics of the datatype-constructors, and then finally the semantics of the programs.

To obtain a $\lambda \omega^+_\Sigma$-model from a given $\lambda \omega_\Sigma$-model, it has to be extended to provide interpretations for the new datatypes and for the new programs. In the general model definition for $\lambda \omega_\Sigma$ the functions $\lfloor \cdot \rfloor$ and $\Pi$ give the meaning of $\Sigma$- and $\Pi$-datatypes. We now also need functions $\lfloor + \rfloor$, $\lfloor \times \rfloor$ and $\lfloor \Sigma \rfloor$ to give the meaning of $+$, $\times$- and $\Sigma$-datatypes. In the general model definition for $\lambda \omega_\Sigma$ the domain equations for $\Sigma$- and $\Pi$-datatypes provide
the interpretation for the associated program constructions. We now have to include domain equations for the +, \times and \Sigma-datatype constructors.

The semantics of the kinds and datatype-constructors

As far as the kinds are concerned, there is no difference between \( \omega_0 \) and \( \omega_1 \). So, as for the \( \omega_0 \)-model, a family of sets \( \text{Kind} = \{ \text{Kind}_{\mathcal{K}} \mid \mathcal{K} \text{ is a kind} \} \) is needed.

The new datatype-constructors are given by the definition of Cons in definition 4.28 (We will not bother with the subscript \( * \) of the empty product \( \Pi(*) \) and the empty sum \( \Sigma(*) \) here.) Functions \( +, \times \) and \( \Sigma \) are needed to give the meaning of the new datatyp-constructors. The function \( \Sigma \) will have the same type as \( \Pi \), i.e.

\[
\Sigma \in \prod_{\mathcal{K} \in \mathcal{C}} (\text{Kind}_{\mathcal{K}} \rightarrow \text{Kind}_{\mathcal{K}}^*) \rightarrow \text{Kind}_{\mathcal{K}}^* .
\]

Using \( \Sigma \), the meaning of a datatype \( (\Sigma: \mathcal{K} \rightarrow \sigma) \) in \( \text{Kind}_{\mathcal{K}} \) is defined in terms of the function in \( \text{Kind}_{\mathcal{K}} \rightarrow \text{Kind}_{\mathcal{K}} \) that maps all possible interpretations of \( \sigma \) to the resulting meaning of \( \sigma \).

The meanings of datatypes \( \Pi(l_1 \sigma_1, \ldots, l_n \sigma_n) \) and \( \Sigma(l_1 \sigma_1, \ldots, l_n \sigma_n) \) in \( \text{Kind}_{\mathcal{K}} \) are defined in terms of the function in \( \{l_1, \ldots, l_n\} \rightarrow \text{Kind}_{\mathcal{K}} \) that maps a label \( l_i \) to the meaning of \( \sigma_i \). For this functions \( \times \) and \( + \) are used, with

\[
\times, + \in \prod_{\mathcal{L} \sqcap \text{label}} (L \rightarrow \text{Kind}_{\mathcal{K}}^*) \rightarrow \text{Kind}_{\mathcal{K}}^* .
\]

This results in the following definition for an environment frame for the constructors:

7.1 DEFINITION. An environment frame for the datatype-constructors of \( \omega^+ \) is a 7-tuple 
\[
(\text{Kind}, \xi_{\text{Kind}}, \Pi, \Sigma, \times, +),
\]

where

- \( \text{Kind} = \{ \text{Kind}_{\mathcal{K}} \mid \mathcal{K} \text{ is a kind} \} \) is a family of sets, indexed by kinds
- \( \xi_{\text{Kind}} = \{ \xi_{\mathcal{K}, \mathcal{K}_1} \mid \mathcal{K}_1 \rightarrow \mathcal{K}_2 \text{ is a kind} \} \) is a family of bijections with \( \xi_{\mathcal{K}, \mathcal{K}_1} \in \text{Kind}_{\mathcal{K}_1} \rightarrow \text{Kind}_{\mathcal{K}_2} \), where the square brackets denote some subset of the function space.
- \( \Pi, \Sigma, \times, + \in \prod_{\mathcal{L} \sqcap \text{label}} (\text{Kind}_{\mathcal{K}} \rightarrow \text{Kind}_{\mathcal{K}}) \rightarrow \text{Kind}_{\mathcal{K}}^* \)
- \( \Pi, \Sigma, \times, + \) are used, with

We will not distinguish the term \( (l_1, \ldots, l_n) : \text{label} \) and the set \( \{l_1, \ldots, l_n\} \subseteq \mathcal{L} \). Beware that \( \mathcal{L} : \text{label} \) is not equivalent with \( \mathcal{L} \subseteq \mathcal{L} \), because if \( \mathcal{L} \subseteq \mathcal{L} \) is an infinite set, then we do not have \( \mathcal{L} : \text{label} \). The fact that labelled cartesian products and disjoint sums are finite products and sums may be needed for certain model constructions.

Defining the interpretation of the new datatype-constructors using \( +, \times \) and \( \Sigma \) is straightforward:
7.1 GENERAL MODEL DEFINITION FOR $\lambda \omega^+_5$

7.2 DEFINITION (semantics of $\lambda \omega^+_5$-datatype-constructors).
For datatype-constructors $\sigma$ we define $[\Gamma \vdash \sigma : \mathcal{K}] \eta$ for all $\Gamma \vdash \sigma : \mathcal{K}$ and $\eta \models \Gamma^{\mathcal{K}}$ by induction on the derivation of $\Gamma \vdash \sigma : \mathcal{K}$ as in definition 6.3, extended with the following clauses:

$$[\Gamma \vdash \Pi(l_1 : \sigma_1, \ldots, l_n : \sigma_n) : *] \eta \equiv \prod_{(l_1 : \sigma_1) \in \{l_1, \ldots, l_n\}} [\Gamma \vdash \sigma_1 : *] \eta$$

$$[\Gamma \vdash \Sigma(l_1 : \sigma_1, \ldots, l_n : \sigma_n) : *] \eta \equiv \sum_{(l_1 : \sigma_1) \in \{l_1, \ldots, l_n\}} [\Gamma \vdash \sigma_1 : *] \eta$$

$$[\Gamma \vdash (\Sigma_{i \in \mathcal{K}.} \alpha_i : \sigma) : *] \eta \equiv \sum_{\alpha \in \text{Kind}_{\mathcal{K}}} (\alpha \in \text{Kind}_{\mathcal{K}}) \cap [\Gamma, \alpha : \mathcal{K} \vdash \sigma : *] \eta[\alpha := a]$$

For $\prod$ and $\sum$ the same notational conventions are used as for their syntactical counterparts. For instance, we write $S_1 \times S_2$ for $\prod_{i \in \{1, 2\}} (l \in \{1, 2\}, S_i)$. The indices $L$ and $K$ of $\prod_{L}^{K}$ and $\prod_{K}$ will usually be omitted.

As in chapter 6, the meaning of some datatype-constructor may be undefined for a given frame, for exactly the same reason, namely that the range of the $\Phi_{\mathcal{K}_1} \rightarrow \mathcal{K}_2$ may not be large enough. Analogous to definition 6.4 we define:

7.3 DEFINITION. An environment model for the datatype-constructors of $\lambda \omega^+_5$ is an environment frame for the datatype-constructors of $\lambda \omega^+_5$ for which $[\Gamma \vdash \sigma : \mathcal{K}] \eta$ is defined for all $\Gamma \vdash \sigma : \mathcal{K}$ and $\eta \models \Gamma^{\mathcal{K}}$.

The properties proved in chapter 6 for arbitrary environment models for the datatype-constructors of $\lambda \omega^+_5$ also hold for arbitrary environment models for the datatype-constructors of $\lambda \omega^+_5$.

7.4 LEMMA (Soundness of type assignment for datatype-constructors).
If $\Gamma \vdash \sigma : \mathcal{K}$ then $[\Gamma \vdash \sigma : \mathcal{K}] \eta \in \text{Kind}_{\mathcal{K}}$ for all $\eta \models \Gamma^{\mathcal{K}}$.

7.5 LEMMA (Soundness of $\beta$-conversion for datatype-constructors).
Suppose $\Gamma \vdash \sigma : \mathcal{K}$, $\Gamma \vdash \sigma' : \mathcal{K}$, and $\sigma \equiv_\beta \sigma'$.

Then $[\Gamma \vdash \sigma : \mathcal{K}] \eta = [\Gamma \vdash \sigma' : \mathcal{K}] \eta$ for all $\eta \models \Gamma^{\mathcal{K}}$.

These lemmas can be proved in exactly the same way as in chapter 6.

The semantics of programs

Upgrading the general model definition from $\lambda \omega^+_5$ to $\lambda \omega^+_5$ is more work for the programs than it is for the datatype-constructors. The general model definition for $\lambda \omega^+_5$ includes domain equations for $\cdot$, and $\Pi$-types:

$$\text{Dom}(\Gamma \vdash \sigma : *] \eta \equiv [\text{Dom}(\Gamma \vdash \sigma : *] \eta \rightarrow \text{Dom}(\Gamma \vdash \sigma : *] \eta)$$

$$\text{Dom}(\Gamma \vdash \Pi(l_1 : \sigma_1, \ldots, l_n : \sigma_n) : *] \eta \equiv \prod_{(l_1 : \sigma_1) \in \{l_1, \ldots, l_n\}} [\text{Dom}(\Gamma \vdash \sigma_1 : *] \eta[\alpha := a])$$

with the square brackets denoting some subset of the function space and the generalised Cartesian product. Now for $\lambda \omega^+_5$ domain equations have to be added for the $\cdot$, $\times$- and
\[ \sum_{l_i \in \{l_i \mid l_i \neq 0\}} \text{Dom} \{ \sum_{i \in \{l_i \mid l_i \neq 0\}} \text{Dom} \{ l_i \cdot \cdot \cdot \} \} = \bigcup_{l_i \in \{l_i \mid l_i \neq 0\}} \{ (l_i, x) \mid x \in \text{Dom} \{ l_i \cdot \cdot \cdot \} \} \]

Note that the whole cartesian product and discriminated union are used in the domain equations for product and sum types. This in contrast to the domain equations for function type and polymorphic types, where we are content with subsets of the function space and generalised product. This is because some functions in \( \text{Dom}_a \rightarrow \text{Dom}_b \) or \( \prod_{a \in \text{Kind}_b} \text{Dom}_F(a) \) may not be \( \lambda \)-definable, whereas all tuples in \( \prod_{a \in \{l_i \mid l_i \neq 0\}} \text{Dom}_F(a) \) and all injections into \( \bigcup_{l_i \in \{l_i \mid l_i \neq 0\}} \text{Dom}_F(a) \) are \( \lambda \)-definable (or rather, \( \lambda \)- and \( \lambda \)-indefinable).

Given the interpretation of data types in Definition 7.2, the domain equations for \( + \) and \( \times \)-types are

\[ \text{Dom} \{ \square \} \cong \prod_{i \in \mathcal{L}} \text{Dom}_{l_i} \text{ and } \text{Dom} \{ \square \} \cong \sum_{i \in \mathcal{L}} \text{Dom}_{l_i} \]

for all \( \mathcal{L} \subseteq \mathcal{L} \) and \( F \in \mathcal{L} \rightarrow \text{Kind}_b \). For the binary products and sums we get

\[ \text{Dom} \{ r \cdot \sigma \cdot \tau \cdot \cdot \cdot \} \cong \text{Dom} \{ l \cdot \sigma \cdot \tau \cdot \cdot \cdot \} \cong \text{Dom} \{ l \cdot \sigma \cdot \tau \cdot \cdot \cdot \} \cong \text{Dom} \{ l \cdot \sigma \cdot \tau \cdot \cdot \cdot \} \cong \text{Dom} \{ l \cdot \sigma \cdot \tau \cdot \cdot \cdot \} \]

where in the right hand sides \( \times \) and \( + \) are the set-theoretic cartesian product and discriminated union, i.e

\[ \text{Dom} \{ l \cdot \sigma \cdot \tau \cdot \cdot \cdot \} \cup \text{Dom} \{ l \cdot \sigma \cdot \tau \cdot \cdot \cdot \} = \{(1, x) \mid x \in \text{Dom} \{ l \cdot \sigma \cdot \tau \cdot \cdot \cdot \} \} \cup \{(2, x) \mid x \in \text{Dom} \{ l \cdot \sigma \cdot \tau \cdot \cdot \cdot \} \}

For the empty product \( \prod() \) and the empty sum \( \sum() \) we get that \( \text{Dom} \{ \prod() \} \) is isomorphic to a singleton set and \( \text{Dom} \{ \sum() \} \) is isomorphic to the empty set.

For the \( \Sigma \)-types the situation is more complicated. An obvious choice for the domain equation for a \( \Sigma \)-type is one similar to the one for a \( \times \)-type:

\[ \text{Dom} \{ \sum_{\alpha \in \text{Kind}_b} \{ \alpha \} \} \cong \sum_{\alpha \in \text{Kind}_b} \text{Dom} \{ \alpha \cdot \cdot \cdot \} \]

The associated isomorphism can indeed be used to interpret the program-constructions for \( \Sigma \)-types. With the isomorphism from right to left the meaning of \( \{ \text{in}_{\text{Kind}_b} , \cdot \cdot \cdot \} \) can be defined in terms of the meanings of \( \tau \) and \( N \). With the isomorphism from left to right the meaning of \( \nabla f \) (\( \Sigma : \text{Kind}_b \cdot \cdot \cdot \rightarrow \rho \)) can be defined in terms of the meaning of \( f : (\Pi \alpha \cdot \cdot \cdot \rightarrow \rho) \). However,
the domain equation above requires more than is strictly necessary. Only an interpretation for a weak $\Sigma$-type is needed, and (i) provides the interpretation of the strong $\Sigma$-type (discussed in section 4.1.3). This is because with (i) inhabitants of a $\Sigma$-type are interpreted as pairs consisting of a datatype-constructor and a program, and the associated isomorphism can be used to define projections $\pi_1$ and $\pi_2$ such that

\[ \pi_1([\Gamma \vdash (i_{\Sigma:K} \sigma \tau N): (\Sigma \alpha:K. \sigma)]\eta) = [\Gamma \vdash \tau : \tau, 2] \eta \]

\[ \pi_2([\Gamma \vdash (i_{\Sigma:K} \sigma \tau N): (\Sigma \alpha:K. \sigma)]\eta) = [\Gamma \vdash N : \tau[\alpha := \tau]]\eta \]

Indeed, in PER-model equation (i) cannot be solved, as can be shown by considering the cardinality of the two sides. Take $K \equiv \Sigma$. Then the left hand side of (i) is a set of equivalence classes in a partial equivalence relation on $N$, and the right hand side is a set of pairs consisting of a partial equivalence relation on $N$ and an equivalence class.

Later, in chapter 8, a model will be given that does satisfy (i) (but in which the $\text{Dom}_\alpha$ are cpos instead of sets).

We will give another domain equation for $\Sigma$-types. This domain equation does not require that $\text{Dom}_{\Sigma:K} \text{F}_a$ is isomorphic to $\sum_a \text{Dom}_{\text{F}(a)}$, but only requires that it is isomorphic to $\sum_a \text{Dom}_{\text{F}(a)}$ modulo some equivalence relation $\approx$. The following example explains the idea behind this.

7.6 EXAMPLE. Suppose $(i_{\Sigma:K} \sigma \tau N)$ and $(i_{\Sigma:K} \sigma \tau' N')$ are of type $(\Sigma \alpha:K. \sigma)$, and suppose for all functions $f : (\Pi \sigma:K. \sigma \rightarrow \rho)$ and all environments $\eta$ that satisfy the context

\[ [\Gamma \vdash f \tau N : \rho] \eta = [\Gamma \vdash f \tau' N' : \rho] \eta \]

Then the model does not have to distinguish $(i_{\Sigma:K} \sigma \tau N)$ and $(i_{\Sigma:K} \sigma \tau' N')$, because there is no function $\nabla f : (\Sigma \alpha:K. \sigma) \rightarrow \rho$ that can distinguish them. We will define a relation $\approx$ on $\sum_a \text{Dom}_{\text{F}(a)}$ so that the pairs $([\tau], [N])$ and $([\tau'], [N'])$ are in this relation. \hfill \Box

To define $\approx$ the following notation is used.

7.7 DEFINITION ($\text{App}(\_, \_)$)

For $f \in \text{Dom}_{\Pi F}$ and $a \in \text{Kind}_K$ we write $\text{App}(f, a)$ for $\Phi_F(f)(a)$.

For $f \in \text{Dom}_{\alpha} \text{Dom}_{\text{F}(a)}$ we write $\text{App}(f, \xi)$ for $\Phi_{\text{F}(a)}(f)(\xi)$.

So for example $[\Gamma \vdash f \tau N : \rho] \eta = \text{App}(\text{App}([\Gamma], [\tau]), [N])$, for $[\_]$ as defined in definition 6 32

7.8 DEFINITION ($\approx$)

Let $F \in \text{Kind}_K \rightarrow \text{Kind}_{\ast}$. The relation $\approx$ on $\sum_a \text{Kind}_K \text{Dom}_{\text{F}(a)}$ is then defined as follows:

\[ (a, \chi) \approx (a', \chi') \text{ iff } \text{App}(f, a), \chi) = \text{App}(f, a'), \chi') \]

for all $b \in \text{Kind}_{\ast}$ and all $f \in \text{Dom}_{\Pi (\lambda a \in \text{Kind}_K. F(a)) (b)}$. \hfill \Box
So for the datatypes $\tau, \tau', \sigma$, and the programs $N : \sigma[\alpha := \tau]$ and $N' : \sigma[\alpha := \tau']$ in example 7.6 we have $([[\tau]], [[N]]) \approx ([[\tau']], [[N']])$

As the domain equation for $\Sigma$-types we now take

$$\text{Dom} \left[ \Sigma \right]_{\Phi} \cong \left( \sum_{\alpha \in \text{Kind}_\Sigma} \text{Dom}_{E(\alpha)} \right) / \approx$$

The associated isomorphism can be used to interpret the program-constructions for $\Sigma$-types. With the isomorphism $\Phi^{-1}$ from right to left the meaning of $(\in \Sigma_\alpha, K, \sigma \to N)$ can be defined in terms of the meanings of $\tau$ and $N$, namely as $\Phi^{-1}$ applied to the equivalence class containing $([[\tau]], [[N]])$. With the isomorphism $\Phi$ from left to right the meaning of $\forall f : (\Sigma_\alpha, K, \sigma) \to \rho$ can be defined in terms of the meaning of $f : (\Pi \alpha, K, \sigma \to \rho)$, namely as the function which maps an element of $\xi \in \text{Dom} \left[ \Sigma \right]_{\Phi}$ to the result of applying $[[f]]$ to $\alpha$ and $\chi$, where $(\alpha, \chi)$ is any element in the equivalence class $\Phi(\xi)$. The definition of $\approx$ guarantees that it does not matter which $(\alpha, \chi) \in \Phi(\xi)$ we choose.

With the domain equations for $\Sigma$-types and $\Sigma$-program-frames, the $\lambda \omega^\Sigma$-environment frames are now defined as follows.

7.9 Definition ($\lambda \omega^\Sigma$ environment frame).

An environment frame for $\lambda \omega^\Sigma$ is a tuple $(\text{KIND}, \text{Dom}, \Phi^-, \Phi^+, \Phi^\Sigma, \Phi^\Pi, \Phi^\times, \Phi^\vdash)$, where

- $\text{KIND} = (\text{Kind}, \Phi_{\text{Kind}}, \rightarrow, \Pi, \Sigma, \times, +)$ is an environment model for the $\lambda \omega^\Sigma$-constructors.
- $\text{Dom} = \{ \text{Dom}_a | a \in \text{Kind}_\Sigma \}$ is a family of sets.
- $\Phi^-$ and $\Phi^\Pi$ are as in definition 6.9, and $\Phi^\Sigma = \{ \Phi^\Sigma_F | \vdash F : \text{Kind}_\Sigma \to \text{Kind}_\Sigma \}$, $\Phi^\times = \{ \Phi^\times_F | \vdash F : \text{Kind}_\Sigma \times \text{Kind}_\Sigma \to \text{Kind}_\Sigma \}$, and $\Phi^+ = \{ \Phi^+_F | \vdash F : \text{Label} \to \text{Kind}_\Sigma \}$ are families of bijections with

\[
\begin{align*}
\Phi^-_F & \in \text{Dom} \left[ \Sigma \right]_{\Phi} 
\to (\sum_{\alpha \in \text{Kind}_\Sigma} \text{Dom}_{E(\alpha)}) / \approx \\
\Phi^\Sigma_F & \in \text{Dom} \left[ \Sigma \right]_{\Phi} 
\to \Pi \sum_{\epsilon, \phi} \text{Dom}_{E(\epsilon)} \\
\Phi^\times_F & \in \text{Dom} \left[ \Sigma \right]_{\Phi} 
\to \sum_{\epsilon, \phi} \text{Dom}_{E(\epsilon)}
\end{align*}
\]

We now define the interpretation of the new program constructions in $\lambda \omega^\Sigma$ with respect to an arbitrary environment frame. This simply amounts to inserting the right isomorphisms in the right places, but some of the results look very unappetizing. In example 7.10 the interpretations of case and abtype are given, which are a lot easier to read than the interpretation of $\forall$ for $\Sigma$-types.

7.10 Definition (semantics of $\lambda \omega^\Sigma$-programs).

For a $\lambda \omega^\Sigma$-program $M$ with $\Gamma \vdash M : \sigma$, $\Gamma \vdash M : \sigma$ is defined for $\eta = \Gamma \vdash \cdot \cdot \cdot$ by induction on the derivation of $\Gamma \vdash M : \sigma$, as in definition 6.32, extended with the clauses given below.
For $\lambda$-types.

Let $\sigma = \Pi(l_1, \ldots, l_n) \cdot \tau$ and $F = (\mathbb{A}_i \in \{l_1, \ldots, l_n\} \cdot [\Gamma \vdash \sigma : \tau] \eta)$. So $\mathbb{X} F = [\Gamma \vdash \sigma : \tau] \eta$. Then we define

$$
[\Gamma \vdash (l_1 \rightarrow M_1, \ldots, l_n \rightarrow M_n) : \sigma] \eta \equiv \Phi^{-1}_1 (\mathbb{A}_i \in \{l_1, \ldots, l_n\} \cdot [\Gamma \vdash M_i : \sigma] \eta)
$$

$$
[\Gamma \vdash M : \sigma] \eta \equiv (\Phi_1 \mid [\Gamma \vdash M : \sigma] \eta) \cdot_1
$$

where $\Phi_1 = \Phi^\lambda_F \in \text{Dom}_{[\Gamma \vdash \sigma : \tau]} \longrightarrow \prod_i \text{Dom}_{F(i)}$.

For $\tau$-types.

Let $\sigma = \Sigma(l_1, \ldots, l_n) \cdot \tau$ and $F = (\mathbb{A}_i \in \{l_1, \ldots, l_n\} \cdot [\Gamma \vdash \sigma : \tau] \eta)$. So $\mathbb{X} G = [\Gamma \vdash \sigma : \tau] \eta$. Then we define

$$
[\Gamma \vdash \lambda \xi : \sigma \rightarrow \rho] \eta \equiv \Phi^{-1}_{2} (\lambda \xi \in \text{Dom}_{[\Gamma \vdash \sigma : \tau]} \eta).
$$

For $\Sigma$-types.

Let $F = (\mathbb{A}_a \in \text{Kind}_{\mathbb{K}} \cdot [\Gamma, \alpha : N : \eta[\alpha := a])$, $G = (\mathbb{A}_e \in \text{Kind}_{\mathbb{E}} \cdot F(a) \rightarrow R)$ and $R = [\Gamma \vdash \rho : \tau] \eta)$. So $\mathbb{X} F = [\Gamma \vdash (\Sigma \mathbb{A} : \mathbb{K} \cdot \tau) : \tau] \eta$, and $\mathbb{X} G = [\Gamma \vdash (\Pi \mathbb{A} : \mathbb{K} \cdot \rho) : \tau] \eta$. Then we define

$$
[\Gamma \vdash \lambda \alpha \cdot N \cdot (\Sigma \alpha : \mathbb{K} \cdot \sigma)] \eta \equiv \Phi^{-1}_1 (\lambda \alpha \cdot \mathbb{E}[\eta[\alpha := a])
$$

$$
[\Gamma \vdash \forall f \cdot (\Sigma \alpha : \mathbb{K} \cdot \sigma) \rightarrow \rho] \eta \equiv \Phi^{-1}_{2} (\lambda \xi \in \text{Dom}_{[\Gamma \vdash \sigma : \tau]} \eta).
$$

The definition of $\approx$ guarantees that it does matter which $(n, x) \in \Phi_1(x)$ is chosen.
7.11 Example The interpretations of the case- and abtype-constructions are easier to read then the interpretation of \( \triangledown \) given above. Definition 7.10 gives the following interpretation for case:

\[
\begin{align*}
[I] & \vdash \text{ (case } N \text{ of in } 1 \ x \mapsto M_1 \mid \ldots \mid 2 \ y \mapsto M_n \text{ esac } 
\triangledown \eta \ 
= \ & \ [[I] \vdash \triangledown (\lambda x_1, \ldots, x_n. M)] \ N : \tau \eta \ 
= \ & \ [[I, x_1\sigma_i \mapsto M_i, x_2 \mapsto \lambda x_n. M_n] \ N : \tau \eta \ 
& \text{ by the definition of case} \ 
& \text{ by definition 7.10} \ 
\end{align*}
\]

where \((l_i, \chi_i) = \Phi^+_F([I] \vdash N : \Sigma(l_1, \ldots, l_n, \sigma_n) \eta) \in \sum_i \text{Dom}_{F_i}(t),\) with \(F = (\lambda \alpha \in Knd_{\Sigma}; [I, \alpha \mapsto K, \lambda \sigma \mapsto M, \rho \mapsto \eta[\alpha \mapsto a[x := \chi]])\)

As the interpretation of abtype we get

\[
\begin{align*}
[I] & \vdash \text{ (abtype } \alpha \mapsto K \text{ with } x: \sigma \text{ is } N \text{ in } M) \ 
\rho \eta \ 
= \ & \ [[I] \vdash \triangledown (\lambda x. K) : \lambda \sigma. M) \ N : \rho \eta \ 
= \ & \ [[I, \alpha. K, x: \sigma \mapsto M, \rho \mapsto \eta[\alpha \mapsto a[x := \chi]) \ 
& \text{ by the definition of abtype} \ 
& \text{ by definition 7.10} \ 
\end{align*}
\]

where \((\alpha, \chi)\) is any element of the \(\equiv\)-equivalence class \(\Phi^+_F([I] \vdash N : (\Sigma \alpha K) \eta)\), with \(F = (\lambda \alpha \in Knd_{\Sigma}; [I, \alpha \mapsto K, \lambda \sigma \mapsto M, \rho \mapsto \eta[\alpha \mapsto a[x := \chi])]\)

Analogous to definition 6.12 we define:

7.12 Definition A \(\lambda_\omega^+\)-environment model is a \(\lambda_\omega^+\)-environment frame for which \(\eta[I] \vdash M : \sigma \eta\) is defined for all \(\eta[I] \vdash M : \sigma \eta\).

If \(\lambda_\omega^\text{-frame}\) is not \(\lambda_\omega^+\)-model - i.e. the meaning of some program is not defined for the frame - then the reason is that the range of one of the bijections \(\Phi^+_\alpha\beta\) or \(\Phi^+_{\eta\beta}\) is too small. The reason cannot be that the range of a bijection \(\Phi^+_\alpha\beta\) or \(\Phi^+_{\eta\beta}\) is too small. This is because the ranges of these bijections are prescribed by the definition of an environment frame, whereas all subsets of \(\text{Dom}_a \longrightarrow \text{Dom}_b\) and \(\prod_a \text{Dom}_{F_i}(t)\) are allowed as the range of \(\Phi^+_\alpha\beta\) and \(\Phi^+_{\eta\beta}\)

The properties proved in chapter 6 for arbitrary environment models of \(\lambda_\omega\) also hold for arbitrary environment models of \(\lambda_\omega^+\), and they can be proved in exactly the same way as in chapter 6.

7.13 Lemma. Let \(\text{der}_1\) and \(\text{der}_2\) be derivations of \(\eta[I] \vdash M : \sigma \eta\) and \(\eta[I] \vdash M : \sigma' \eta\), respectively. Then

\[
\begin{align*}
[I] & \vdash M : \sigma \eta = [I] \vdash M : \sigma' \eta \ 
\end{align*}
\]

where the meanings are defined using \(\text{der}_1\) and \(\text{der}_2\) respectively.

7.14 Lemma (Soundness of type assignment for programs)

If \(\eta[I] \vdash M : \sigma\eta\) then \(\eta[I] \vdash M : \sigma\eta \in \text{Dom}_{\text{nor}}\) for all \(\eta[I] \vdash M : \sigma\eta\).

7.15 Lemma (Soundness of \(\beta\)-conversion for programs).

Suppose \(\eta[I] \vdash M : \sigma\eta, \eta[I] \vdash M' : \sigma'\eta\), then \(\eta[I] \vdash M' : \sigma' \eta\) for all \(\eta[I] \vdash M' : \sigma' \eta\).
7.2 PER-Model for $\lambda \omega_1^+$

In section 6.2 it was shown that the PER-model for $\lambda \omega$ is an instantiation of the general model definition for $\lambda \omega$. We will now give a PER-model for $\lambda \omega_1^+$ that extends the one given in section 6.2 and show that it is an instantiation of the general model definition for $\lambda \omega_1^+$.

Most accounts of PER-models in the literature only deal with $\rightarrow$- and $\Pi$-types. In [Gir72] interpretations for $\rightarrow$, $\times$- and $\Sigma$-types in the PER-model can be found. The interpretation of $\times$-types given below is different from the one given there. This is because we have $n$-ary product types and not just binary ones.

For the sake of simplicity we assume that all labels are of the form $l_n$ for some $n \in \mathbb{N}$. This gives us an easy way to associate a unique natural number with every label.

The interpretations $\rightarrow$ and $\Pi$ of $\rightarrow$ and $\Pi$ are defined as in definition 6.19. To interpret the $\rightarrow$-types we need a pairing function and projections.

7.16 Definition. The function $\langle \_ , \_ \rangle \in \mathbb{N}^2 \rightarrow \mathbb{N}$ is a recursive surjective pairing function and $\pi_1(\_ , \_ ) \in \mathbb{N} \rightarrow \mathbb{N}$ are the associated projection functions.

The datatype constructors $\rightarrow$, $\times$ and $\Sigma$ are now interpreted as the following functions:

7.17 Definition.

1. The functions $\times$, $+$ $\in \prod_{L \in \text{Lab}} (L \rightarrow \text{PER}) \rightarrow \text{PER}$ are defined by

$$\times F \triangleq \{(n, n') \in \mathbb{N}^2 \mid (n, n') \in F(l_j) \text{ for } l_j \in L\}$$

$$+ F \triangleq \{((n, n'), (n', n'')) \in \mathbb{N}^2 \mid (n, n') \in F(l_j) \text{ and } l_j \in L\}$$

for all $F \in L \rightarrow \text{PER}$.

2. The function $\Sigma \in \prod_{K \in \mathbb{K}}(\text{Kind}_K \rightarrow \text{PER}) \rightarrow \text{PER}$ is defined by

$$\Sigma F \triangleq \{(n, n') \in \mathbb{N}^2 \mid (n, n'), (n', n'') \in \bigcup_{a \in \text{Kind}_K} F(a) \text{ and } (f, n, f', n') \in R \}$$

for all $R \in \text{PER}$ and $(f, f') \in \prod (\lambda a \in \text{Kind}_K \rightarrow \text{PER})$.

In the definition of $\Sigma$ we can recognize the definition of $\approx$. If $(n, n) \in F(a)$, $(n', n') \in F(a')$, and $(f, f') \in \prod (\lambda a \in \text{Kind}_K \rightarrow \text{PER})$, and we define

$$[f] \triangleq [f]_F \mid \lambda a \in \text{Kind}_K \rightarrow \text{PER} \quad [n] \triangleq \mathord{[n]}_{F(a)}$$

then $(f \cdot n, f' \cdot n') \in R$ is equivalent with $\text{App}(\text{App}([f], a), [n]) = \text{App}(\text{App}([f'], a'), [n'])$. 


7.18 **Lemma.** \( \text{KIND}_{HEO} = (\text{Kind} \, \Phi_{K_{\text{HEO}}}, \prod, [\Sigma], [ \cdot ], [+] \) is an environment model for the \( \lambda^+_\omega \) datatype-constructors.

The sets \( \text{Dom}_K \) and the bijections \( \Phi^\pi_{\mathcal{J}} \) and \( \Phi^\Pi_F \) are defined as in definition 6.21. To complete the model bijections \( \Phi^\pi_F, \Phi^\pi_{\mathcal{J}} \) and \( \Phi^\Pi_F \) are needed:

7.19 **Definition.** For \( G \in L \rightarrow \text{PER} \), and \( F \in \text{Kind}_K \rightarrow \text{PER} \), the functions

\[
\Phi^G_{\mathcal{J}} \in \text{Dom} \, \left[ \prod \right]_G \rightarrow \Pi_{\in L} \text{Dom}_{C(i)}
\]

\[
\Phi^G_F \in \text{Dom} \, \left[ \Sigma \right]_F \rightarrow \Sigma_{\in \text{Dom}_{C(i)}}
\]

\[
\Phi^F_E \in \text{Dom} \, \left[ + \right]_E \rightarrow \left( \Sigma_{\in \text{Kind}_K} \text{Dom}_{F(a)} \right)/ \approx
\]

are defined by

\[
\Phi^G_{\mathcal{J}} \left[ \frac{a}{\left[ n \right]_G} \right] \triangleq \lambda j : G \left[ n \cdot j \right]_{C(i)}
\]

\[
\Phi^G_F \left[ \frac{\left( j, n \right)}{\left[ \cdot \right]_G} \right] \triangleq \left( j, \left[ n \right]_{C(i)} \right)
\]

\[
\Phi^F_E \left[ \frac{\left[ n \right]}{\left[ \cdot \right]_E} \right] \triangleq \left[ \left( a, \left[ n \right]_{F(a)} \right) \right]_E
\]

where \( a \) is an arbitrary element of \( \text{Kind}_K \).

Checking that these \( \Phi^G_{\mathcal{J}}, \Phi^G_F \) and \( \Phi^E_F \) are well-defined functions on equivalence classes is straightforward. For \( \Phi^G_{\mathcal{J}} \) - for which this is the most complicated - this amounts to proving

7.20 **Lemma.** Let \( F \in \text{Kind}_K \rightarrow \text{PER} \), \( (n, n') \in \sum F \) (so \( \left[ n \right]_F = \left[ n' \right]_F \)) and let \( a, a' \in \text{Kind}_K \). Then

\[
\left( a, \left[ n \right]_{F(a)} \right) \approx \left( a', \left[ n' \right]_{F(a')} \right)
\]

(and hence \( \left[ (a, \left[ n \right]_{F(a)}) \right]_E = \left[ (a', \left[ n' \right]_{F(a')} \right]_E \)).

**Proof.** To prove \( (a, \left[ n \right]_{F(a)}) \approx (a', \left[ n' \right]_{F(a')}) \) we have to prove that

\[
\text{App}(\text{App}(f, a), n) = \text{App}(\text{App}(f, a'), n'), \quad (i)
\]

where \( R \in \text{PER} \) and \( f \in \text{Dom} \, \left[ \Pi \right]_{\lambda a \in \text{Kind}_K} F(a) \rightarrow R \). This \( f \) is an equivalence class in the partial equivalence relation \( \Pi \, \left( \lambda a \in \text{Kind}_K \right) F(a) \rightarrow R \). Let \( m, n \in \text{Dom} \).

\[
f = \left[ m \right] \left[ \Pi \right]_{\lambda a \in \text{Kind}_K} F(a) \rightarrow R.
\]

Then by the definitions of \( \text{App}(\cdot, \cdot) \) (definition 7.7) and of \( \Phi^F \) and \( \Phi^G \) (definition 6.21) (i) is equivalent with

\[
\left[ m \, n \right]_R = \left[ n \, n' \right]_R,
\]

and by the definition of \( \sum \). This follows from \( (n, n') \in \sum F \).

To prove that we have an environment frame for \( \lambda^+_\omega \) we have to show:

7.21 **Lemma.** The functions \( \Phi^G_{\mathcal{J}}, \Phi^G_F \) and \( \Phi^F_E \) are bijections.

**Proof.** Easy.

Finally

7.22 **Lemma.** \( \text{KIND}_{HEO}, \, \text{Dom}, \, \Phi^-, \Phi^H, \Phi^\pi, \Phi^x, \Phi^+ \) is an environment model for \( \lambda^+_\omega \)

**Proof.** Proving that \( \left[ \Pi \right] \left( \Gamma \vdash M : \sigma \right) \) \( \eta \) is defined for all \( \Gamma \vdash M : \sigma \) and \( \eta \vdash \Gamma \left[ \sigma^* \right] \) is done exactly as in lemma 6.23.
7.3 The Programming Logic

In the previous chapter proof-irrelevance models were given for $\lambda_0$ and $\lambda_L$. In section 6.3 the general model definition for $\lambda$ was instantiated to produce a proof-irrelevance model for $\lambda_0$. In section 6.4 a proof-irrelevance model for the "logical" part of $\lambda_L$ was defined given an arbitrary model for the theorem language $\lambda_0$. Extending these models to deal with the additional primitives of $\lambda_0^+$ and $\lambda_L^+$ is very easy, and will therefore not be treated in much detail.

7.3.1 Proof-irrelevance model for $\lambda_0^+$

The proof-irrelevance model for $\lambda_0$ defined in section 6.3 can be extended to a model for $\lambda_0^+$. The new prop-constructors $\forall$, $\land$ and $\exists$ are given their usual truth-table interpretations:

7.23 Definition. The functions $\bigwedge, \bigvee \in \prod_{L \in \mathbb{L}} (L \to \{0, 1\}) \to \{0, 1\}$ and $\exists \in \prod_{K \in \mathbb{K}} (\text{Kind}_K \to \{0, 1\}) \to \{0, 1\}$ are defined by

\[
\bigwedge L F = \bigcap_{l \in L} F(l)
\]

\[
\bigvee L F = \bigcup_{l \in L} F(l)
\]

\[
\exists Y F = \bigcup_{X \in \text{Prop}_Y} F(X)
\]

where we take $\cap_{l \in \emptyset} F(l) = 1$.

However, the proof-irrelevance model for $\lambda_0^+$ cannot meet the general model definition given in section 7.1. The problem is that this general model definition is already too specific. In particular, it requires that $\text{Dom}_0[\bigvee]_0$ is isomorphic with the set-theoretical disjoint union of $\text{Dom}_0$ and $\text{Dom}_e$. So, if $\text{Dom}_0$ and $\text{Dom}_e$ are singletons, $\text{Dom}_0[\bigvee]_0$ has to be a two-element set. This is clearly not the case in the proof-irrelevance model, because there $\text{Dom}_0[\bigvee]_0$ is the singleton set 1 if $\text{Dom}_0$ and $\text{Dom}_e$ are both singletons.

7.3.2 Proof-irrelevance model for $\lambda_L^+$

Let

$\mathcal{M} = (\text{KIND}, \text{Dom}, \Phi^-, \Phi^+, \Phi^{\Sigma}, \Phi^X, \Phi^\text{Prop})$

be any environment model for $\lambda_L^+$. A model for $\lambda_L^+$ can be defined in which $\mathcal{M}$ is the submodel for $\lambda_L^+$. The only difference with the construction in section 6.4 are the interpretations for the new prop-constructors, which are of course interpreted as in the $\lambda_L^+$-model above.

The interpretation of the kinds, datatype-constructors and programs is given by $\mathcal{M}$, because by lemma 4.37 $\lambda_L^+$ has the same kinds, datatype-constructors and programs as $\lambda_L^+$. The interpretation of the prop-kinds is defined as for $\lambda_L^+$ (definition 6.33).

The new prop-constructors are given by the definition of $\text{PCons}$ in definition 4.34. The definition given in section 6.4 for the interpretation of prop-constructors has to be extended to deal with these new ones.
7.24 Definition (semantics of the new \( \lambda \omega^+_L \)-propconstructors)

For \( \lambda \omega_L \)-propconstructors \( P \), we define \( \Gamma \vdash P : \mathcal{P} \eta \) for all \( \Gamma \vdash P : \mathcal{P} \), and \( \eta \vdash \Gamma \cdot \star \cdot \mathcal{P} \eta \) by induction on the derivation of \( \Gamma \vdash P : \mathcal{P} \), as in definition 6.38, extended with the following clauses:

\[
\begin{align*}
\Gamma \vdash \forall (u_1 : P_1, \ldots, u_n : P_n) : \star_p \eta & \equiv \bigwedge_{i \in \{0, \ldots, n\}} \Gamma \vdash P_i : \star_p \eta \\
\Gamma \vdash \exists (u_1 : P_1, \ldots, u_n : P_n) : \star_p \eta & \equiv \bigvee_{i \in \{0, \ldots, n\}} \Gamma \vdash P_i : \star_p \eta \\
\Gamma \vdash (\exists x. A, P) : \star_p \eta & \equiv \bigwedge_{\xi} \Gamma[v : \xi] \vdash A \cdot P : \star_p \eta \end{align*}
\]

where \( \bigcap_{i \in \emptyset} P_i = 1 \), and \( A = \begin{cases} \text{Kind}_A & \text{if } \Gamma \vdash A : \square_s \\
\text{Dom}_{\{\tau, A, \star_s\}} \eta & \text{if } \Gamma \vdash A : \star_s \\
\Gamma \vdash A : \square_p \eta & \text{if } \Gamma \vdash A : \square_p \\
\Gamma \vdash A : \star_p \eta & \text{if } \Gamma \vdash A : \star_p \end{cases} \)

Finally, as in \( \lambda \omega_L \), all proof terms are interpreted as the element of 1. The properties proved in section 6.4 for the proof-irrelevance model for \( \lambda \omega_L \) also hold for this proof-irrelevance model for \( \lambda \omega^+_L \), and they can be proved in exactly the same way.

7.25 Theorem (Soundness)

1. Let \( \text{der}_1 \) and \( \text{der}_2 \) be derivations of \( \Gamma \vdash a : A \) and \( \Gamma \vdash a : A' \), respectively. Then

\[
\Gamma \vdash a : A \eta = [\Gamma \vdash a : A'] \eta ,
\]

where the meanings are defined using \( \text{der}_1 \) and \( \text{der}_2 \) respectively.

2. If \( \Gamma \vdash a : A \), then for all \( \eta \vdash \Gamma \)

\[
[\Gamma \vdash a : A] \eta \in \begin{cases} 
\text{Kind}_A & \text{if } \Gamma \vdash A : \square_s \\
\text{Dom}_{\{\tau, A, \star_s\}} \eta & \text{if } \Gamma \vdash A : \star_s \\
\Gamma \vdash A : \square_p \eta & \text{if } \Gamma \vdash A : \square_p \\
\Gamma \vdash A : \star_p \eta & \text{if } \Gamma \vdash A : \star_p 
\end{cases}
\]

3. If \( a \equiv_A a', \Gamma \vdash a : A \), and \( \Gamma \vdash a : A' \), then \( [\Gamma \vdash a : A] \eta = [\Gamma \vdash a' : A] \eta \) for all \( \eta \vdash \Gamma \)

\( \square \)

Like the proof-irrelevance models given before, this one can be used to prove consistency.

7.26 Corollary (Consistency of \( \lambda \omega^+_L \)). \( \lambda \omega^+_L \) is consistent (False is not provable). \( \square \)

and consistency of contexts, for instance.

7.27 Lemma (Consistency of \( AXIOM^+ \) in \( \lambda \omega^+_L \))

False is not provable in a context containing only axioms from \( AXIOM^+ \).

Proof. As in the proof of lemma 6.49, we have to supply a model \( M \) for the programming language – the PER-model will do – and check that all axioms from \( AXIOM^+ \) are then interpreted as 1 ("true") in the resulting \( \lambda \omega^+_L \)-model. \( \square \)

In fact, any model \( M \) that meets the general model definition for \( \lambda \omega^+_L \) can be used to prove consistency of all axioms in \( AXIOM^+ \). The domain equations ensure that the properties of \( +, \times \) and \( \Sigma \)-datatypes given by axioms in \( AXIOM^+ \) are true.
Chapter 8

Recursion

In this chapter we treat the semantics of the systems introduced in chapter 5: the programming language $\lambda \omega_5^\mu$ and the associated programming logic $\lambda \omega_7^\mu$. This chapter is organised in exactly the same way as chapter 7. First, in section 8.1, a general model definition for $\lambda \omega_5^\mu$ is given. Then, in section 8.2, a model is constructed that is an instantiation of this general model definition. And finally, in section 8.3, this model for the programming language is combined with a proof-irrelevance model for the logic, and the resulting model is used to prove soundness of $\lambda \omega_7^\mu$ and soundness of all the axioms introduced in chapter 5.

The main difference between the programming language $\lambda \omega_5^\mu$ and the programming languages $\lambda \omega$, and $\lambda \omega^+$ is that in $\lambda \omega_5^\mu$ we have unrestricted recursion at both program and datatype level. Consequently, in the general model definition for $\lambda \omega_5^\mu$ datatypes can no longer be interpreted as sets. Instead, types will be interpreted as cpos, the most commonly used semantic domains in denotational semantics. Recursive programs and recursive datatypes can then be interpreted as usual: recursive programs as least least fixpoints in cpos, and recursive datatypes as solutions of recursive domain equations.

The general model definition gives a collection of domain equations any model has to satisfy. In section 8.2 a model is constructed by solving these coupled domain equations. Because datatypes are interpreted as cpos, the standard technique can be used to do this. Earlier versions of this model construction – for different systems – are given in [EH89] and [PHE93]. Compared to the PER-models given in sections 6.2 and 7.2 this cpo-model is more in line with conventional programming language semantics, and it is compatible with conventional denotational semantics.

Given any model for $\lambda \omega_5^\mu$ that meets the general model definition, a proof-irrelevance model for $\lambda \omega_5^\mu$ can be defined. Because $\lambda \omega_5^\mu$ provides the same logical primitives as $\lambda \omega_7^\mu$, this is done in exactly the same way as for $\lambda \omega_7^\mu$ in section 7.3. Since datatypes are interpreted as cpos, it is easy to verify the soundness of the axioms introduced in chapter 5 for reasoning about recursive programs. This proves the consistency of $\lambda \omega_5^\mu$, of the context $\Gamma_{CPO}$, and of the axioms in $AXIOM^\mu$.

As in the previous chapters, only the semantics of the systems without the definition mechanism is treated. By theorems 5.8.5 and 5.12.5 – elimination of definitions for $\lambda \omega_5^\delta$ and $\lambda \omega_7^\delta$ – any model for $\lambda \omega_5^\mu$ or $\lambda \omega_7^\mu$ can also be used as an interpretation of $\lambda \omega_5^\delta$ or $\lambda \omega_7^\delta$.  

141
8.1 General Model Definition \( \lambda \omega^\mu \)

In this section the general model definition for \( \lambda \omega^+ \) given in section 7.1 is adapted to provide a general model definition for \( \lambda \omega^\mu \). The main difference is that programs are now interpreted as elements of cpos rather than sets. So instead of a set, we now associate a cpo \( \text{Dom} \lceil \text{lift} \circ \sigma \rceil \) with every datatype \( \sigma \).

From now on, by a cpo we always mean an \( \omega \)-cpo.

8.1 DEFINITION. An \( \omega \)-cpo is a set with a partial order \( \subseteq \), a least element \( \bot \), and limits of all chains of the form \( c_0 \subseteq c_1 \subseteq c_2 \subseteq \ldots \).

For countable sets this definition is equivalent with the one given in definition 5.13. For the general model definition it does not really matter what kind of domains are used.

New domain equations have to be included for the \( \mu \)-types in order to interpret the associated program construction, i.e., the functions fold and unfold.

A final difference with respect to the general model definition for \( \lambda \omega^+ \) is that the domain equations for the \( + \) and \( \Sigma \)-types have to be changed, because the sum construction on cpos differs from the one on sets. Apart from elements constructed using the injections \( \text{in}_C(1: A_1, \ldots, A_n) \) and \( \text{in}_E A \), the \( + \) and \( \Sigma \)-types now also contain bottom elements.

The semantics of the kinds and datatype-constructors

As far as the semantics of kinds and datatype-constructors is concerned, there is not much difference between \( \lambda \omega^+ \) and \( \lambda \omega^\mu \). We only have to extend the definition of an environment frame for the datatype-constructors of \( \lambda \omega^+ \) - definition 7.1 - with a function \( \mu \)

\[
\mu \in (\text{Kind}_*, \rightarrow \text{Kind}_*) \rightarrow \text{Kind}_* ,
\]

which gives the meaning of the new datatype-constructor \( \mu \).

8.2 DEFINITION. An environment frame for the datatype-constructors of \( \lambda \omega^\mu \) is a 8-tuple \( (\text{Kind}, \Phi_{\text{Kind}}, \rightarrow, \Pi, \Sigma, \times, +, [E]) \), where

- \( \text{Kind} = \{\text{Kind}_K \mid K \text{ is a kind}\} \) is a family of sets, indexed by kinds
- \( \Phi_{\text{Kind}} = \{\Phi_{K_1, K_2} \mid K_1 \rightarrow K_2 \text{ is a kind}\} \) is a family of bijections with \( \Phi_{K_1, K_2} \in \text{Kind}_{K_1} \rightarrow \text{Kind}_{K_2} \)
- \( \rightarrow \in \text{Kind}_* \rightarrow \text{Kind}_* \rightarrow \text{Kind}_* \)
- \( \Pi, \Sigma \in \Pi_{K \in \text{Kind}}(\text{Kind}_K \rightarrow \text{Kind}_*) \rightarrow \text{Kind}_* \)
- \( \times, + \in \prod_{L \in \text{Kind}_*}(L \rightarrow \text{Kind}_*) \rightarrow \text{Kind}_* \)
- \( [E] \in (\text{Kind}_*, \rightarrow \text{Kind}_*) \rightarrow \text{Kind}_* \)

The function \( \mu \) is used to define the semantics of the recursive datatypes.
8.1. GENERAL MODEL DEFINITION $\lambda\omega^\alpha$

8.3 DEFINITION (semantics of $\lambda\omega^\alpha$-datatype-constructors).
For datatype-constructors $\sigma$ we define $[\Gamma \vdash \sigma : \mathcal{K}] \eta$ for all $\Gamma \vdash \sigma : \mathcal{K}$ and $\eta \models \Gamma^\mathcal{K}$ by induction on the derivation of $\Gamma \vdash \sigma : \mathcal{K}$ as in definition 7.2, extended with the following clause:

$$[\Gamma \vdash (\mu \alpha : \omega^\star, \sigma) : \omega^\star] \eta \equiv \mu \eta (\lambda \alpha \in \text{Kind}_{\star^\omega}, [\Gamma, \alpha : \star, \sigma \vdash \alpha : \sigma] \eta[\alpha := \sigma]).$$

Analogous to definitions 6.4 and 7.3 we define:

8.4 DEFINITION An environment model for the datatype-constructors of $\lambda\omega^\alpha$ is an environment frame for the constructors of $\lambda\omega^\alpha$ for which $[\Gamma \vdash \sigma : \mathcal{K}] \eta$ is defined for all $\Gamma \vdash \sigma : \mathcal{K}$ and $\eta \models \Gamma^\mathcal{K}$.

For any environment model for the datatype-constructors of $\lambda\omega^\alpha$ we can prove the same properties as for environment models for the datatype-constructors of $\lambda\omega$ or $\lambda\omega^\beta$.

8.5 LEMMA (Soundness of type assignment for datatype-constructors).
If $\Gamma \vdash \sigma : \mathcal{K}$ then $[\Gamma \vdash \sigma : \mathcal{K}] \eta \in \text{Kind}_{\star^\omega}$ for all $\eta \models \Gamma^\mathcal{K}$.

8.6 LEMMA (Soundness of $\beta$-conversion for datatype-constructors).
Suppose $\Gamma \vdash \sigma : \mathcal{K}$, $\Gamma \vdash \sigma' : \mathcal{K}$, and $\sigma \equiv_{\beta} \sigma'$.

Then $[\Gamma \vdash \sigma : \mathcal{K}] \eta = [\Gamma \vdash \sigma' : \mathcal{K}] \eta$ for all $\eta \models \Gamma^\mathcal{K}$.

These lemmas can be proved in exactly the same way as in chapters 6 and 7.

The semantics of $\lambda\omega^\alpha$-terms

As mentioned before, instead of a set, we now associate a cpo $\text{Dom}_{\eta[\Gamma \vdash \sigma : \mathcal{K}]}$ with every datatype $\sigma$. So for every $\alpha \in \text{Kind}_{\star^\omega}$ there is a cpo $\text{Dom}_{\alpha}$, and programs of type $\sigma$ will be interpreted as elements of the cpo $\text{Dom}_{\eta[\Gamma \vdash \sigma : \mathcal{K}]}$. For a datatype $\sigma$, the program $\forall \sigma : (\sigma \to \sigma) \to \sigma$ is of course interpreted as the least fixpoint operator on the cpo $\text{Dom}_{\eta[\Gamma \vdash \sigma : \mathcal{K}]}$.

Recursive types should be isomorphic to their unfoldings. So it is obvious what the domain equation for a recursive type $(\mu \alpha : \omega, \sigma)$ should be, namely

$$\text{Dom}_{[\Gamma \vdash (\mu \alpha : \omega^\star, \sigma) : \omega^\star]} \equiv \text{Dom}_{[\Gamma \vdash [\sigma \equiv (\mu \alpha : \omega, \sigma)]] \omega^\star]}$$

The associated isomorphism then gives the interpretation of the operations $\text{fold}_{\mu \alpha : \omega, \sigma}$ and $\text{unfold}_{\mu \alpha : \omega, \sigma}$. Given the definition of $[\Gamma \vdash (\mu \alpha : \omega^\star, \sigma) : \omega^\star] \eta$ in definition 8.3, the new domain equations for the recursive types can also be given as

$$\text{Dom}_{\mu F} \equiv \text{Dom}_{\hat{k}(\mu F)}$$

Because cpos are used instead of sets, we have to reconsider the domain equations for $\to$, $\Pi$, $\to$, $\times$, and $\Sigma$-types given in the previous chapters. These were

$$\text{Dom}_{\alpha} \subset \text{Dom}_{\beta} \equiv [\text{Dom}_{\alpha} \hookrightarrow \text{Dom}_{\beta}]$$

$$\text{Dom}_{\Pi F} \equiv [\Pi \alpha \in \text{Kind}_{\star^\omega} \text{Dom}_{F(\alpha)}]$$

$$\text{Dom}_{\times F} \equiv \Pi \alpha \in \text{Kind}_{\star^\omega} \text{Dom}_{F(\alpha)}$$

$$\text{Dom}_{\Sigma F} \equiv \Sigma \alpha \in \text{Kind}_{\star^\omega} \text{Dom}_{F(\alpha)}$$

Because cpos are used instead of sets, we have to reconsider the domain equations for $\to$, $\Pi$, $\to$, $\times$, and $\Sigma$-types given in the previous chapters. These were

$$\text{Dom}_{\alpha} \subset \text{Dom}_{\beta} \equiv [\text{Dom}_{\alpha} \hookrightarrow \text{Dom}_{\beta}]$$

$$\text{Dom}_{\Pi F} \equiv [\Pi \alpha \in \text{Kind}_{\star^\omega} \text{Dom}_{F(\alpha)}]$$

$$\text{Dom}_{\times F} \equiv \Pi \alpha \in \text{Kind}_{\star^\omega} \text{Dom}_{F(\alpha)}$$

$$\text{Dom}_{\Sigma F} \equiv \Sigma \alpha \in \text{Kind}_{\star^\omega} \text{Dom}_{F(\alpha)}$$
where in the right-hand sides \( \prod \) and \( \sum \) denote the set-theoretic function space, cartesian product and disjoint sum, respectively, and \(|A|\) denotes some subset of \(A\).

We now have to turn the right-hand sides into cpos. For (i), (ii) and (iii) this is not a problem, because the natural ordering on these sets produces a cpo. If we look at the underlying sets, then only the domain equations (iv) and (v) will change.

8.7 **Definition (FS).** Let \(B\) and \(C\) be cpos, and let \((D_i \mid i \in I)\) be a family of cpos indexed by some set \(I\). Then

1. the cpo \(\text{FS}(B, C)\) is the set of the continuous functions from \(B\) to \(C\) with the ordering pointwise.

2. the cpo \(\text{GP}(D_i \mid i \in I)\) is the set \(\Pi_{i \in I} D_i\) with the ordering coordinate-wise, i.e.
   \[
   (d_i \mid i \in I) \leq (d'_i \mid i \in I) \iff \forall_{i \in I} d_i \subseteq d'_i.
   \]

3. the cpo \(\text{GS}(D_i \mid i \in I)\) is the set \(\{\bot\} \cup \sum_{i \in I} D_i\), partially ordered as follows
   \[
   c \subseteq c' \iff (c = \bot \lor (c = (i, d) \land c' = (i, d') \land d \subseteq d')).
   \]

The new domain equations are

\[
\begin{align*}
\text{Dom}_a \text{FS} & \cong \text{FS}(\text{Dom}_a, \text{Dom}_b) \quad (i) \\
\text{Dom}_a \Pi & \cong \text{GP}(\text{Dom}_a^{\{i\}} \mid a \in \text{Kind}^b) \quad (ii) \\
\text{Dom}_a \Sigma & \cong \text{GP}(\text{Dom}_a^{\{i\}} \mid i \in I) \quad (iii) \\
\text{Dom}_a \bar{\Sigma} & \cong \text{GS}(\text{Dom}_a^{\{i\}} \mid a \in \text{Kind}^b) \quad (iv) \\
\text{Dom}_a \mu & \cong \text{GS}(\text{Dom}_a^{\{i\}} \mid i \in I) \quad (v) \\
\text{Dom}_a \nu & \cong \text{Dom}_a^{\{\mu\}} \quad (vi)
\end{align*}
\]

where the square brackets denote a sub-cpo instead of a subset of \(\text{GP}(\text{Dom}_a^{\{i\}} \mid a \in \text{Kind}^b)\).

Below the differences between the old and the new domain equations for \(\to, \Pi, +, \times, \text{and } \Sigma\)-types are discussed.

- (i)
  The old domain equations required \(\text{Dom}_a \text{FS}\) to be isomorphic to some subset of the function space \(\text{Dom}_a \to \text{Dom}_b\). In the new domain equation it is fixed what this subset should be, namely the collection of continuous functions from \(\text{Dom}_a\) to \(\text{Dom}_b\), because this is the natural -- if not the only possible -- choice. We cannot take the strict continuous functions, because by the \(\beta\)-reduction rule \((\lambda x : A \ b) \triangleleft b[i - a]\) functions are not always strict. For instance, if \(x \notin \text{FV}(b)\) then \((\lambda x : A \ b) \triangleright b\) and so \((\lambda x : A \ b)\) is not strict if \(b \neq \bot\).
For the \( \Pi \)- and \( \times \)-types there is no real change. As far as the underlying sets are concerned, the new domain equations are the same as the old ones.

Unlike for the \( \to \)-types, for the \( \Pi \)-types there is no obvious choice for the sub-\( \text{cpo} \) in the right-hand side of the domain equation. In the model we construct in section 8.2 we will simply take the whole \( \text{cpo} \) \( GP(Dom_{\mathcal{F}(e)} \mid e \in \text{Kind}_{\mathcal{K}}) \).

Equation (iii) requires that the domain for Unit, the empty product type \( \Pi() \), is isomorphic with a one-point \( \text{cpo} \). This means that the program unit of type Unit is interpreted as the only element of this \( \text{cpo} \), i.e. its bottom element. An alternative is to require that the domain for Unit is isomorphic with a two-point \( \text{cpo} \), and take the interpretation of unit different from \( \bot_{\text{unit}} \).

For the \( \Sigma \)- and \( + \)-types there has been a real change. For example, the old domain equation for the type \( \sigma + \tau \) was

\[
\text{Dom}_{[\tau, \sigma + \tau, ~ \ast]}_\eta = \{(1, x) \mid x \in \text{Dom}_{[\tau, \sigma, ~ \ast]}_\eta\} \cup \{(2, x) \mid x \in \text{Dom}_{[\tau, \tau, ~ \ast]}_\eta\}.
\]

The problem is that the set on the right hand side cannot be partially ordered to produce a \( \text{cpo} \). At least, not in a such way that all the programs that can be constructed using \( \eta \) and \( \nabla \) are all continuous.

There are two constructions on \( \text{cpo} \)s that are possible interpretations of \( \sigma + \tau \): the lazy sum -- also known as the disjoint or separated sum --, and the strict or coalesced sum. Forgetting the \( \text{cpo} \)-ordering for the moment, and treating \( \text{cpo} \)s as sets, the lazy sum would result in the following domain equation.

\[
\text{Dom}_{[\tau, \sigma + \tau, ~ \ast]}_\eta = \{\bot\} \cup \{(1, x) \mid x \in \text{Dom}_{[\tau, \sigma, ~ \ast]}_\eta\} \cup \{(2, x) \mid x \in \text{Dom}_{[\tau, \tau, ~ \ast]}_\eta\},
\]

i.e. a new bottom element is provided. The strict sum would result in the following domain equation:

\[
\text{Dom}_{[\tau, \sigma + \tau, ~ \ast]}_\eta = \{\bot\} \cup \{(1, x) \mid x \in \text{Dom}_{[\tau, \sigma, ~ \ast]}_\eta\}\setminus\{\bot\} \cup \{(2, x) \mid x \in \text{Dom}_{[\tau, \tau, ~ \ast]}_\eta\}\setminus\{\bot\}.
\]

Here the bottom elements of \( \text{Dom}_{[\tau, \sigma, ~ \ast]}_\eta \) and \( \text{Dom}_{[\tau, \tau, ~ \ast]}_\eta \) are identified.

The reduction rules for \( + \)-types rule out the second possibility. If we interpret \( \sigma + \tau \) as a strict sum, then the value of the function \( f \lor g : \sigma + \tau \to \rho \) in \( (\text{in}_{\sigma + \tau} \bot_{\sigma}) \) and \( (\text{in}_{\sigma + \tau} \bot_{\tau}) \). But this is in conflict with the reduction behaviour of \( f \lor g \):

\[
(f \lor g)(\text{in}_{\sigma + \tau} \bot_{\sigma}) \triangleright \delta f \bot_{\sigma},
\]

\[
(f \lor g)(\text{in}_{\sigma + \tau} \bot_{\tau}) \triangleright \delta g \bot_{\tau},
\]

and \( f \bot_{\sigma} \) and \( g \bot_{\tau} \) may well be distinct.

Similarly, the \( \beta \)-reduction rules make it impossible to interpret \( \Pi \)- and \( \times \)-types as smashed products.

Note that \( GS() \) is a one-point \( \text{cpo} \). So the datatype \( \text{Empty}_{\mathcal{E}} \) \( \Sigma() \) is no longer interpreted as an empty type, but as a one-element type.
The domain equation

\[ \text{Dom} \sum_F \cong \text{GS}(\text{Dom}_F(a) \mid a \in \text{Kind}_K) \]  

requires more than is necessary for the interpretation of the associated program constructions, as we already discussed in chapter 7 for the same domain equation with GS replaced by \( \sum \). As for \( \lambda \omega^*_\tau \), it would be sufficient if the following domain equation is satisfied

\[ \text{Dom} \sum_F \cong \left( \text{GS}(\text{Dom}_F(a) \mid a \in \text{Kind}_K) \right) \cong \]  

with \( \cong \) as defined in definition 7.8. But for the particular cpo model that is given in section 8.2 the domain equations (i) and (ii) are identical. In this model all equivalence classes in \( \cong \) are singletons, which is caused by the fact that \( \text{Dom} \sum_F \) is isomorphic to the whole cpo \( \text{GP}(\text{Dom}_F(a) \mid a \in \text{Kind}_K) \). because of this, we will not go to the extra trouble of using (ii) instead of (i).

8.8 Definition (\( \lambda \omega^*_\tau \) cpo environment frame).

A cpo environment frame for \( \lambda \omega^*_\tau \) is a tuple \((\text{KIND}, \text{Dom}, \Phi^-, \Phi^+, \Phi^0, \Phi^\times, \Phi^\tau, \Phi^\mu)\), where

- \( \text{KIND} = (\text{Kind}, \Phi_{\text{Kind}}, \rightarrow, \mathbb{H}, \mathbb{L}, \mathbb{X}, \mathbb{Z}, \mathbb{+}, \mathbb{U}) \) is an environment model for the \( \lambda \omega^*_\tau \)-datatype-constructors.
- \( \text{Dom} = \{ \text{Dom}_a \mid a \in \text{Kind}_\tau \} \) is a family of cpos
- \( \Phi^- = \{ \Phi^-_a \mid a, b \in \text{Kind}_\tau \}, \Phi^0 = \{ \Phi^0_\mathbb{H} \mid \mathbb{H} : \mathbb{H} \rightarrow \text{Kind}_\tau \rightarrow \text{Kind}_\tau \}, \Phi^\times = \{ \Phi^\times_\mathbb{L} \mid \mathbb{L} : \mathbb{L} \rightarrow \text{Kind}_\tau \rightarrow \text{Kind}_\tau \}, \Phi^+ = \{ \Phi^+_\mathbb{X} \mid \mathbb{X} : \mathbb{X} \rightarrow \text{Kind}_\tau \rightarrow \text{Kind}_\tau \}, \Phi^\tau = \{ \Phi^\tau_\mathbb{Z} \mid \mathbb{Z} : \mathbb{Z} \rightarrow \text{Kind}_\tau \rightarrow \text{Kind}_\tau \}, \Phi^\mu = \{ \Phi^\mu_\mathbb{U} \mid F \in \text{Kind}_\tau \rightarrow \text{Kind}_\tau \} \) are families of bijections with
  
  \[ \Phi^-_a \in \text{Dom}_a \rightarrow \text{FS}(\text{Dom}_a, \text{Dom}_b) \]
  \[ \Phi^0_\mathbb{H} \in \text{Dom} \rightarrow \text{GP}(\text{Dom}_{F(a)} \mid a \in \text{Kind}_K) \]
  \[ \Phi^\times_\mathbb{L} \in \text{Dom} \rightarrow \text{GP}(\text{Dom}_{F(a)} \mid a \in \text{Kind}_K) \]
  \[ \Phi^+_\mathbb{X} \in \text{Dom} \rightarrow \text{GP}(\text{Dom}_{F(a)} \mid a \in \text{Kind}_K) \]
  \[ \Phi^\tau_\mathbb{Z} \in \text{Dom} \rightarrow \text{GP}(\text{Dom}_{F(a)} \mid a \in \text{Kind}_K) \]
  \[ \Phi^\mu_\mathbb{U} \in \text{Dom} \rightarrow \text{GP}(\text{Dom}_{F(a)} \mid a \in \text{Kind}_K) \]

\[ \square \]

We now define the interpretation of the \( \lambda \omega^*_\tau \)-programs in an arbitrary environment frame. Only the differences with respect to definition 7.10, which defines the semantics of \( \lambda \omega^*_\tau \)-programs, are given. The differences are the interpretation of \( \nabla \), where we now have to take the bottom elements into account, and the interpretation of the new program constructions (unfold and \( Y \)). In example 8.10 the interpretations of case and abstype are given, which are a lot easier to read than the interpretation of \( \nabla \) for \( + \) and \( \Sigma \)-types.

8.9 Definition (semantics of \( \lambda \omega^*_\tau \)-programs).

For programs \( M \) we define \( \Gamma \vdash M : \sigma \eta \) for all \( \Gamma \vdash M : \sigma \) and \( \eta \vdash \Gamma^{\sigma \cdot \eta} \), as in definition 7.10 - i.e. by induction on the derivation of \( \Gamma \vdash M : \sigma \) with the following extra clauses:
8.1. GENERAL MODEL DEFINITION $\lambda\omega^\mu$

For $\mu$-types:
Let $F = (\exists a \in \text{Kind}_a. [\Gamma, \alpha : * \vdash \sigma : *], \eta(\alpha := a)) \in \text{Kind}_a \rightarrow \text{Kind}_a$.
Then
\[
\Gamma \vdash \text{fold } M : (\mu \alpha . \sigma, \alpha) \Rightarrow \Phi_1(\Gamma \vdash M : \sigma|\alpha := (\mu \alpha . \sigma, \alpha)) \eta
\]
\[
\Gamma \vdash \text{unfold } M : \sigma|\alpha := (\mu \alpha . \sigma, \alpha) \Rightarrow \Phi_2(\Gamma \vdash M : (\mu \alpha . \sigma, \alpha)) \eta
\]
where $\Phi = \Phi_F \in \text{Dom} [\mu]_F \rightarrow \text{Dom} F(\mu F)$.

For $\Sigma$-types:
Let $F = (\exists a \in \text{Kind}_a. [\Gamma, \alpha : * \vdash \sigma : *], \eta(\alpha := a)) \in \text{Kind}_a \rightarrow \text{Kind}_a$.
Then
\[
\Gamma \vdash \forall \chi . \Sigma \vdash \eta(\chi) \Rightarrow \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_1 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_2 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_3 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
where $\Phi_1 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)$.
\[
\Phi_2 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_3 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_4 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]

For $\Sigma$-types:
Let $F = (\exists a \in \text{Kind}_a. [\Gamma, \alpha : * \vdash \sigma : *], \eta(\alpha := a)) \in \text{Kind}_a \rightarrow \text{Kind}_a$.
Then
\[
\Gamma \vdash \forall \chi . \Sigma \vdash \eta(\chi) \Rightarrow \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_1 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_2 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_3 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_4 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]

For $\Sigma$-types:
Let $F = (\exists a \in \text{Kind}_a. [\Gamma, \alpha : * \vdash \sigma : *], \eta(\alpha := a)) \in \text{Kind}_a \rightarrow \text{Kind}_a$.
Then
\[
\Gamma \vdash \forall \chi . \Sigma \vdash \eta(\chi) \Rightarrow \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_1 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_2 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_3 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
\[
\Phi_4 = \Phi_3 F \equiv \text{Dom}^{[\Sigma]}_F \rightarrow \text{Dom} F(\chi)
\]
where $\Phi_1 = \Phi_{F}^{\sum} \in \text{Dom}(\mathbb{S})_F \rightarrow \{\bot\} \cup \sum_n \text{Dom}_{F(a)}$,

$\Phi_2 = \Phi_{F(a) \otimes} \in \text{Dom}(\mathbb{F})_F \otimes \mathbb{R} \rightarrow \text{Dom}_{F(a)} \otimes \text{Dom}_F$,

$\Phi_3 = \Phi_{F}^{\Pi} \in \text{Dom}(\mathbb{F})_F \rightarrow \Pi_n \text{Dom}_{F(a)} \otimes \mathbb{R}$,

$\Phi_4 = \Phi_{F(a) \otimes} \in \text{Dom}_{F(a)} \otimes \mathbb{R} \rightarrow \text{Dom}_{F(a)} \otimes \text{Dom}_F$.

8.10 Example. As in chapter 7, the interpretation of the case- and abstype-construction is easier to read than the interpretation of the following interpretation for the case- and abstype-construction:

\[
\Gamma \vdash (\text{case } N \text{ of } m.n \leftarrow M_1 \vdash \ldots \vdash m.n \leftarrow M_n \text{ esac}) : \tau \]

\[
\begin{aligned}
&= \Gamma \vdash \bigcup l_1 \leftarrow (\lambda \tau \sigma_1 M_1), \ldots, l_n \leftarrow (\lambda \tau \sigma_n M_n)) \quad N \quad \tau
\end{aligned}
\]

\[
= \left\{ \begin{array}{ll}
\Gamma \vdash \xi : \sigma_1 \vdash M_1 \quad \tau & \text{if } \Phi(\Gamma \vdash \Sigma(l_1 : \sigma_1, \ldots, l_n : \sigma_n)) \eta = (l_1, \chi) \\
\bot & \text{if } \Phi(\Gamma \vdash \Sigma \vdash l_1 : \sigma_1, \ldots, l_n : \sigma_n)) \eta = \bot
\end{array} \right.
\]

where $\Phi = \Phi_{\lambda l_1 \in \{l_1, \ldots, l_n\} \bigcup \{l 1 \leq \ldots \leq l_n\}}$.

\[
\Gamma \vdash (\text{abstype } \alpha: I_{K} \text{ with } x: \sigma \text{ is } N \text{ in } M) : \rho
\]

\[
= \Gamma \vdash \bigcup (\lambda \alpha I_{K}, \lambda \xi \sigma M \quad N) \quad \tau
\]

\[
= \left\{ \begin{array}{ll}
\Gamma \vdash \xi : \alpha \vdash I_{K} \quad \sigma \vdash M \quad \tau & \text{if } \Phi(\Gamma \vdash \Sigma l_1 : \sigma_1, \ldots, l_n : \sigma_n) \eta = (\alpha, \chi)
\end{array} \right.
\]

where $\Phi = \Phi_{\lambda l_1 \in \{l_1, \ldots, l_n\} \bigcup \{l 1 \leq \ldots \leq l_n\} | \eta = \eta |}$

8.11 Definition. A $\lambda \omega^+_{\alpha}$-environment model is a $\lambda \omega^+_{\alpha}$-environment frame for which $\Gamma \vdash M : \sigma \eta$ is defined for all $\Gamma \vdash M : \sigma$ and $\eta \models \Gamma^\alpha$.

The properties proved in chapters 6 and 7 for arbitrary environment models of $\lambda \omega^\alpha$ and $\lambda \omega^+_{\alpha}$ also hold for arbitrary environment models of $\lambda \omega^+_{\alpha}$, and they can be proved in exactly the same way.

8.12 Lemma. Let $\text{der}_1$ and $\text{der}_2$ be derivations of $\Gamma \vdash M : \sigma$ and $\Gamma \vdash M : \sigma'$, respectively. Then

\[
[\Gamma \vdash M : \sigma] \eta = [\Gamma \vdash M : \sigma'] \eta,
\]

where the meanings are defined using $\text{der}_1$ and $\text{der}_2$ respectively.

8.13 Lemma (Soundness of type assignment for programs).
If $\Gamma \vdash M : \sigma$ then $[\Gamma \vdash M : \sigma] \eta \in \text{Dom}_{[\Gamma^\sigma \tau \omega^\alpha]} \eta$ for all $\eta \models \Gamma^\alpha$.

8.14 Lemma (Soundness of $\beta_{\eta}$-conversion for programs).
Suppose $M \approx_{\beta_{\eta}} M'$, $\Gamma \vdash M : \sigma$, and $\Gamma \vdash M : \sigma'$.
Then $[\Gamma \vdash M : \sigma] \eta = [\Gamma \vdash M' : \sigma'] \eta$ for all $\eta \models \Gamma^\alpha$. 

\[\square\]
8.2 CPO-MODEL FOR $\lambda \omega_2$

In this section we construct a cpo-model that is an $\lambda \omega_2$-environment model as defined in the previous section. The general model definition gives a system of coupled domain equations that have to be satisfied:

$$
\begin{align*}
\text{Dom}_a \rightarrow b & \cong \text{FS}(\text{Dom}_a, \text{Dom}_b) \\
\text{Dom} \left[ \Pi \right]_F & \cong \left[ \text{GP}(\text{Dom}_{F(a)} \mid a \in \text{Kind}_F) \right] \\
\text{Dom} \left[ \Sigma \right]_F & \cong \text{GS}(\text{Dom}_{F(a)} \mid a \in \text{Kind}_F) \\
\text{Dom} \left[ \times \right]_F & \cong \text{GP}(\text{Dom}_{F(l)} \mid l \in L) \\
\text{Dom} \left[ + \right]_F & \cong \text{GS}(\text{Dom}_{F(l)} \mid l \in L) \\
\text{Dom} \left[ ; \right]_F & \cong \text{Dom}_{F(\left[ ; \right]_F)}
\end{align*}
$$

These equations are mutually recursive, because of the equations (ii), (iii) and (vi). It is obvious that (vi) is recursive. For (ii) and (iii) this is less obvious, but the right-hand sides of these equations refer to all $\text{Dom}_{F(a)}$, which includes many $\text{Dom}_{F(a)}$ with $\left[ \Pi \right]_F$ or $\left[ \Sigma \right]_F$ a subexpression of $F(a)$ (for instance $\text{Dom}_{F(\left[ \Pi \right]_F)}$ or $\text{Dom}_{F(\left[ \Sigma \right]_F)}$).

To construct a $\lambda \omega_2$-model we will construct a family of cpos $\text{Dom} = \langle \text{Dom}_a \mid a \in \text{Kind}_g \rangle$ that solves this system of coupled domain equations. For this the standard technique for solving domain equations, as described in for instance [SP82], is used. The necessary tools for this technique, which involve some category theory, are introduced in subsection 8.2.1. In subsection 8.2.2 the results given in subsection 8.2.1 are applied to construct a solution of the domain equations above.

The domain equations above leave open the choice of a particular sub-cpo of the cpo $\text{GP}(\text{Dom}_{F(a)} \mid a \in \text{Kind}_g)$. Here we choose the whole cpo. So the model that is constructed will satisfy

$$
\text{Dom} \left[ \Pi \right]_F \cong \text{GP}(\text{Dom}_{F(a)} \mid a \in \text{Kind}_g)
$$

8.2.1 Category-theoretic solution of recursive domain equations

We assume the reader is familiar with the basic notions of category theory. For a category $C$, we write $\text{Obj}(C)$ for the collection of objects in $C$. For $c, c' \in \text{Obj}(C)$, we write $\text{Hom}_C(c, c')$ for the collection of morphisms from $c$ to $c'$ in $C$.

Fixed-points of Functors

Solutions of a recursive domain equations $\text{Dom} \cong F(\text{Dom})$ can be regarded as fixed points of a functor $F$ on some category

8.15 DEFINITION. A \textit{fixed point} of a functor $F$ on a category $C$, is a pair $\langle \text{Dom}, \phi \rangle$, where $\text{Dom}$ is a $C$-object and $\phi$ an isomorphism between $\text{Dom}$ and $F(\text{Dom})$. $$
$$

The initial fixed point theorem given below gives a class of functors for which (initial) fixed points exists, namely so-called $\omega$-continuous functors on $\omega$-categories.
8.16 Definition (ω-chain, ω-continuous, ω-colimit, ω-category)

1. An ω-chain is a diagram of the form \( c_0 \xrightarrow{\phi_0} c_1 \xrightarrow{\phi_1} c_2 \).

2. A functor is called ω-continuous if it preserves ω-colimits, i.e., colimits of ω-chains.

3. An ω-category is a category with an initial object which has all ω-colimits, i.e., in which every ω-chain has a colimit.

8.17 Theorem (Initial fixpoint theorem).
Every ω-continuous functor on an ω-category has an initial fixed-point.

This theorem is similar to the least fixpoint theorem for ω-poses, which states that every continuous function on a ω-pose has a least fixpoint. In fact, the fixpoint theorem for cpos is a particular case of the initial fixed point theorem for ω-categories. In denotational semantics this general result is applied to construct solutions of a recursive domain equation \( \text{Dom} \cong F(\text{Dom}) \).

CPO and functors on CPO

We now introduce the particular categories and functors that will be used. The following category that plays a central role.

8.18 Definition. CPO is the category with ω-poses, i.e., partially ordered sets with an initial object and limits of all chains \( c_0 \subseteq c_1 \subseteq c_2 \subseteq \ldots \) as objects, and continuous functions as morphisms.

Because of the interdependence of the domain equations they all have to be solved simultaneously. Therefore we will construct a solution in a product category.

8.19 Definition (product category).

Let \( I \) be an index set and \( C \) a category. The product category \( \prod_I C \) is then defined as follows:

- a \( \prod_I C \)-object is a family \( (c_i \mid i \in I) \), where each \( c_i \) is a \( C \)-object,
- a \( \prod_I C \)-morphism from \( (c_i \mid i \in I) \) to \( (c'_i \mid i \in I) \) is a family \( (\phi_i \mid i \in I) \), where each \( \phi_i \) is a \( C \)-morphism from \( c_i \) to \( c'_i \).

A product category \( \prod_I C \) inherits many of the properties of \( C \). In particular:

8.20 Lemma ([HS73] corollary 25.7)
If \( C \) has all ω-colimits, i.e., \( C \) has colimits of all ω-chains, then so does \( \prod_I C \).

So the family of cpos \( \text{Dom} = (\text{Dom}_a \mid a \in \text{Kind}_+) \) needed for the \( \lambda^{\omega^\omega} \)-model is an object in the category \( \prod_{\text{Kind}_+} \text{CPO} \).

The constructions on cpos that are used in the domain equations - FS, GP, and GS are all functors.
8.2 CPO-MODEL FOR $\omega_0^+$

8.21 Definition (FS, GP, GS).

The object-parts of the functors $FS : \text{CPO}^\times \rightarrow \text{CPO}$ and $GP, GS : \Pi CPO \rightarrow \text{CPO}$ have been defined in definition 8.7. The morphism-parts are defined below.

- Suppose $\phi \in \text{Hom}(B', B)$ in CPO and $\psi \in \text{Hom}(C, C')$ in CPO.
  Then $FS(\phi, \psi) \in \text{Hom}(FS(B, C), FS(B', C'))$ is the function that maps $\xi \in FS(B, C)$ to $\psi \circ \xi \circ \phi \in FS(B', C')$.

- Suppose $\phi \in \Pi CPO$ so $\phi_i \in \text{Hom}(D_i, E_i)$ in CPO for all $i \in I$.
  Then $GP(\phi) \in \text{Hom}(GP(D), GP(E))$ is the function that maps $\langle d_i | i \in I \rangle \in GP(D)$ to $\langle \phi_i(d_i) | i \in I \rangle \in GP(E)$.

$GS(\phi) \in \text{Hom}(GS(D), GS(E))$ is the function that maps $\bot \in GS(D)$ to $\bot \in GS(E)$, and $(i, d) \in GS(D)$ to $(i, \phi_i(d)) \in GS(E)$. □

The functor $FS$ is contravariant in its first argument. Because of this, it is not possible to construct the family of cpos $\text{Dom} = \langle \text{Dom}_a | a \in \text{Kind}_a \rangle$ needed for a $\omega_0^+$-model as an initial fixed-point in the category $\Pi CPO$. There is a standard technique to overcome this problem, which is described below.

O-categories

The standard technique for solving domain equations that involve the function space functor or other contravariant functors is described in [LS81] [SP82]. The method is a generalisation of Scott’s inverse limit construction. We just give a short overview of the method. For a clear and self-contained presentation we refer to [BH88]. Below we just list all the results that we will need.

A special kind of category, the so-called O-categories, is used. The crucial property of these O-categories is given by theorem 8.25 below. It states that given a functor $\mathcal{H}$ on an O-category $\mathcal{C}$, which is contravariant in one or more of its arguments, there is a corresponding functor $\mathcal{F}$ on an associated category $CPR$, which is covariant in all its arguments. Moreover, $\omega$-continuity of this functor $\mathcal{F}$ can be proved relatively easily. But first, some definitions are needed.

8.22 Definition (O-category) A category is an O-category iff

- every hom-set is a partially ordered set, in which every ascending $\omega$-chain has a least upper bound,
- composition is $\omega$-continuous with respect to the partial order on the hom-sets □

It is trivial to verify that $\text{CPO}$ and $\Pi CPO$ are O-categories. The ordering on the hom-sets of $\Pi CPO$ is of course defined coordinate-wise.
8.23 Definition (category of embedding-projection pairs). If \( C \) is an \( O \)-category, then the associated category of embedding-projection pairs \( C_{PR} \) is the category with

- the same objects as \( C \), i.e. \( \text{Obj}(C_{PR}) = \text{Obj}(C) \),
- as morphisms embedding-projection pairs of morphisms, i.e. \( (\phi, \psi) \in \text{Hom}(a, b) \) in \( C_{PR} \) iff \( \phi \in \text{Hom}_C(a, b) \land \psi \in \text{Hom}_C(b, a) \land \phi \psi \subseteq \text{id}_b \land \psi \phi = \text{id}_a \).

\[ \square \]

The following notion can be used to prove \( \omega \)-continuity of functors on a category \( C_{PR} \).

8.24 Definition (local continuity). Let \( C \) be an \( O \)-category, and \( \mathcal{H} : C^{op} \times C \to C \) be a functor, i.e. \( \mathcal{H} \) is a bifunctor on \( C \) that is contravariant in its first and covariant in its second argument.

\( \mathcal{H} \) is called locally continuous if it is continuous with respect to the partial order on hom-sets, i.e. if, for all \( b, b', c, c' \in \text{Obj}(C) \), the mapping

\[ \phi \in \text{Hom}(b', b), \psi \in \text{Hom}(c, c') \mapsto \mathcal{H}(\phi, \psi) \in \text{Hom}(\mathcal{H}(b', c), \mathcal{H}(b, c')) \]

is continuous w.r.t. the ordering on these hom-sets.

\[ \square \]

For example, it is easy to check that the functor \( FS \) is locally continuous. We can now state the main property of (functors on) \( O \)-categories.

8.25 Theorem (\( \omega \)-continuity from local continuity). Let \( \mathcal{H} : C^{op} \times C \to C \) be a locally continuous functor, and \( C \) be an \( O \)-category which has all \( \omega \)-colimits, i.e. every \( \omega \)-chain has a colimit.

Then the functor \( \mathcal{F} : C_{PR} \to C_{PR} \) defined by

\[ \mathcal{F}(c) = \mathcal{H}(c, c) \quad \text{for } C_{PR}\text{-objects } c \]
\[ \mathcal{F}(\phi, \psi) = (\mathcal{H}(\psi, \phi), \mathcal{H}(\phi, \psi)) \quad \text{for } C_{PR}\text{-morphisms } (\phi, \psi) \]

is an \( \omega \)-continuous functor.

\[ \text{Proof.} \quad \text{This theorem is a slightly weakened version of theorem 3 in [SP82]. The difference is that the rather technical condition that } C \text{ has "locally determined } \omega \text{-colimits of embeddings" has been replaced with the condition that } C \text{ has all } \omega \text{-colimits. By the corollary to theorem 2 in [SP82] this condition is stronger.} \]

This result will be used in the next section to prove \( \omega \)-continuity of a functor, with which we then construct a \( \lambda \omega \beta \)-model as an initial fixpoint.

8.2.2 Construction of a CPO-model

Before the family of cpos \( \text{Dom} \) can be constructed, an environment model for the datatype-constructor is needed. Any environment model for the datatype-constructor can be used. We take the simplest possible model, i.e. the term model:
8.26 Definition. \( \text{KIND}_\text{TERM} = (\text{Kind}, \Phi_{\text{Kind}}, \longrightarrow, \Pi, [\Sigma], [\sqcap], [\otimes], [\sqcup], [\mu]) \) is the closed term model for the \( \lambda\omega^\mu \)-constructors.

So \( \text{Kind}_{K} \) is the collection of \( \beta \)-equivalence classes of closed datatype-constructors of type \( K \), i.e.

\[ \text{Kind}_{K} = \{ \sigma \mid \sigma \in K \} / \sim_{\beta} \]

with the associated bijections \( \Phi_{K_1 \rightarrow K_2} \in \text{Kind}_{K_1} \rightarrow \text{Kind}_{K_2} \) defined by

\[ \Phi_{K_1 \rightarrow K_2} = \lambda \sigma \cdot [\sigma]_{\sim_{\beta}} \in \text{Kind}_{K_1} \rightarrow \text{Kind}_{K_2}, \quad [\sigma]_{\sim_{\beta}} \in \text{Kind}_{K_1}, \quad [\sigma \rightarrow \tau]_{\sim_{\beta}} b. \]

Obviously, \( \text{KIND}_\text{TERM} \) is an environment model for the datatype-constructors of \( \lambda\omega^\mu \). The function \( \longrightarrow \) \( \in \text{Kind}_{\ast} \rightarrow \text{Kind}_{\ast} \rightarrow \text{Kind}_{\ast} \) is

\[ \longrightarrow = \lambda \sigma \cdot [\sigma]_{\sim_{\beta}}, \quad [\tau]_{\sim_{\beta}} \in \text{Kind}_{\ast}. \quad [\sigma \rightarrow \tau]_{\sim_{\beta}}. \]

The other datatype-constructors are interpreted similarly. We will not distinguish a datatype-constructor \( \sigma \) and the equivalence class \( [\sigma]_{\sim_{\beta}} \) to which it belongs, and we also do not distinguish \( \longrightarrow \) and \( \rightarrow, \Pi \) and \( \Pi, \otimes \) and \( \otimes, \) etc.

To complete the \( \lambda\omega^\mu \)-model, a family of cpos \( \text{Dom} = \langle \text{Dom}_a \mid a \in \text{Kind}_{\ast} \rangle \) is needed that solves the domain equations. To construct such a \( \text{Dom} \) as the initial fixpoint, an appropriate \( \omega \)-category and \( \omega \)-continuous functor \( F \) on that category are needed. The category should have families of cpos as objects, and the functor \( F \) should map an object \( \text{Dom} = \langle \text{Dom}_a \mid a \in \text{Kind}_{\ast} \rangle \) to \( F(\text{Dom}) = \langle F(\text{Dom})_a \mid a \in \text{Kind}_{\ast} \rangle \) with

\[
\begin{align*}
F(\text{Dom})_{\sigma \rightarrow \tau} &= F\Sigma(\text{Dom}_\sigma, \text{Dom}_\tau) \\
F(\text{Dom})_{\Pi F} &= G\Pi(\text{Dom}_{F(a)} \mid a \in \text{Kind}_{K}) \\
F(\text{Dom})_{D F} &= G\Sigma(\text{Dom}_{F(a)} \mid a \in \text{Kind}_{K}) \\
F(\text{Dom})_{\times F} &= G\Pi(\text{Dom}_{F(l)} \mid l \in L) \\
F(\text{Dom})_{+ F} &= G\Sigma(\text{Dom}_{F(l)} \mid l \in L) \\
F(\text{Dom})_{\mu F} &= \text{Dom}_F(\mu F)
\end{align*}
\]

Then any fixpoint of \( F \) provides a solution of the domain equations.

As the category we use \( (\Pi_{\text{Kind}_{\ast}} \text{CPO})_{PR} \). We will omit the subscript \( \text{Kind}_{\ast} \) and just write \( (\Pi \text{CPO})_{PR} \). By definition 8.23 the category \( (\Pi \text{CPO})_{PR} \) is the category with

- as objects families of cpos \( \langle \text{Dom}_a \mid a \in \text{Kind}_{\ast} \rangle \),

- as the morphisms from \( D \) to \( E \) projection-embedding pairs \( (\phi, \psi) \), i.e. \( \phi \in \text{Hom}(D, E) \) and \( \psi \in \text{Hom}(E, D) \) in \( \Pi \text{CPO} \), and \( \psi \circ \phi = \text{id}_D \) and \( \phi \circ \psi \subseteq \text{id}_E \).

By the definition of product category (def. 8.19), this means that \( \phi \) and \( \psi \) are families of continuous functions, with \( \phi_a \in D_a \rightarrow E_a \) and \( \psi_a \in E_a \rightarrow D_a \) and \( \psi_a \circ \phi_a = \text{id}_{D_a} \) and \( \phi_a \circ \psi_a \subseteq \text{id}_{E_a} \) for all \( a \in \text{Kind}_{\ast} \).
Instead of the category $\Pi \Pi CPO_{PR}$ we could also use the category $\Pi (CPO_{PR})$. In fact, the two categories are isomorphic. They have the same objects. The morphisms in $\Pi CPO_{PR}$ are pairs of families of continuous functions $((\phi_0, a \in Kind^*_a), \psi_a | a \in Kind^*_a)$, and the morphisms in $\Pi (CPO_{PR})$ are families of pairs of continuous functions $((\phi_a, \psi_a) | a \in Kind^*_a)$. Using $\Pi (CPO_{PR})$ instead of $\Pi (CPO_{PR})$ requires slightly more work.

To apply the initial fixed point theorem we need.

8.27 Lemma. $\Pi (CPO_{PR})$ is an $\omega$-category

Proof. We must show that the category $\Pi (CPO_{PR})$ has all $\omega$-colimits, i.e. that every $\omega$-chain has a colimit, and that it has an initial element.

The obvious candidate for the initial object is the constant family $\{1\} | a \in Kind^*_a$ which maps every index $a$ to the one-point cpo. It can easily be verified that this is indeed an initial element.

The category $CPO_{PR}$ has all $\omega$-colimits (see for instance [SP82]). Then by lemma 8.20 $\Pi (CPO_{PR})$ has all $\omega$-colimits, and this category is isomorphic to $\Pi (CPO_{PR})$.

We now define the functor $\mathcal{F}$ on the category $\Pi (CPO_{PR})$ that is used to construct the family of cpos $\text{Dom} = (\text{Dom}_a | a \in Kind^*_a)$ which solves the domain equations. The definition of the object-part of $\mathcal{F}$ is prescribed by the domain equations. For the definition of the morphism-part we then just have to be careful to give $\mathcal{F}$ the right arguments.

8.28 Definition. The functor $\mathcal{F}$ from $\Pi (CPO_{PR})$ to $\Pi (CPO_{PR})$ is defined as follows:

- (Object-part) Suppose $D \in \text{Obj}(\Pi (CPO_{PR}))$. So $D = (\text{Dom}_a | a \in Kind^*_a)$ is a family of cpos. Then $\mathcal{F}(D) = (\mathcal{F}(D)_a | a \in Kind^*_a)$ is defined as follows:

  \[
  \begin{align*}
  \mathcal{F}(D)_{S_{1}} &= \text{FS}(D_{S_{2}}, D_{S_{1}}) \\
  \mathcal{F}(D)_{S_{2}} &= \text{GP}(D_{S_{4}}, a \in \text{Kind}_{R}) \\
  \mathcal{F}(D)_{S_{4}} &= \text{GS}(D_{S_{5}}, a \in \text{Kind}_{R}) \\
  \mathcal{F}(D)_{S_{5}} &= \text{GP}(D_{S_{6}}, l \in L) \\
  \mathcal{F}(D)_{S_{6}} &= \text{GS}(D_{S_{7}}, l \in L) \\
  \mathcal{F}(D)_{S_{7}} &= D_{S_{8}}
  \end{align*}
  \]

- (Morphism-part) Suppose $(\phi, \psi) \in \text{Hom}(D, E)$ in $\Pi (CPO_{PR})$. So all $\phi_a$ and $\psi_a$ are continuous functions, $\phi_a \in \text{Dom}_a \rightarrow E_a$ and $\psi_a \in E_a \rightarrow \text{Dom}_a$.

  Then $\mathcal{F}(\phi, \psi) = (\phi', \psi')$, with $\phi'_a \in \mathcal{F}(D)_a \rightarrow \mathcal{F}(E)_a$ and $\psi'_a \in \mathcal{F}(E)_a \rightarrow \mathcal{F}(D)_a$ defined as follows:

  \[
  \begin{align*}
  \phi'_{S_{1}} &= \text{FS}(\psi_{S_{2}}, \phi_{S_{1}}) \\
  \phi'_{S_{2}} &= \text{GP}(\psi_{S_{4}}, a \in \text{Kind}_{R}) \\
  \phi'_{S_{4}} &= \text{GS}(\psi_{S_{5}}, a \in \text{Kind}_{R}) \\
  \phi'_{S_{5}} &= \text{GP}(\psi_{S_{6}}, l \in L) \\
  \phi'_{S_{6}} &= \text{GS}(\psi_{S_{7}}, l \in L) \\
  \phi'_{S_{7}} &= \phi_{S_{8}}
  \end{align*}
  \]

  \[
  \begin{align*}
  \psi'_{S_{1}} &= \text{FS}(\phi_{S_{2}}, \psi_{S_{1}}) \\
  \psi'_{S_{2}} &= \text{GP}(\phi_{S_{4}}, a \in \text{Kind}_{R}) \\
  \psi'_{S_{4}} &= \text{GS}(\phi_{S_{5}}, a \in \text{Kind}_{R}) \\
  \psi'_{S_{5}} &= \text{GP}(\phi_{S_{6}}, l \in L) \\
  \psi'_{S_{6}} &= \text{GS}(\phi_{S_{7}}, l \in L) \\
  \psi'_{S_{7}} &= \psi_{S_{8}}
  \end{align*}
  \]

It is easy to verify coordinate-wise that $\mathcal{F}$ preserves identities and composition, so that it is indeed a functor
The domain equations for $\lambda \omega_\omega$ can now be stated as $\text{Dom} \cong \mathcal{F}(\text{Dom})$. Theorem 8.25 will be used to prove that $\mathcal{F}$ is $\omega$-continuous.

8.29 Lemma. $\mathcal{F}$ is $\omega$-continuous.

Proof. To apply theorem 8.25 we first have to prove that $\prod \text{CPO}$ has all $\omega$-colimits. CPO has all $\omega$-colimits (see for instance [SP82]), so then by lemma 8.20 $\prod \text{CPO}$ has all $\omega$-colimits.

All that is needed now to apply theorem 8.25 is a locally continuous functor $\mathcal{H} : (\prod \text{CPO})^{\text{op}} \times \prod \text{CPO} \to \prod \text{CPO}$ such that

$$\mathcal{F}(D) = \mathcal{H}(D, D) \quad \text{for } (\prod \text{CPO})_{PR-\text{objects }} D$$

$$\mathcal{F}(\phi, \psi) = (\mathcal{H}(\psi, \phi), \mathcal{H}(\phi, \psi)) \quad \text{for } (\prod \text{CPO})_{PR-\text{morphisms }} (\phi, \psi)$$

This functor is defined as follows:

- **Object-part** Suppose $D \in \text{Obj}(\prod \text{CPO})^{\text{op}}$ and $E \in \text{Obj}(\prod \text{CPO})$. So $D$ and $E$ are elements of $\prod \text{CPO}$. Then $\mathcal{H}(D, E)$ is defined by

  $$\mathcal{H}(D, E)_\sigma \tau = \text{FS}(D_\sigma, E_\tau)$$

  $$\mathcal{H}(D, E) \eta F = \text{GP}(\text{F}_\eta(a) | a \in \text{Kind } F)$$

  $$\mathcal{H}(D, E) \Sigma F = \text{GS}(\text{F}_\eta(a) | a \in \text{Kind } F)$$

  $$\mathcal{H}(D, E)_l F = \text{GP}(\text{F}_l(l) | l \in L)$$

  $$\mathcal{H}(D, E)_L F = \text{GS}(\text{F}_l(l) | l \in L)$$

- **Morphism-part** Suppose $\phi \in \text{Hom}(D, E)$ in $(\prod \text{CPO})^{\text{op}}$, and $\psi \in H\sigma\tau(D', E')$ in $\prod \text{CPO}$. Then $\mathcal{H}(\phi, \psi) \in \text{Hom}(\mathcal{H}(D, E), \mathcal{H}(D', E'))$ in $\prod \text{CPO}$ is defined by

  $$\mathcal{H}(\phi, \psi)_\sigma \tau = \text{FS}(\phi_\sigma, \psi_\tau)$$

  $$\mathcal{H}(\phi, \psi) \eta F = \text{GP}(\psi_\eta(a) | a \in \text{Kind } F)$$

  $$\mathcal{H}(\phi, \psi) \Sigma F = \text{GS}(\psi_\eta(a) | a \in \text{Kind } F)$$

  $$\mathcal{H}(\phi, \psi)_l F = \text{GP}(\psi_1(l) | l \in L)$$

  $$\mathcal{H}(\phi, \psi)_L F = \text{GS}(\psi_1(l) | l \in L)$$

Note that $\mathcal{H}$ uses its first argument, which in the definition above is $D$ or $\phi$, in contravariant places, i.e. as first argument of FS. Its second argument is used in all other places. It is easy to check - coordinate-wise - that $\mathcal{H}$ preserves identities and composition, so that it is indeed a functor, and it immediately follows from the definitions of $\mathcal{F}$ and $\mathcal{H}$ that $\mathcal{F}(D) = \mathcal{H}(D, D)$ and $\mathcal{F}(\phi, \psi) = (\mathcal{H}(\psi, \phi), \mathcal{H}(\phi, \psi))$.

It is also easy to prove - again coordinate-wise - that $\mathcal{H}$ is locally continuous. This follows immediately from the fact that FS, GP, and GS are locally continuous.

Then by theorem 8.25 the functor $\mathcal{F}$ is $\omega$-continuous.

Now that we have proved that $(\prod \text{CPO})_{PR}$ is an $\omega$-category and that $\mathcal{F}$ is an $\omega$-continuous functor, by the initial fixpoint theorem (Theorem 8.17) there is an initial fixpoint $(\text{Dom}, (\phi, \psi))$ of $\mathcal{F}$. This fixpoint provides a family of cpos $\text{Dom} = \{\text{Dom}_a | a \in \text{Kind } a\}$ and an $\phi$ and $\psi$ giving an isomorphism between $\text{Dom}$ and $\mathcal{F}(\text{Dom})$. 


8.30 Lemma.
Let \((\text{Dom}, (\phi, \psi))\) be the initial fixpoint of \(F\) in the category \((\prod \text{CPO})_{\text{PH}}\).
Let \(\Phi_{a,b} = \phi_{a-b}, \Phi_F = \phi_{\text{Dom}K_F(a)}, \Phi^X_F = \phi_{H(F(l_1), \ldots, F(l_n))}, \Phi^\mu_F = \phi_{\mu_{\text{Dom}}F(a)}\), etc.
Then \((\text{KIND}_{\text{ERM}}, \text{Dom}, \Phi, \Phi^X, \Phi^\mu)\) is an environment model for \(\lambda \omega^\mu\).

Proof. We have to prove that \(\Gamma \vdash M : \sigma \vdash \eta\) is defined for all \(\Gamma \vdash M : \sigma\) and \(\eta \models \Gamma^\sigma_{\text{ERM}}\).
Recall that this amounts to checking if the ranges of the isomorphisms \(\Phi^{-1}_{\sigma, \eta}\) and \(\Phi_{\eta}\) are large enough. It easy to see that this is the case, because the range of \(\Phi^{-1}_{\sigma, \eta}\) is the collection of all continuous functions from \(\text{ Dom}_{\sigma}\) to \(\text{ Dom}_{\eta}\), and the range of \(\Phi_{\eta}\) is the whole product \(\text{ GP}(\text{Dom}_{F(a)} \mid a \in \text{Kind}_{\text{ERM}})\).

Discussion

The fact that we have used the category CPO is not essential. Other O-categories could be used, for instance the category of directed complete partial orderings (posets with lubs of all directed sets; a set \(S\) is directed if every finite subset of \(S\) has an upper bound in \(S\)) or complete lattices. Types would then be interpreted as directed complete partial orderings or complete lattices.

A drawback of the model we have described is that the interpretations of the polymorphic datatypes are too big, because the cpo \(\text{ Dom} \prod F(a)\) is isomorphic with the whole product \(\prod_a \text{ Dom}_{F(a)}\). This product contains many functions which are not parametric, i.e. which behave in completely different ways when applied to different arguments. For example, the cpo \(\text{ Dom}\{\text{Nat}*, \text{bool}\}\) includes functions that return true or false depending on the type-argument that they get, whereas all closed terms of type \(\text{Nat}*, \text{bool}\) are constant functions. Alternative models which do not have this drawback are the PER-based models described in [AP90] and [BM92], which provide much smaller interpretation of the polymorphic types. In these models \(\text{ Dom}\{\text{Nat}*, \text{bool}\}\) does indeed only contain constant functions.

However, an advantage of the model construction we have described is that it is much simpler. All that is needed for the model construction is the collection of domain equations given by the general model definition. It can easily be extended to include other type-constructions on cpos, such as smashed products and coalesced sums. It can also be extended to incorporate subtyping, as is shown in [PE93].
8.3 The Programming Logic

As in the previous chapters, given any model for the programming language that meets the general model definition, a proof-irrelevance semantics for the associated logic can be defined. In fact, because in $\lambda\omega^+_L$ we have the same logical primitives as in $\lambda\omega^+_L$, the proof-irrelevance model for $\lambda\omega^+_L$ can be defined exactly as it was defined for $\lambda\omega^+_L$ in section 7.3.

Let

$$M = (\text{KIND}, \text{Dom}, \Phi^-, \Phi^P, \Phi^D, \Phi^X, \Phi^+, \Phi^\mu)$$

be any environment model for $\lambda\omega^+_L$. A model for $\lambda\omega^+_L$ in which $M$ is the sub-model for $\lambda\omega^+_L$ can be defined as follows

- the interpretation of the kinds, datatype-constructors and programs is given by $M$, because by lemma 4.37 $\lambda\omega^+_L$ has the same kinds, datatype-constructors and programs as $\lambda\omega^+_L$.

- the interpretation of all other expressions is defined as for $\lambda\omega^+_L$ in section 7.3. So the interpretation of the propkinds is as given in definition 6.33, (in $\lambda\omega^+_L$ propkinds were interpreted as in $\lambda\omega_L$), the interpretation for the prop-constructors is as given in definition 7.24, and all proof terms are interpreted as the element of 1.

The properties proved in section 7.3 for the proof-irrelevance model for $\lambda\omega^+_L$ also hold for this proof-irrelevance model for $\lambda\omega^+_L$, and they can be proved in exactly the same way:

8.31 Theorem (Soundness).

1. Let $\text{der}_1$ and $\text{der}_2$ be derivations of $\Gamma \vdash a : A$ and $\Gamma \vdash a : A'$, respectively. Then

$$[\Gamma \vdash a : A]_\eta = [\Gamma \vdash a : A']_\eta,$$

where the meanings are defined using $\text{der}_1$ and $\text{der}_2$ respectively.

2. If $\Gamma \vdash a : A$, then for all $\eta \models \Gamma$

$$[\Gamma \vdash a : A]_\eta \in \begin{cases} \text{KIND}_A & \text{if } \Gamma \vdash A : \Box_x \\ \text{Dom}(\Gamma \vdash A : \ast_x) & \text{if } \Gamma \vdash A : \ast_x \\ [\Gamma \vdash A : \Box_p]_\eta & \text{if } \Gamma \vdash A : \Box_p \\ [\Gamma \vdash A : \ast_p]_\eta & \text{if } \Gamma \vdash A : \ast_p \end{cases}$$

3. If $a \beta \equiv a'$, $\Gamma \vdash a : A$, and $\Gamma \vdash a' : A$, then $[\Gamma \vdash a : A]_\eta = [\Gamma \vdash a' : A]_\eta$ for all $\eta \models \Gamma$.

As before, the proof-irrelevance model can be used to prove consistency (of contexts)

8.32 Corollary (Consistency of $\lambda\omega^+_L$).

$\lambda\omega^+_L$ is consistent (False is not provable).

8.33 Lemma (Consistency of $\Gamma_{\text{CPO}}$ and $\text{AXIOM}^\mu$ in $\lambda\omega^+_L$).

False is not provable in the context $\Gamma_{\text{CPO}}$ extended with axioms from $\text{AXIOM}^\mu$. 


PROOF. \( \text{[False : \ast_p]} = 0 \), so we supply a model \( M \) for the programming language and show that in the resulting \( \lambda \omega^\mu \)-model there is an environment \( \eta \) that satisfies the context \( \Gamma_{\text{CPO}} \) extended with any axioms from \( AXIOM^n \).

As \( M \) we can take the model constructed in section 8.2.

The environment \( \eta \) should of course interpret the relation \( \subseteq \) (\( \text{Ho} \ast_1 \alpha \rightarrow \alpha \rightarrow \ast_p \)) declared in \( \Gamma_{\text{CPO}} \) as (the characteristic function of) the cpo-ordering in the model, i.e.

\[
\eta(\subseteq) = \forall a \in \text{Kind}_a. \forall x, y \in \text{Dom}_a. \begin{cases} 1 & \text{if } x \subseteq_{\text{Dom}_a} y \\ 0 & \text{if } x \not\subseteq_{\text{Dom}_a} y \end{cases}
\]

\( \in \prod_{a \in \text{Kind}_a} \text{Dom}_a \rightarrow \text{Dom}_a \rightarrow \{0, 1\} \)

With this interpretation of \( \subseteq \), it can then be checked that all the axioms in \( \Gamma_{\text{CPO}} \) and \( AXIOM^n \) are true in the model, i.e. that they are interpreted as 1.

There is an apparent discrepancy between the notion of chain in the model and the notion of chain defined in \( \Gamma_{\text{CPO}} \). In the model \( M \) constructed in section 8.2 all datatypes are \( \omega \)-cpos, which means that chains of the form \( c_0 \subseteq c_1 \subseteq c_2 \subseteq \) have a limit. In \( \Gamma_{\text{CPO}} \) (definition 5.16), on the other hand, a chain is defined as a totally ordered set, and the axiom \( \text{complete} \) in \( \Gamma_{\text{CPO}} \) states that all these chains have limits. However, because all cpos in \( M \) are countable, these two notions of chain are equivalent. \( \square \)
Chapter 9

Conclusion

We now look back on our work, compare it with related work by others, and point out some directions for future research.

9.1 Evaluation

We have investigated the possibility of using type theory as the basis for a typed functional programming language and an associated external programming logic. Three programming logics have been introduced, for three richly-typed functional programming languages of increasing complexity.

The basic system $\lambda\omega_L$ is a small and homogeneous system, which is defined as a single PTS. It provides one language for datatypes, programs, specifications, propositions and proofs, including proofs that programs meet certain specifications. The programming language and the logic are well-matched, because we use a single formalism for both of them. For every abstraction that is possible in the programming language, the logic provides matching abstractions to reason about it. For instance, in the programs we can abstract over all datatypes - $\lambda\alpha \ast_\alpha$ - and in propositions we can quantify over all datatype - $\forall \alpha \ast_\alpha$.

Mechanical verification of proofs in these systems is possible. Verification of proofs amounts to typechecking. The conversion relation in the programming language has to be kept decidable, which does impose some restrictions when the programming language is extended with recursion in chapter 5 (see discussion 5.10).

The logics are all higher-order logics, providing very powerful quantifications. This is useful for an implementation, because without these quantifications many propositions that can be now expressed inside the system would have to be given as schematic rules, and then it would be up to the implementation to provide ways for dealing with the necessary quantifications. There are however occasions where the abstractions that are possible are still not powerful enough. For instance, it is not possible to quantify over all kinds or over all labelled products and sums.

Advantages of using Pure Type Systems

The notion of PTS has proved very useful. By defining the basic system $\lambda\omega_L$ as a PTS, we obtain a lean and elegant system. Also, PTSs are by nature very orthogonal systems. The different kinds of abstraction that are allowed in a PTS can be freely combined.
CHAPTER 9 CONCLUSION

One advantage of using PTSs is that we get some of the syntactic properties for free. However, as proofs of these properties are easy, but boring, induction proofs, we feel this is not the most important advantage. More important is that the compact specifications of PTSs make it easy to compare and relate different systems. This helped to guide the design of the basic system in chapter 3. It is easy to distinguish the \( *_s \)-part of the system that provides the programming language, and the \( *_p \)-part of the system that provides the logic, and the effect of adding a single PTS-rule can be considered. It also helped to prove strong normalisation of the systems. It is easy to observe that strong normalisation of \( \lambda \omega \) and its extension with definitions \( \lambda \omega_L \) immediately follows from strong normalisation of \( \lambda C \), the Calculus of Constructions with definitions.

The fact that DPTSs can easily be compared also provided the key to the proof of strong normalisation for \( \lambda C \), the Calculus of Constructions with definitions. Strong normalisation of this DPTS can easily be deduced from SN of a related PTS (namely ECC).

Advantages of separating programs from proofs

In the introduction we explained the difference between internal and external programming logics, and we motivated our choice for external programming logics: \( \lambda \omega \) and its extensions are all external programming logics. Programs and their correctness proofs are separate but related objects, as are datatypes and specifications. The datatypes express as much information as is possible without making typing undecidable or introducing irrelevant proofs objects in programs. In other words, datatypes express structural information but not logical information. The strict separation between logic and programming language, and the fact that programs and datatypes cannot depend on propositions and proofs, has several advantages.

First, it makes it possible to extend programming language and logic in different directions. For example, in proofs we want to use classical logic and in programs we want to use recursion. The fact that datatypes cannot express logical information makes it possible to have a fixpoint operator for all datatypes (without causing inconsistencies in the logic). The fact that we are not interested in the algorithmic contents of proofs means we can use classical logic.

An example of a further extension of the programming language, which immediately suggests itself once we have labelled products and sums, is subtyping. Subtyping would provide some much-needed flexibility in the type system. It is more difficult to envisage a notion of subtyping in internal programming logics.

The separation between programming language and logic means that for the larger part of the system the semantics can be kept simple. A simple truth-value interpretation can be used for the propositions and their proofs. It also makes it possible to give a conventional denotational semantics for the programming language \( \lambda \omega^n \), which interprets recursion in the usual way.

Pragmatics

We have shown that although they are separate objects, programs and their correctness proofs can be constructed together. This involves a double bookkeeping, of programs and their datatypes on the one hand, and predicates and correctness proofs on the other.

We have shown that for each language construction in the programming language there is not only a typing rule, but there are also -- possibly several -- associated proof rules that
9.2. COMPARISON WITH RELATED WORK

are derivable in the logic. These rules can be used for the top-down, or compositional, development of programs together with their correctness proofs.

The pragmatics of program construction still requires a lot more work. Most of the primitives for program construction offered by \( \lambda \omega \) and its extensions are very primitive indeed. For practical program construction larger building blocks for programs together with their typing and useful proof rules are needed. An example of this is given in chapter 4, where some derivable proof rules are given for a more complicated language construction, namely the abstract-constructive for abstract datatypes.

Apart from these compositional rules, we have also given a few examples of provable equalities between programs. These provide correctness-preserving transformations which can be used to prove that a program meets a certain specification. Examples of simple program transformation rules have been given in chapters 4 and 5. Note that any conditions that have to be satisfied for a transformation to be correct can also be given in the systems.

9.2 Comparison with related work

Several ways of using type theory as a formal basis for programming logics have been proposed. We now compare some of these approaches with ours.

Program Extraction in the Calculus of Constructions

The ongoing work on program extraction from constructive proofs in the Calculus of Constructions and its successor Coq, based on [PM89a], is closely related to our work, at least as far as the type systems that are involved are concerned. In section 3.5 we have already compared the type systems involved in the two approaches. The target language of the extraction procedure is the same programming language provided by \( \lambda \omega \), namely Girard's system \( F' \), or in PTS-terms, the PTS \( \lambda \omega \).

From a pragmatic point of view there is a big difference. Instead of constructing a proof from which a program and its correctness proof are then extracted, we directly construct a program with a correctness proof. In the introduction we already motivated our choice for an external rather than an internal programming logic. An advantage is that the program under construction is clearly visible at all times. Design choices can then be made not only on the basis of the specification, but also on the basis of an operational understanding of the algorithm and efficiency considerations. Also we have the possibility of giving an incomplete specification, or of specifying only a part of the program.

A big difference with our approach is the way recursion is dealt with. As shown in chapter 5, we can extend the programming language with a fixpoint operator for making recursive programs. In the programming language there are then non-terminating programs and partial objects, and domain theory can be used to reason about these.

When the Calculus of Constructions is used as an internal programming logic, a fixpoint operator cannot be added because this would make the system inconsistent. However, the system can be extended with a a well-founded recursor instead of a fixpoint operator. With such a well-founded recursor any recursive program can be constructed, provided a proof is supplied that the recursion is well-founded.

The restriction to well-founded recursion has obvious advantages. All programs terminate and there are no partial functions. For example, this means that there can be a type nat
which contains the natural numbers. If we have a fixpoint operator, any type Nat will also contain a bottom element, and a predicate Nat : Nat \rightarrow \ast_p is needed to characterise the natural numbers. A disadvantage is that there is a mismatch between the programs and datatypes in the programming logic and those available in actual programming languages. For example, in the programming logic it is not possible to reason directly about the datatype of possibly infinite lists as available in lazy functional programming languages.

This difference is a fundamental difference between programming logics where programs cannot depend on proofs and programming logics where programs can depend on proofs. In programming logics where programs cannot depend on proofs, partial functions and objects cannot be avoided if we want more flexible forms of recursion than primitive recursion, or similar fixed recursion patterns for which termination is guaranteed (e.g. [Men87]).

**Deliverables**

Burstall has introduced the name deliverable for a pair consisting of a program and a correctness proof. The approach to program construction using deliverables, discussed in [BM90] [McK92], is similar to ours in spirit. In this approach the system ECC, the Extended Calculus of Constructions [Luo94], is used as an external programming logic for programs in the simply typed lambda calculus.

Our difference with our work is the type systems used for the programming language. Instead of the higher order lambda calculus \( \lambda \omega \) that we use, the simply typed lambda calculus \( \lambda \rightarrow \) is used.

The main difference with our approach is that the strong sum types of ECC are used to form pairs of programs and correctness proofs - deliverables - and pairs of datatypes and predicates - specifications - inside the system ECC. This has the advantage that these pairs can then be manipulated inside the system. Some examples of operations on specifications - i.e. pairs of datatypes and predicates - that can be defined in ECC are given in [Luo94].

Manipulating these pairs inside ECC does impose some restrictions on the shape of programs and specifications. Programs have to be given in a combinatorial notation. It is not immediately possible to express a relation between input and output of functions, but this requires so-called second-order deliverables.

Although the intention is the construction of programs in the simply typed lambda calculus, the system ECC is really much too powerful for this purpose. Also, ECC does not separate the world of programs and datatypes from the world of proofs and propositions in the way that \( \lambda \omega_L \) and its extensions do. The type \( \ast_p \) of all propositions is in fact treated as a datatype. Because of this, it is possible to form programs and datatypes that depend on proofs or propositions. In particular, the specification formed by a datatype and a predicate can again be used as a datatype. This means that the introduction of a fixpoint operator for programs would make the system inconsistent.

**ATTT**

Hayaishi has introduced the programming logic ATTT [Hay93]. The approach to program construction he suggests is also very close to ours. As far as the programming language is concerned, the only difference is that the second order lambda calculus \( \lambda 2 \) is used instead of the higher order lambda calculus \( \lambda \omega \). And as in \( \lambda \omega_L \) in ATTT programs and datatypes
cannot depend on proofs or propositions. Instead of predicates on datatypes, Hayashi uses subsets of datatypes, which are called refinement types.

The possibility of including well-behaved recursive datatypes, such as natural numbers and lists, with primitive recursors is considered. However, the problem of providing more flexible forms of recursion than primitive recursion in the system is not considered.

Using a logical framework

If we are not interested in execution of programs, but just want computer assistance for constructing correct programs, and mechanical verification of proofs, then there is an alternative to implementing $\lambda\omega_L$ (or, indeed, to implementing any of the other theories mentioned above). This alternative is to use a so-called logical framework, such as AUTOMATH [dB80] or Edinburgh LF [HHP93].

These logical frameworks are type theories in which arbitrary formal systems can be represented, for example the programming logic of our choice. We then do not directly interpret certain types as datatypes and others as propositions. Instead, we define representations for programs, datatypes, propositions, and specifications in the logical framework, and supply all the typing rules for programs and all the inference rules for proving propositions. The logical framework then provides support for proving statements in the formal system that has been given, such as "program $M$ has datatype $\sigma$" or "program $M$ satisfies predicate $P$".

There are several differences between implementing $\lambda\omega_L$ directly, and encoding it in a logical framework.

The obvious advantage of the second approach is that an existing implementation can be used. However, the price for this is that the encoding of a formal system in the logical framework makes things more difficult to read and write.

Because we are already interested the $\sigma$-part of $\lambda\omega_L$ by itself, as a typed programming language, it seems preferable not to use a logical framework. The important disadvantage of using a logical framework is namely is that statements such as "program $M$ has datatype $\sigma$" are expressed inside the framework, and have to be (dis)proved using the type inference rules. The whole point of having a typed programming language is that the verification of statements "$\Gamma \vdash M . \sigma$" is left to the type checker, so that we do not have to prove these ourselves.

LCF

In chapter 5 the extension of the programming language with a fixpoint combinator is considered. Domain theory is used as the basis for reasoning about recursive programs in the associated programming logic $\lambda\omega_L^\tau$. This means we reason about recursion in the same way as in LCF [GMW79], [Pau87]. There are however many differences between LCF and $\lambda\omega_L^\tau$. Like the logical frameworks discussed above, LCF does not offer the possibility of executing programs. Also, LCF is only concerned with verification of programs, i.e. with proving that a given program meets a certain specification, and not with the construction of correct programs.

In $\lambda\omega_L^\tau$ programs are explicitly typed, whereas in LCF programs are implicitly typed, in the style of ML. Finally, $\lambda\omega_L^\tau$ provides a much richer logical language than LCF. LCF is a first order logic, and the original definition of LCF in [GMW79] provides conjunction and universal quantification as the only logical connectives, and $\subseteq$ as the only predicate symbol.
\( \lambda \omega_L \) is a higher-order logic, in which predicates are first-class citizens. This has the advantage that many interesting predicates can be defined or declared inside the formal system. For example, we have shown that the notion of admissibility can be expressed in \( \lambda \omega_L \), whereas in LCF this is left to the meta-theory. This additional strength of \( \lambda \omega_L \) makes it possible to build more interesting theories inside the system, in which we no longer have to refer to the cpo-ordering \( \sqsubseteq \) and on the bottom element \( \bot \).

### 9.3 Future Work

As we have already mentioned, a lot more work has to be done to make program construction in \( \lambda \omega_L \) and its extensions practical. The language constructs offered by the type lambda calculi are very primitive, but also very powerful. For practical program construction we want to have more convenient constructs for buildings programs at our disposal, with associated proof rules. We have given a few simple examples of derived constructs, e.g. if-then-else and abstype, and shown how proof rules for them can be obtained. More of such language constructs are needed, with associated proof rules, and possibly some special syntax to keep things readable. In addition to such compositional rules for these constructs, we also want program transformation rules for them which can be used to prove correctness of programs.

In the system with recursion, it is awkward to have to go back to the cpo-ordering \( \sqsubseteq \) every time we want to prove a property of a recursive program. Many recursive programs will follow more or less standard recursion patterns, such as primitive recursion, or recursion on the natural numbers or lists with all recursive calls on smaller natural numbers or shorter lists. For such common recursion patterns we would like to prove termination once and for all, and obtain associated induction rules that can be used to prove properties of programs using that recursion patterns.

The explicit typing in the programming language and the logic results in a large amount of fairly trivial bookkeeping, which is well-suited for machine support by an implementation of the type systems. Such an implementation would offer a programming environment that combines a syntax-directed editor for well-typed programs and a goal-directed proof assistant. Suitable tactics for the construction of programs with then correctness proofs would have to be investigated.

At several places we have introduced special notation for certain language constructs. Sometimes we also omitted type parameters, arguing that these could easily be reconstructed from the context. An implementation should ideally offer such a flexible syntax, with possibilities to introduce new notations and to suppress some of the type information.

A topic for future research are further extensions of the programming language. Cardelli's language Quest [Car89], which is based on \( \lambda \omega \), suggests several possibilities to extend the programming language. Here it is useful that we have a more or less conventional denotational semantics for the programming language, because it can accommodate many extensions.

One important extension is subtyping. As shown in [PHE93], the cpo-model given in chapter 8 can be extended to interpret subtyping. Subtyping makes the type system more flexible. It makes it easy to extend the datastructures used in a program, and hence supports the evolution of programs. Higher-order lambda calculi such as \( \lambda \omega \) extended with subtyping have been used to mimic some of the features of object-oriented programming languages [PT92] [FM94]. By incorporating subtyping in \( \lambda \omega_L \) and its extensions we could investigate suitable logical rules for reasoning about these features.
Bibliography


Index

→-types, 12
→?, 109
for PER-model, 117
+ -types, 60–62, 67–69
+i, 130
for PER-model, 137
× -types, 59, 65 67
×, 130
for PER-model, 137
Π -types, 12
Π i, 109
for PER-model, 117
Σ -types, 62–65
Σ, 130
for PER-model, 137
μ -types, 86
μ, 142
⇔, 35
¬, 35
∀, 34
∀, 119
∃, 35, 76
∃, 139
⇒, 34
⇒, 119
∨, 35, 76
∨, 139
∧, 35, 76
∧, 139
₁, 88
 insecure (type of datatypes), 28
* p (type of propositions), 33
□ x, 28
□ p, 33
 0, 119
 →, 119
e (composition), 84
η ¹ Γ, 126
η ¹ Γ0, 110
η ¹ Γ₀₀, 113
η ¹ Γ₀₀₀, 124
Γ�λ, 35
ΓCPO, 95
for datatype-constructors of λω₂, 110
for datatype-constructors of λω₂⁺, 131
for datatype-constructors of λω₂⁺⁺, 142
for programs of λω₁, 114
for programs of λω₂⁺, 134
for programs of λω₂⁺⁺, 146
for proofs, 126
for prop-constructors of λω₁, 124
for prop-constructors of λω₂⁺⁺, 140
for prop-constructors of λω₂⁺⁺⁺, 157
for prop-kinds of λω₁, 123
for prop-kinds of λω₂⁺⁺, 139
for prop-kinds of λω₂⁺⁺⁺, 157
E (one-step reduction), 11
E (many-step reduction), 11
E (β-reduction), 11
for × -types, 59
for + -types, 62
for Σ -types, 64
for labelled products, 66
for labelled sums, 69
E (β-reduction), 16
E (μ-reduction), 86
≈ (conversion), 11
≈, 11
≈, 16
= (Leibniz' equality of programs), 41
λ → (simply typed λ-calculus), 15
λΣ (second-order typed λ-calculus), 15
λω (higher-order typed λ-calculus), 15
λC (Calculus of Constructions), 15
λC°, 54
INDEX

\( \lambda \omega_s \), 28  
PER-model, 117-119  
general model definition, 108-116

\( \lambda \omega_p \), 33  
proof-irrelevance model, 119-121

\( \lambda \omega_L \), 38  
consistency, 42, 43  
consistency of, 126  
proof-irrelevance model, 122-128

\( \lambda \omega_L^+ \), 71  
PER-model, 137-138  
general model definition, 129-136

\( \lambda \omega_L^\mu \), 76  
consistency, 80  
consistency of, 140  
proof-irrelevance model, 139-140

\( \lambda \omega_P \), 86  
CPO-model, 149-156  
general model definition, 142-148

\( \lambda \omega_P^\mu \), 91  
consistency, 98  
consistency of, 157  
proof-irrelevance model, 157-158

A (PTS-axioms), 10  
abstract datatypes, 72-74  
proof rules for, 82-83  
admissible, 93, 95  
annotation, 44

AXIOM, 42  
consistency of, 128

AXIOM\(^+\), 80  
consistency of, 140

AXIOM\(^\mu\), 97  
consistency of, 157

bool, 71  
bound variables, 10

C (pseudocontextes), 11  
Calculus of Constructions, 1, 2, 4, 54  
Calculus of Constructions (\( \lambda C \)), 15

cartesian product types, 59  
\( \text{case} \), 61

Church numerals, 32  
Church-Rosser

for PTS, 11  
for PTS with \(+, \times \) and \( \Sigma \), 70

for DPTS, 18  
for DPTS with \(+, \times \) and \( \Sigma \), 70  
for \( \lambda \omega_P^\mu \), 89

for \( \lambda \omega_L^\mu \), 90

classical logic, 36, 43

composition, 84

confluence (see Church Rosser), 11

Cons (datatype-constructors)  
for \( \lambda \omega_s \), 30  
for \( \lambda \omega_L^+ \), 74

for \( \lambda \omega_P^\mu \), 88

conservativity  
of DPTS over PTS, 21

of \( \lambda \omega_L \) over \( \lambda \omega_s \), 39

of \( \lambda \omega_L^+ \) over \( \lambda \omega_L^\mu \), 78

of \( \lambda \omega_P^\mu \) over \( \lambda \omega_P^\mu \), 92

consistency  
of AXIOM, 128

of AXIOM\(^+\), 140

of AXIOM\(^\mu\), 157

of \( \Gamma \text{CPO} \), 157

of \( \lambda \omega_P \), 120

of \( \lambda \omega_L \), 42, 43, 126

of \( \lambda \omega_L^+ \), 80, 140

of \( \lambda \omega_P^\mu \), 98, 157

coupled derivation rule, 44

CPO, 150

CR (see Church Rosser)

datatype, 28  
datatype-constructor, 28

dependent sum types, 62-65

disjoint sum types, 60-62

DPTS, 16-23

DPTS with \(+, \times \) and \( \Sigma \), 58-70

elimination of definitions  
for DPTS, 21

for DPTS with \(+, \times \) and \( \Sigma \), 70

for \( \lambda \omega_P^\mu \), 90

eMBEDDING-PROJECTION PAIRS, 152

Empty, 71

environment frame  
for \( \lambda \omega_s \), 113

for \( \lambda \omega_L^+ \), 134
for $\lambda\omega^\mu$, 146
for datatype-constructors of $\lambda\omega^\mu$, 110
for datatype-constructors of $\lambda\omega^\mu_+$, 130
for datatype-constructors of $\lambda\omega^\mu_+$, 142

environment model
for $\lambda\omega$, 114
for $\lambda\omega_+$, 136
for $\lambda\omega^\mu$, 148
for datatype-constructors of $\lambda\omega$, 111
for datatype-constructors of $\lambda\omega_+$, 131
for datatype-constructors of $\lambda\omega^\mu$, 143

extensionality, 43

$F^\omega$ (see $\lambda\omega$), 15
false, 71
False, 35, 76
fixpoint induction, 93, 98
FS, 144, 151
functional (D)PTS, 14
functional (D)PTS with $+, \times$ and $\Sigma$, 58
FV (free variables), 10

global definition, 16
GP, 144, 151
GS, 144, 151

if, 71
kind, 28
Kind (kinds), 30

labelled product types, 65-67
labelled sum types, 67-69
Leibniz' equality, 41
interpretation of, 126
local definition, 16

nat, 88

O-category, 151

PCons (prop-constructors)
for $\lambda\omega_L$, 39
for $\lambda\omega^+_L$, 77

PKind (prop-kinds), 39
PKind_p, 119
poynat, 32
product category, 150
Prog (programs)

for $\lambda\omega$, 30
for $\lambda\omega^+_L$, 74
for $\lambda\omega^+_L$, 88
program, 28
program extraction, 4, 54-56
Proof (proof terms)
for $\lambda\omega_L$, 39
for $\lambda\omega^+_L$, 77
proof, 33
prop-constructor, 33
prop-kind, 33
proposition, 33
PTS, 10 15
PTS with $+, \times$ and $\Sigma$, 58-70

R (PTS-rules), 10
R^+, 58
R^X, 58
R^H, 58
R^E, 58

S (PTS-sorts), 10
second-order typed $\lambda$-calculus ($\lambda\omega$), 15
simply typed $\lambda$-calculus ($\lambda\rightarrow$), 15
SN (see strong normalisation), 14

soundness of $\beta$-conversion
for datatype-constructors of $\lambda\omega$, 112
for datatype-constructors of $\lambda\omega^+_L$, 131
for datatype-constructors of $\lambda\omega^+_L$, 143
for programs of $\lambda\omega$, 116
for programs of $\lambda\omega^+_L$, 136
for programs of $\lambda\omega^+_L$, 148
for $\lambda\omega_L$, 124-126
for $\lambda\omega^+_L$, 140
for $\lambda\omega^+_L$, 157

soundness of type assignment
for datatype-constructors of $\lambda\omega$, 111
for datatype-constructors of $\lambda\omega^+_L$, 131
for datatype-constructors of $\lambda\omega^+_L$, 143
for programs of $\lambda\omega$, 114
for programs of $\lambda\omega^+_L$, 136
for programs of $\lambda\omega^+_L$, 148
for $\lambda\omega_L$, 125-126
for $\lambda\omega^+_L$, 140
for $\lambda\omega^+_L$, 157

specification, 44
specification of (D)PTS, 10
INDEX

specification of (D)PTS with +, \( \times \) and \( \Sigma \), 58

SR (see subject reduction)

strong normalisation (SN), 14
  for \( \delta \)-reduction, 18
  of \( \lambda C \), 15
  of \( \lambda C_{\delta} \), 20
  of \( \lambda \omega_s \), 31
  of \( \lambda \omega_L \), 40
  of \( \lambda \omega_L^+ \), 75
  of \( \lambda \omega_L^- \), 78
  of \( \lambda \omega_L^\mu \), 90

strong sum types, 64-65

subject reduction (SR)
  for PTS, 14
  for PTS with +, \( \times \) and \( \Sigma \), 70
  for DPTS, 19
  for DPTS with +, \( \times \) and \( \Sigma \), 70
  for \( \lambda \omega_s^\mu \), 89
  for \( \lambda \omega_L^\mu \), 90

\( T \) (pseudoterms), 10

true, 71

\( \text{True} \), 35, 76

uniqueness of types (UT)
  for PTS, 14
  for PTS with +, \( \times \) and \( \Sigma \), 70
  for DPTS, 19
  for DPTS with +, \( \times \) and \( \Sigma \), 70
  for \( \lambda \omega_s^\mu \), 89
  for \( \lambda \omega_L^\mu \), 90

unit, 71

\( \text{Unit} \), 71

UT (see uniqueness of types)

weak sum types, 62-65

where, 64
Curriculum Vitae

14 juli 1967 geboren te Haarlemmermeer

mei 1985 diploma International Baccalaureate, International School of London

september 1985 aanvang studie Informatica

april 1990 doctoraal examen Informatica, met lof, Technische Universiteit Eindhoven


vanaf oktober 1994 EuroFocs Fellowship aan INRIA Rocquencourt, Frankrijk

huidig adres
Faculteit Wiskunde en Informatica
Technische Universiteit Eindhoven
Postbus 513
5600 MB Eindhoven
Nederland

e-mail erik@win.ruc.nl
STELLINGEN

behoorende bij het proefschrift

A Programming Logic Based on Type Theory

van

Erik Poll

1 De uitbreiding van het Bruce-Meyer-Mitchell model met Σ-types is niet zo eenvoudig als wordt beweerd in [1] (zie hoofdstuk 7 van dit proefschrift).


2 De in [2] beschreven (co)inductieve types met (co)recursoren kunnen in de polymorfe lambda-calculus Λ2 uitgebreid met inductieve types en primitieve recursoren (beschreven in bijv. [3]) worden gecodeerd.


3 In [4] wordt opgemerkt dat voor de type-constructor "→" subtypering contravariantie vereist en recursieve types covariantie, en dat de combinatie van subtypering en recursieve types hierdoor problematisch lijkt. Bij niet-standaard gebruik van de inverse-limitconstructie zijn deze schijnbaar tegenstrijdige eisen aan → eenvoudig te verenigen (zie [5]).


4. In typering-algoritmen voor Pure Type Systems is het handig om naast het type van een term tegelijkertijd ook het type van dat type te bepalen.


5. Aangezien er meer ervaring is met het ontwikkelen van grote programma's dan met het ontwikkelen van grote formele bewijzen, is het nuttig om bij het ontwerp van bewijstalen te kijken naar faculiteiten die programmeertalen bieden.

6. Bewijzen met inductie zijn vaak goede voorbeelden van bewijzen met intimidatie.

7. Promotie aan een universiteit zou niet direct gevolgd mogen worden door een aanstelling aan dezelfde universiteit.

8. Tekstverwerkers maken het aanbrengen van veranderingen te eenvoudig.

9. Het is jammer dat zowel Griekse hoofdletters ook Latijnse hoofdletters zijn.

10. Het nadeel van computerwerken is dat het afleidingen van agressie op de apparatuur op je bureau minder bevredigend is.