On the Correspondence Between Proofs and λ-Terms

Jean Gallier*
Department of Computer and Information Science
University of Pennsylvania
200 South 33rd St.
Philadelphia, PA 19104, USA
e-mail: jean@saul.cis.upenn.edu

May 5, 1997

Abstract. The correspondence between natural deduction proofs and λ-terms is presented and discussed. A variant of the reducibility method is presented, and a general theorem for establishing properties of typed (first-order) λ-terms is proved. As a corollary, we obtain a simple proof of the Church-Rosser property, and of the strong normalization property, for the typed λ-calculus associated with the system of (intuitionistic) first-order natural deduction, including all the connectors $\rightarrow$, $\times$, $+$, $\forall$, $\exists$, and $\perp$ (falsity) (with or without η-like rules).

*This research was partially supported by ONR Grant NOOO14-88-K-0593.

Contents

1 Introduction

Curry ([2], 1958) made the remarkably insightful observation that certain typed combinators can be viewed as representations of proofs (in a Hilbert system) of certain propositions. Building up on this observation, Howard ([12], 1969) described a general correspondence between propositions and types, proofs in natural deduction and certain typed λ-terms, and proof normalization and β-reduction. This correspondence, usually referred to as the "Curry/Howard isomorphism" or "formulae–as–types principle", is fundamental and very fruitful. The Curry/Howard isomorphism establishes a deep correspondence between the notion of proof and the notion of computation. It is this correspondence that leads to various "semantics of proofs", the most recent one being Girard's geometry of interaction [10]. However, a discussion of this subject would take us beyond the scope of this paper, and we will restrict ourselves to a (thorough) discussion of the notion of proof normalization.

The idea of proof normalization goes back to Gentzen ([6], 1935). Gentzen noted that (formal) proofs can contain redundancies, or "detours", and that most complications in the analysis of proofs are due to these redundancies. Thus, Gentzen had the idea that the analysis of proofs would be simplified if it was possible to show that every proof can be converted to an equivalent irredundant proof, a proof in normal form. Gentzen proved a technical result to that effect, the "cut-elimination theorem", for a sequent-calculus formulation of first-order logic [6]. Cut-free proofs are direct, in the sense that they never use auxiliary lemmas via the cut rule. It is important to note that Gentzen's result gives a particular algorithm to produce a proof in normal form. Thus, we know that every proof can be reduced to some normal form using a specific strategy, but there may be more than one normal form, and certain normalization strategies may not terminate.

About thirty years later, Prawitz ([16], 1965) reconsidered the issue of proof normalization, but in the framework of natural deduction rather than the framework of sequent calculi.[1] Prawitz explained very clearly what redundancies are in systems of natural deduction, and he proved that every proof can be reduced to a normal form. Furthermore, this normal form is unique. A few years later, Prawitz ([17], 1971) showed that in fact, every reduction sequence terminates, a property also called *strong normalization*.

Sometimes between 1965 and 1967, Tait ([20]) proved that β-reduction in the simply-typed λ-calculus is strongly normalizing. For this, he used a method usually known as *reducibility* or *computability*. The word computability already having a meaning in recursion theory, we prefer to use the word reducibility. In view of the Curry-Howard isomorphism (which, although it only appeared in print in 1969, was known to the experts earlier that 1969), it was to be expected that a proof of strong normalization for natural deduction could be obtained using the reducibility method. More specifically, by representing (natural deduction) proofs as certain λ-terms, and exploiting the fact that proof normalization steps correspond to reduction steps in a certain typed λ-calculus, one can translate properties of λ-terms in terms of properties of proofs. In fact, Girard did just that (Girard [8] (1971), [9] (1972)), but he proved a much stronger result, namely strong normalization for higher-order (intuitionistic) logic. A similar proof also appears in Stenlund [19]. Prawitz ([17], 1971) also uses a variant of the reducibility method for proving strong normalization of natural

[1]This is somewhat ironical, since Gentzen began his investigations using a natural deduction system, but decided to switch to sequent calculi (known as Gentzen systems!) for technical reasons.

deduction for first-order intuitionistic logic. Prawitz also proves the confluence (Church-Rosser property) of proof normalization.

The reducibility method is a very powerful method, but it is somewhat mysterious, and it has several variations (Tait's version, Girard's version, Krivine's version, etc). These variations have to do with the choice of technical conditions on the so-called "candidates of reducibility", as we shall see later.

Nowadays, the reducibility method is rather well known for proving strong normalization (or normalization), but the fact that it can also be used to prove confluence or other properties does not seem to be as well known. Statman showed that various properties of the simply-typed λ-calculus can be obtained using logical relations [18], but John Mitchell seems to be one of the first who realized that reducibility can be used to prove more general properties than strong normalization. The general idea is that if a unary predicate $\mathcal{P}$ expressing a property of (typed) λ-terms satisfies the conditions for being a "candidate" (as alluded to earlier) and some other closure conditions (typically, if $\mathcal{P}(Mx)$ then $\mathcal{P}(M)$, where x is a variable), then $\mathcal{P}$ holds of all λ-terms that type-check. Although it is very nice, this approach has a defect, namely that it is too sensitive to the notion of candidate chosen. This makes it difficult to generalize the method when we consider richer calculi. Also, some of the closure conditions are not very "inductive".

Recently, we came accross a paper by Koletsos [13] in which confluence results for various typed λ-calculi are shown. What struck us, is that Koletsos uses a notion of candidate different from all the others, and remarkably, this notion remains the same for all the calculi involved. Furthermore, although specifically tailored for proving confluence, this notion works just as well for strong normalization. In fact, we discovered that it was possible to prove a general theorem about the typed λ-calculus associated with first-order intuitionistic logic. Basically, we show that if a unary predicate $\mathcal{P}$ expressing a property of (typed) λ-terms satisfies certain inductive conditions, then $\mathcal{P}$ holds of all λ-terms that type-check. In particular, strong normalization and confluence satisfy these conditions, and thus they hold in this typed λ-calculus. In constrast to Mitchell's approach, it is not necessary to assert that $\mathcal{P}$ is a candidate. The conditions on $\mathcal{P}$ seem more "inductive".

Our plan is to prove the general theorem about the typed λ-calculus associated with first-order intuitionistic natural deduction. First, we will begin with proof systems in natural deduction style (originally due to Gentzen [6] and thoroughly investigated by Prawitz [16] in the sixties). By adopting a description of natural deduction in terms of judgements, as opposed to the tagged trees used by Gentzen and Prawitz, we are also led quite naturally to the encoding of proofs as certain typed λ-terms, and to the correspondence between proof normalization and β-conversion (the *Curry/Howard isomorphism* [12]). We will then present our version of the reducibity mehod adpated from Koletsos. We will prove our general theorem incrementally, by first considering the simply-typed λ-calculus, and then adding other type constructors in stages.

In writing this paper, we tried to uncover some of the intuitions that may either have been lost or obscured in advanced papers on the subject, but we have also tried to present relatively sophisticated material, because this is more exciting for the reader. Thus, we have assumed that the reader has a certain familiarity with logic and the lambda calculus. If the reader does not feel sufficiently comfortable with these topics, we suggest consulting Girard, Lafont, Taylor [7] or Gallier [4] for background on logic, and Barendregt [1], Hindley and Seldin [11], or Krivine [14] for background on the lambda calculus. For an in-depth study of constructivism in mathematics, we highly recommend Troelstra and van Dalen [22].

2 Natural Deduction, Simply-Typed λ-Calculus

We first consider a syntactic variant of the natural deduction system for implicational propositions due to Gentzen [6] and Prawitz [16].

In the natural deduction system of Gentzen and Prawitz, a deduction consists in deriving a proposition from a finite number of packets of assumptions, using some predefined inference rules. Technically, packets are multisets of propositions. During the course of a deduction, certain packets of assumptions can be "closed", or "discharged". A proof is a deduction such that all the assumptions have been discharged. In order to formalize the concept of a deduction, one faces the problem of describing rigorously the process of discharging packets of assumptions. The difficulty is that one is allowed to discharge any number of occurrences of the same proposition in a single step, and this requires some form of tagging mechanism. At least two forms of tagging techniques have been used.

- The first one, used by Gentzen and Prawitz, consists in viewing a deduction as a tree whose nodes are labeled with propositions (for a lucid presentation, see van Dalen [23]). One is allowed to tag any set of occurrences of some proposition with a natural number, which also tags the inference that triggers the simultaneous discharge of all the occurrences tagged by that number.
- The second solution consists in keeping a record of all undischarged assumptions at every stage of the deduction. Thus, a deduction is a tree whose nodes are labeled with expressions of the form $\Gamma \vdash A$, called *sequents*, where A is a proposition, and Γ is a record of all undischarged assumptions at the stage of the deduction associated with this node.

Although the first solution is perhaps more natural from a human's point of view and more economical, the second one is mathematically easier to handle. In the sequel, we adopt the second solution. It is convenient to tag packets of assumptions with labels, in order to discharge the propositions in these packets in a single step. We use variables for the labels, and a packet labeled with x consisting of occurrences of the proposition A is written as $x\colon A$. Thus, in a sequent $\Gamma \vdash A$, the expression Γ is any finite set of the form $x_1\colon A_1, \ldots, x_m\colon A_m$, where the x_i are pairwise distinct (but the A_i need not be distinct). Given $\Gamma = x_1\colon A_1, \ldots, x_m\colon A_m$, the notation $\Gamma, x\colon A$ is only well defined when $x \neq x_i$ for all i, $1 \leq i \leq m$, in which case it denotes the set $x_1\colon A_1, \ldots, x_m\colon A_m, x\colon A$. We have the following axioms and inference rules.

Definition 2.1 The axioms and inference rules of the system $\mathcal{N}_m^{\supset}$ (implicational logic) are listed below:

$$\Gamma, x\colon A \vdash A$$

$$\frac{\Gamma, x\colon A \vdash B}{\Gamma \vdash A \supset B} \quad (\supset\textit{-intro})$$

$$\frac{\Gamma \vdash A \supset B \quad \Gamma \vdash A}{\Gamma \vdash B} \quad (\supset\textit{-elim})$$

In an application of the rule ($\supset$-*intro*), we say that the proposition A which appears as a hypothesis of the deduction is *discharged* (or *closed*).[2] It is important to note that the ability to label packets consisting of occurrences of the same proposition with different labels is essential, in order to be able to have control over which groups of packets of assumptions are discharged simultaneously. Equivalently, we could avoid tagging packets of assumptions with variables if we assumed that in a sequent $\Gamma \vdash C$, the expression Γ, also called a *context*, is a *multiset* of propositions. The following two examples illustrate this point.

Example 2.2 Let

$$\Gamma = x\colon A \supset (B \supset C), y\colon A \supset B, z\colon A.$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \vdash A \supset (B \supset C) \qquad \Gamma \vdash A}{\Gamma \vdash B \supset C} \qquad \dfrac{\Gamma \vdash A \supset B \qquad \Gamma \vdash A}{\Gamma \vdash B}}{x\colon A \supset (B \supset C), y\colon A \supset B, z\colon A \vdash C}}{x\colon A \supset (B \supset C), y\colon A \supset B \vdash A \supset C}}{x\colon A \supset (B \supset C) \vdash (A \supset B) \supset (A \supset C)}}{\vdash (A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))}$$

In the above example, two occurrences of A are discharged simultaneously. Compare with the example below where these occurrences are discharged in two separate steps.

Example 2.3 Let

$$\Gamma = x\colon A \supset (B \supset C), y\colon A \supset B, z_1\colon A, z_2\colon A.$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \vdash A \supset (B \supset C) \qquad \Gamma \vdash A}{\Gamma \vdash B \supset C} \qquad \dfrac{\Gamma \vdash A \supset B \qquad \Gamma \vdash A}{\Gamma \vdash B}}{x\colon A \supset (B \supset C), y\colon A \supset B, z_1\colon A, z_2\colon A \vdash C}}{x\colon A \supset (B \supset C), y\colon A \supset B, z_1\colon A \vdash A \supset C}}{x\colon A \supset (B \supset C), z_1\colon A \vdash (A \supset B) \supset (A \supset C)}}{z_1\colon A \vdash (A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))}}{\vdash A \supset \big((A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))\big)}$$

For the sake of comparison, we show what these two natural deductions look like in the system of Gentzen and Prawitz, where packets of assumptions discharged in the same inference are tagged with a natural number. Example 2.2 corresponds to the following tree:

[2] In this system, the packet of assumptions A is *always* discharged. This is not so in Prawitz's system (as presented for example in van Dalen [23]), but we also feel that this is a slightly confusing aspect of Prawitz's system.

Example 2.4

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(A \supset (B \supset C))^3 \quad A^1}{B \supset C} \qquad \dfrac{(A \supset B)^2 \quad A^1}{B}}{C}\;1}{A \supset C}\;2}{(A \supset B) \supset (A \supset C)}\;3}{(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))}$$

and Example 2.3 to the following tree:

Example 2.5

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(A \supset (B \supset C))^3 \quad A^1}{B \supset C} \qquad \dfrac{(A \supset B)^2 \quad A^4}{B}}{C}\;1}{A \supset C}\;2}{(A \supset B) \supset (A \supset C)}\;3}{(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))}\;4}{A \supset \big((A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))\big)}$$

It is clear that a context (the Γ in a sequent $\Gamma \vdash A$) is used to tag packets of assumptions and to record the time at which they are discharged. From now on, we stick to the presentation of natural deduction using sequents.

Proofs may contain redundancies, for example when an elimination immediately follows an introduction, as in the following example in which $\mathcal{D}_1$ denotes a deduction with conclusion $\Gamma, x\colon A \vdash B$ and $\mathcal{D}_2$ denotes a deduction with conclusion $\Gamma \vdash A$.

$$\dfrac{\dfrac{\begin{matrix}\mathcal{D}_1 \\ \Gamma, x\colon A \vdash B\end{matrix}}{\Gamma \vdash A \supset B} \qquad \begin{matrix}\mathcal{D}_2 \\ \Gamma \vdash A\end{matrix}}{\Gamma \vdash B}$$

Intuitively, it should be possible to construct a deduction for $\Gamma \vdash B$ from the two deductions $\mathcal{D}_1$ and $\mathcal{D}_2$ without using at all the hypothesis $x\colon A$. This is indeed the case. If we look closely at the deduction $\mathcal{D}_1$, from the shape of the inference rules, assumptions are never created, and the leaves must be labeled with expressions of the form $\Gamma', \Delta, x\colon A, y\colon C \vdash C$ or $\Gamma, \Delta, x\colon A \vdash A$, where

$y \neq x$ and either $\Gamma = \Gamma'$ or $\Gamma = \Gamma', y{:}\,C$. We can form a new deduction for $\Gamma \vdash B$ as follows: in $\mathcal{D}_1$, wherever a leaf of the form $\Gamma, \Delta, x{:}\,A \vdash A$ occurs, replace it by the deduction obtained from $\mathcal{D}_2$ by adding Δ to the premise of each sequent in $\mathcal{D}_2$. Actually, one should be careful to first make a fresh copy of $\mathcal{D}_2$ by renaming all the variables so that clashes with variables in $\mathcal{D}_1$ are avoided. Finally, delete the assumption $x{:}\,A$ from the premise of every sequent in the resulting proof. The resulting deduction is obtained by a kind of substitution and may be denoted as $\mathcal{D}_1[\mathcal{D}_2/x]$, with some minor abuse of notation. Note that the assumptions $x{:}\,A$ occurring in the leaves of the form $\Gamma', \Delta, x{:}\,A, y{:}\,C \vdash C$ were never used anyway. This illustrates the fact that not all assumptions are necessarily used. Also, the same assumption may be used more than once, as we can see in the ($\supset$-*elim*) rule. The step which consists in transforming the above redundant proof figure into the deduction $\mathcal{D}_1[\mathcal{D}_2/x]$ is called a *reduction step* or *normalization step*.

We now show that the simply-typed λ-calculus provides a natural notation for proofs in natural deduction, and that β-conversion corresponds naturally to proof normalization. The trick is to annotate inference rules with terms corresponding to the deductions being built, by placing these terms on the righthand side of the sequent, so that the conclusion of a sequent appears to be the "type of its proof". This way, inference rules have a reading as "type-checking rules". This discovery due to Curry and Howard is known as the *Curry/Howard isomorphism*, or *formulae-as-types principle* [12]. An early occurrence of this correspondence can be found in Curry and Feys [2] (1958), Chapter 9E, pages 312-315. Furthermore, and this is the deepest aspect of the Curry/Howard isomorphism, proof normalization corresponds to term reduction in the λ-calculus associated with the proof system.

Definition 2.6 The type-checking rules of the λ-calculus $\lambda^{\supset}$ (simply-typed λ-calculus) are listed below:

$$\Gamma, x{:}\,A \vdash x{:}\,A$$

$$\frac{\Gamma, x{:}\,A \vdash M{:}\,B}{\Gamma \vdash (\lambda x{:}\,A.\, M){:}\,A \supset B} \quad (\textit{abstraction})$$

$$\frac{\Gamma \vdash M{:}\,A \supset B \qquad \Gamma \vdash N{:}\,A}{\Gamma \vdash (MN){:}\,B} \quad (\textit{application})$$

Now, sequents are of the form $\Gamma \vdash M{:}\,A$, where M is a simply-typed λ-term representing a deduction of A from the assumptions in Γ. Such sequents are also called *judgements*, and Γ is called a *type assignment* or *context*.

The example of redundancy is now written as follows:

$$\frac{\dfrac{\Gamma, x{:}\,A \vdash M{:}\,B}{\Gamma \vdash (\lambda x{:}\,A.\, M){:}\,A \supset B} \qquad \Gamma \vdash N{:}\,A}{\Gamma \vdash (\lambda x{:}\,A.\, M)N{:}\,B}$$

Now, $\mathcal{D}_1$ is incorporated in the deduction as the term M, and $\mathcal{D}_2$ is incorporated in the deduction as the term N. The great bonus of this representation is that $\mathcal{D}_1[\mathcal{D}_2/x]$ corresponds to $M[N/x]$, the result of performing a β-reduction step on $(\lambda x{:}\,A.\, M)N$.

Example 2.7

$$\dfrac{\dfrac{\dfrac{x\colon P \supset (Q \supset P), u\colon P \vdash u\colon P}{x\colon P \supset (Q \supset P) \vdash \lambda u\colon P.\, u\colon (P \supset P)}}{\vdash \lambda x\colon (P \supset (Q \supset P)).\, \lambda u\colon P.\, u\colon (P \supset (Q \supset P)) \supset (P \supset P)} \qquad \dfrac{\dfrac{y\colon P, z\colon Q \vdash y\colon P}{y\colon P \vdash \lambda z\colon Q.\, y\colon (Q \supset P)}}{\vdash \lambda y\colon P.\, \lambda z\colon Q.\, y\colon P \supset (Q \supset P)}}{\vdash (\lambda x\colon (P \supset (Q \supset P)).\, \lambda u\colon P.\, u)\lambda y\colon P.\, \lambda z\colon Q.\, y\colon (P \supset P)}$$

The term $(\lambda x\colon (P \supset (Q \supset P)).\, \lambda u\colon P.\, u)\lambda y\colon P.\, \lambda z\colon Q.\, y$ reduces to $\lambda u\colon P.\, u$, which is indeed the term representation of the natural deduction proof

$$\dfrac{u\colon P \vdash P}{\vdash (P \supset P)}$$

Thus, the simply-typed λ-calculus arises as a natural way to encode natural deduction proofs, and β-reduction corresponds to proof normalization. The correspondence between proof normalization and term reduction is the deepest and most fruitful aspect of the Curry/Howard isomorphism. Indeed, using this correspondence, results about the simply-typed λ-calculus can be translated into the framework of natural deduction proofs, a very nice property. On the other hand, one should not be too dogmatic (or naive) about the Curry/Howard isomorphism and make it into some kind of supreme commandment (as we say in French, "prendre ses désirs pour des réalités"). In the functional style of programming, λ-reduction corresponds to parameter-passing, but more is going on, in particular recursion. Thus, although it is fruitful to view a program as a proof, the specification of a program as the proposition proved by that proof, and the execution of a program as proof normalization (or cut elimination, but it is confusing to say that, since in most cases we are dealing with a natural deduction system), it is abusive to claim that this is what programming is all about. In fact, I believe that statements to that effect are detrimental to our field. There are plenty of smart people who are doing research in the theory of programming and programming language design, and such statements will only make them skeptical (at best). Programming cannot be reduced to the Curry/Howard isomorphism.

When we deal with the calculus $\lambda^{\supset}$, rather than using $\supset$, we usually use $\rightarrow$, and thus, the calculus is denoted as $\lambda^{\rightarrow}$. In order to avoid ambiguities, the delimiter used to separate the lefthand side from the righthand side of a judgement $\Gamma \vdash M\colon A$ will be $\triangleright$, so that judgements are written as $\Gamma \triangleright M\colon A$.

Before moving on to more fascinating topics, we cannot resist a brief digression on notation (at least, we will spare the reader the moralistic lecture that we have inflicted upon students over more than fourteen years!). Notation is supposed to help us, but the trouble is that it can also be a handicap. This is because there is a very delicate balance between the explicit and the implicit. Our philosophy is that the number of symbols used should be minimized, and that notation should *help* remembering what things are, rather than *force* remembering what things are. The most important thing is that notation should be as unambiguous as possible. Furthermore, we should allow ourselves dropping certain symbols as long as no serious ambiguities arise, and we should avoid using symbols that already have a standard meaning, although this is nearly impossible.

Lambda-abstraction and substitution are particularly spicy illustrations. For example, the notation $\lambda x{:}\,\sigma M$ together with (MN) for application is unambiguous. However, when we see the term $(\lambda x{:}\,\sigma MN)$, we have to think a little (in fact, too much) to realize that this is indeed the application of $\lambda x{:}\,\sigma M$ to N, and not the abstraction $\lambda x{:}\,\sigma(MN)$. This is even worse if we look at the term $\lambda x{:}\,\sigma MN$ where the parentheses have been dropped. So, we may consider introducing extra markers, just to help readability, although they are not strictly necessary. For example, we can add a dot between σ and M: abstraction is then written as $\lambda x{:}\,\sigma.\,M$. Similarly, universally quantified formulae are written as $\forall x{:}\,\sigma.\,A$. Now, $\lambda x{:}\,\sigma.\,MN$ is a little better, but still requires an effort. Thus, we will add parentheses around the lambda abstraction and write $(\lambda x{:}\,\sigma.\,M)N$. Yes, we are using more symbols than we really need, but we feel that we have removed the potential confusion with $\lambda x{:}\,\sigma.MN$ (which should really be written as $\lambda x{:}\,\sigma.(MN)$). Since we prefer avoiding subscripts or superscripts unless they are really necessary, we favor the notation $\lambda x{:}\,\sigma.\,M$ over the (slightly old-fashion) $\lambda x^{\sigma}.\,M$ (we do not find the economy of one symbol worth the superscript).[3] Now, let us present another choice of notation, a choice that we consider poor since it forces us to remember something rather than help us. In this choice, abstraction is written as $[x{:}\,\sigma]M$, and universal quantification as $(x{:}\,\sigma)A$. The problem is that the reader needs to remember which kind of bracket corresponds to abstraction or to (universal) quantification. Since additional parentheses are usually added when applications arise, we find this choice quite confusing. The argument that this notation corresponds to some form of machine language is the worst that can be given. Humans are not machines, and thus should not be forced to read machine code! An interesting variation on the notations $\lambda x{:}\,\sigma.\,M$ and $\forall x{:}\,\sigma.\,A$ is $\lambda(x{:}\,\sigma)M$ and $\forall(x{:}\,\sigma)A$, which is quite defendable. Substitution is an even more controversial subject! Our view is the following. After all, a substitution is a function whose domain is a set of variables and which is the identity except on a finite set. Furthermore, substitutions can be composed. But **beware**: composition of substitutions is **not** function composition (indeed, a substitution φ induces a homomorphism $\widehat{\varphi}$, and the composition of two substitutions φ and ψ is the function composition of $\widehat{\varphi}$ and ψ, and **not** of φ and ψ). Thus, the choice of notation for composition of substitutions has an influence on the notation for substitution. If we choose to denote composition of substitution in the order $\varphi\,;\psi$, then it is more convenient to denote the result of applying a substitution φ to a term M as $M\varphi$, or $(M)\varphi$, or as we prefer as $M[\varphi]$. Indeed, this way, $M[\varphi][\psi]$ is equal to $M[\varphi\,;\psi]$. Now, since a substitution is a function with domain a finite set of variables, it can be denoted as $[x_1 \mapsto M_1, \ldots, x_n \mapsto M_n]$. In retrospect, we regret not having adopted this notation. If this was the case, applying a substitution to M would be denoted as $M[x_1 \mapsto M_1, \ldots, x_n \mapsto M_n]$. Instead, we use the notation $[t_1/x_1, \ldots, t_n/x_n]$ which has been used for some time in automated theorem proving. Then, applying a substitution to M is denoted as $M[t_1/x_1, \ldots, t_n/x_n]$ (think for just a second of the horrible clash if this notation was used with $[x{:}\,\sigma]M$ for abstraction!). Other authors denote substitutions as $[x_1{:=}\, M_1, \ldots, x_n{:=}\, M_n]$. Personally, we would prefer switching to $[x_1 \mapsto M_1, \ldots, x_n \mapsto M_n]$, because $:=$ is also used for denoting a function f whose value at some argument x is redefined to be a, as in $f[x{:=}\,a]$. Finally, a word about sequents and judgements. To us, the turnstile symbol $\vdash$ means provability. A sequent consists of two parts Γ and Δ, and some separator is needed between them. In principle, anything can do, and if the arrow $\rightarrow$ was not already used as a type-constructor, we would adopt the notation $\Gamma \rightarrow \Delta$. Some authors denote sequents as $\Gamma \vdash \Delta$. A problem then arises when we want to say that a sequent is provable, since this is written as $\vdash \Gamma \vdash \Delta$. The ideal is to use symbols of different size

[3]The notation $\lambda x^{\sigma}.\,M$ seems to appear mostly in systems where contexts are not used, but instead where it is assumed that each variable has been preassigned a type.

for the two uses of $\vdash$. In fact, we noticed that Girard himself has designed his own $\vdash$ which has a thicker but smaller (in height) foot: $\vdash$. Thus, we will use the "Girardian turnstile" $\vdash$ in writing sequents as $\Gamma \vdash \Delta$. Judgements have three parts, Γ, M, and σ. Our view is that Γ and M actually come together to form what we have called elsewhere a "declared term" (thinking of the context Γ as a declaration of the variables). Again we need a way to put together Γ and M, and we use the symbol $\triangleright$, thus forming $\Gamma \triangleright M$. Then, a declared term may have a type σ, and such a judgement is written as $\Gamma \triangleright M\colon \sigma$. To say that a judgement is provable, we write $\vdash \Gamma \triangleright M\colon \sigma$. We find this less confusing than the notation $\vdash \Gamma \vdash M\colon \sigma$, and this is why we favor $\Gamma \triangleright M\colon \sigma$ over $\Gamma \vdash M\colon \sigma$ (but some authors use $\triangleright$ for the reduction relation! We use $\longrightarrow$). And please, avoid the notation $\vdash \Gamma \vdash M \in \sigma$, which we find terribly confusing and cruel to $\in$. But we have indulged too long into this digression, and now back to more serious business.

3 Adding Conjunction, Negation, and Disjunction

First, we present the natural deduction systems, and then the corresponding extensions of the simply-typed λ-calculus. As far as proof normalization is concerned, conjunction does not cause any problem, but as we will see, negation and disjunction are more problematic. In order to add negation, we add the new constant $\perp$ (**false**) to the language, and define negation $\neg A$ as an abbreviation for $A \supset \perp$.

Definition 3.1 The axioms and inference rules of the system $\mathcal{N}_i^{\supset,\wedge,\vee,\perp}$ (intuitionistic propositional logic) are listed below:

$$\Gamma, x\colon A \vdash A$$

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A} \quad (\perp\text{-}elim)$$

$$\frac{\Gamma, x\colon A \vdash B}{\Gamma \vdash A \supset B} \quad (\supset\text{-}intro)$$

$$\frac{\Gamma \vdash A \supset B \quad \Gamma \vdash A}{\Gamma \vdash B} \quad (\supset\text{-}elim)$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \quad (\wedge\text{-}intro)$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \quad (\wedge\text{-}elim) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \quad (\wedge\text{-}elim)$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \quad (\vee\text{-}intro) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \quad (\vee\text{-}intro)$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, x\colon A \vdash C \quad \Gamma, y\colon B \vdash C}{\Gamma \vdash C} \quad (\vee\text{-}elim)$$

Since the rule ($\bot$-*elim*) is trivial (does nothing) when $A = \bot$, from now on, we will assume that $A \neq \bot$. *Minimal propositional logic* $\mathcal{N}_m^{\supset,\wedge,\vee,\bot}$ is obtained by dropping the ($\bot$-*elim*) rule. In order to obtain the system of *classical propositional logic*, denoted $\mathcal{N}_c^{\supset,\wedge,\vee,\bot}$, we add to $\mathcal{N}_m^{\supset,\wedge,\vee,\bot}$ the following inference rule corresponding to the principle of proof by contradiction (*by-contra*) (also called *reductio ad absurdum*).

$$\frac{\Gamma, x\colon \neg A \vdash \bot}{\Gamma \vdash A} \quad (\textit{by-contra})$$

Several useful remarks should be made.

(1) In classical propositional logic ($\mathcal{N}_c^{\supset,\wedge,\vee,\bot}$), the rule

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A} \quad (\bot\text{-}\textit{elim})$$

can be derived, since if we have a deduction of $\Gamma \vdash \bot$, then for any arbitrary A we have a deduction $\Gamma, x\colon \neg A \vdash \bot$, and thus a deduction of $\Gamma \vdash A$ by applying the (*by-contra*) rule.

(2) The proposition $A \supset \neg\neg A$ is derivable in $\mathcal{N}_m^{\supset,\wedge,\vee,\bot}$, but the reverse implication $\neg\neg A \supset A$ is not derivable, even in $\mathcal{N}_i^{\supset,\wedge,\vee,\bot}$. On the other hand, $\neg\neg A \supset A$ is derivable in $\mathcal{N}_c^{\supset,\wedge,\vee,\bot}$:

$$\dfrac{\dfrac{\dfrac{x\colon \neg\neg A, y\colon \neg A \vdash \neg\neg A \qquad x\colon \neg\neg A, y\colon \neg A \vdash \neg A}{x\colon \neg\neg A, y\colon \neg A \vdash \bot}}{x\colon \neg\neg A \vdash A}\ (\textit{by-contra})}{\vdash \neg\neg A \supset A}$$

(3) Using the (*by-contra*) inference rule together with ($\supset$-*elim*) and ($\vee$-*intro*), we can prove $\neg A \vee A$ (that is, $(A \supset \bot) \vee A$). Let

$$\Gamma = x\colon ((A \supset \bot) \vee A) \supset \bot\ .$$

We have the following proof for $(A \supset \bot) \vee A$ in $\mathcal{N}_c^{\supset,\wedge,\vee,\bot}$:

$$\dfrac{\dfrac{\Gamma \vdash ((A \supset \bot) \vee A) \supset \bot \qquad \dfrac{\dfrac{\dfrac{\Gamma, y\colon A \vdash ((A \supset \bot) \vee A) \supset \bot \quad \dfrac{\Gamma, y\colon A \vdash A}{\Gamma, y\colon A \vdash (A \supset \bot) \vee A}}{\Gamma, y\colon A \vdash \bot}}{\Gamma \vdash A \supset \bot}}{\Gamma \vdash (A \supset \bot) \vee A}}{\Gamma \vdash \bot}}{\vdash (A \supset \bot) \vee A}\ (\textit{by-contra})$$

As in (2), $\neg A \vee A$ is not derivable in $\mathcal{N}_i^{\supset,\wedge,\vee,\bot}$. The reader might wonder how one shows that $\neg\neg A \supset A$ and $\neg A \vee A$ are not provable in $\mathcal{N}_i^{\supset,\wedge,\vee,\bot}$. In fact, this is not easy to prove directly. One method is to use the fact (given by theorem 3.4 and theorem 3.5) that every proof-term reduces to a unique normal form. Then, argue that if the above propositions have a proof in normal form, this leads to a contradiction. Another even simpler method is to use cut-free Gentzen systems. The interested reader is referred to Gallier [3].

The typed λ-calculus $\lambda^{\to,\times,+,\perp}$ corresponding to $\mathcal{N}_i^{\supset,\wedge,\vee,\perp}$ is given in the following definition.

Definition 3.2 The typed λ-calculus $\lambda^{\to,\times,+,\perp}$ is defined by the following rules.

$$\Gamma, x\colon A \rhd x\colon A$$

$$\frac{\Gamma \rhd M\colon \perp}{\Gamma \rhd \nabla_A(M)\colon A} \quad (\perp\textit{-elim})$$

with $A \neq \perp$,

$$\frac{\Gamma, x\colon A \rhd M\colon B}{\Gamma \rhd (\lambda x\colon A.\, M)\colon A \to B} \quad (\textit{abstraction})$$

$$\frac{\Gamma \rhd M\colon A \to B \quad \Gamma \rhd N\colon A}{\Gamma \rhd (MN)\colon B} \quad (\textit{application})$$

$$\frac{\Gamma \rhd M\colon A \quad \Gamma \rhd N\colon B}{\Gamma \rhd \langle M, N\rangle\colon A \times B} \quad (\textit{pairing})$$

$$\frac{\Gamma \rhd M\colon A \times B}{\Gamma \rhd \pi_1(M)\colon A} \quad (\textit{projection}) \qquad \frac{\Gamma \rhd M\colon A \times B}{\Gamma \rhd \pi_2(M)\colon B} \quad (\textit{projection})$$

$$\frac{\Gamma \rhd M\colon A}{\Gamma \rhd \mathtt{inl}(M)\colon A + B} \quad (\textit{injection}) \qquad \frac{\Gamma \rhd M\colon B}{\Gamma \rhd \mathtt{inr}(M)\colon A + B} \quad (\textit{injection})$$

$$\frac{\Gamma \rhd P\colon A + B \quad \Gamma, x\colon A \rhd M\colon C \quad \Gamma, y\colon B \rhd N\colon C}{\Gamma \rhd \mathtt{case}(P, \lambda x\colon A.\, M, \lambda y\colon B.\, N)\colon C} \quad (\textit{by-cases})$$

A syntactic variant of $\mathtt{case}(P, \lambda x\colon A.\, M, \lambda y\colon B.\, N)$ often found in the literature is

$$\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon A) \Rightarrow M \mid \mathtt{inr}(y\colon B) \Rightarrow N,$$

or even

$$\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x) \Rightarrow M \mid \mathtt{inr}(y) \Rightarrow N,$$

and the (*by-cases*) rule can be written as

$$\frac{\Gamma \rhd P\colon A + B \quad \Gamma, x\colon A \rhd M\colon C \quad \Gamma, y\colon B \rhd N\colon C}{\Gamma \rhd (\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon A) \Rightarrow M \mid \mathtt{inr}(y\colon B) \Rightarrow N)\colon C} \quad (\textit{by-cases})$$

We also have the following reduction rules.

Definition 3.3 The reduction rules of the system $\lambda^{\rightarrow,\times,+,\perp}$ are listed below:

$$
\begin{aligned}
(\lambda x{:}\,A.\,M)N &\longrightarrow M[N/x],\\
\pi_1(\langle M,N\rangle) &\longrightarrow M,\\
\pi_2(\langle M,N\rangle) &\longrightarrow N,\\
\texttt{case}(\texttt{inl}(P),\lambda x{:}\,A.\,M,\lambda y{:}\,B.\,N) &\longrightarrow M[P/x], \quad \text{or}\\
\texttt{case inl}(P)\ \texttt{of inl}(x{:}\,A) \Rightarrow M \mid \texttt{inr}(y{:}\,B) \Rightarrow N &\longrightarrow M[P/x],\\
\texttt{case}(\texttt{inr}(P),\lambda x{:}\,A.\,M,\lambda y{:}\,B.\,N) &\longrightarrow N[P/y], \quad \text{or}\\
\texttt{case inr}(P)\ \texttt{of inl}(x{:}\,A) \Rightarrow M \mid \texttt{inr}(y{:}\,B) \Rightarrow N &\longrightarrow N[P/y],\\
\bigtriangledown_{A\rightarrow B}(M)N &\longrightarrow \bigtriangledown_B(M),\\
\pi_1(\bigtriangledown_{A\times B}(M)) &\longrightarrow \bigtriangledown_A(M),\\
\pi_2(\bigtriangledown_{A\times B}(M)) &\longrightarrow \bigtriangledown_B(M),\\
\texttt{case}(\bigtriangledown_{A+B}(P),\lambda x{:}\,A.\,M,\lambda y{:}\,B.\,N) &\longrightarrow \bigtriangledown_C(P).
\end{aligned}
$$

A fundamental result about natural deduction is the fact that every proof (term) reduces to a normal form, which is unique up to α-renaming. This result was first proved by Prawitz [17] for the system $\mathcal{N}_i^{\supset,\wedge,\vee,\perp}$.

Theorem 3.4 [Church-Rosser property, Prawitz (1971)] *Reduction in $\lambda^{\rightarrow,\times,+,\perp}$ (specified in Definition 3.3) is confluent. Equivalently, conversion in $\lambda^{\rightarrow,\times,+,\perp}$ is Church-Rosser.*

A proof can be given by adapting the method of Tait and Martin-Löf [15] using a form of parallel reduction (see also Barendregt [1], Hindley and Seldin [11], or Stenlund [19]). We will give another proof in section 8.

Theorem 3.5 [Strong normalization, Prawitz (1971)] *Reduction in $\lambda^{\rightarrow,\times,+,\perp}$ (as in Definition 3.3) is strongly normalizing.*

A proof can be given by adapting Tait's reducibility method [20], [21], as done in Girard [8] (1971), [9] (1972) (see also Gallier [5]). We will give another proof in section 8.

4 First-Order Quantifiers

We extend the system $\mathcal{N}_i^{\supset,\wedge,\vee,\perp}$ to deal with the quantifiers.

Definition 4.1 The axioms and inference rules of the system $\mathcal{N}_i^{\supset,\wedge,\vee,\forall,\exists,\perp}$ for intuitionistic first-order logic are listed below:

$$\Gamma, x{:}\,A \vdash A$$

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A}\quad (\perp\text{-}elim)$$

with $A \neq \perp$,

$$\frac{\Gamma, x{:}\,A \vdash B}{\Gamma \vdash A \supset B}\quad (\supset\text{-}intro)$$

$$\frac{\Gamma \vdash A \supset B \quad \Gamma \vdash A}{\Gamma \vdash B} \quad (\supset\text{-}elim)$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \quad (\wedge\text{-}intro)$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \quad (\wedge\text{-}elim) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \quad (\wedge\text{-}elim)$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \quad (\vee\text{-}intro) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \quad (\vee\text{-}intro)$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, x: A \vdash C \quad \Gamma, y: B \vdash C}{\Gamma \vdash C} \quad (\vee\text{-}elim)$$

$$\frac{\Gamma \vdash A[u/t]}{\Gamma \vdash \forall t A} \quad (\forall\text{-}intro) \qquad \frac{\Gamma \vdash \forall t A}{\Gamma \vdash A[\tau/t]} \quad (\forall\text{-}elim)$$

where in ($\forall$-*intro*), u does not occur free in Γ or $\forall t A$;

$$\frac{\Gamma \vdash A[\tau/t]}{\Gamma \vdash \exists t A} \quad (\exists\text{-}intro) \qquad \frac{\Gamma \vdash \exists t A \quad z: A[u/t], \Gamma \vdash C}{\Gamma \vdash C} \quad (\exists\text{-}elim)$$

where in ($\exists$-*elim*), u does not occur free in Γ, $\exists t A$, or C.

The variable u is called the *eigenvariable* of the inference.

One should observe that we are now using two kinds of variables: term (or package) variables $(x, y, z, \ldots)$, and individual (or type) variables $(t, u, \ldots)$.

The typed λ-calculus $\lambda^{\rightarrow,\times,+,\forall,\exists,\perp}$ corresponding to $\mathcal{N}_i^{\supset,\wedge,\vee,\forall,\exists,\perp}$ is given in the following definition.

Definition 4.2 The typed λ-calculus $\lambda^{\rightarrow,\times,+,\forall,\exists,\perp}$ is defined by the following rules.

$$\Gamma, x: A \triangleright x: A$$

$$\frac{\Gamma \triangleright M: \perp}{\Gamma \triangleright \nabla_A(M): A} \quad (\perp\text{-}elim)$$

with $A \neq \perp$,

$$\frac{\Gamma, x: A \triangleright M: B}{\Gamma \triangleright (\lambda x: A.\, M): A \rightarrow B} \quad (abstraction)$$

$$\frac{\Gamma \triangleright M: A \rightarrow B \quad \Gamma \triangleright N: A}{\Gamma \triangleright (MN): B} \quad (application)$$

$$\frac{\Gamma \triangleright M: A \quad \Gamma \triangleright N: B}{\Gamma \triangleright \langle M, N\rangle: A \times B} \quad (pairing)$$

$$\frac{\Gamma \triangleright M\colon A \times B}{\Gamma \triangleright \pi_1(M)\colon A} \quad (\textit{projection}) \qquad \frac{\Gamma \triangleright M\colon A \times B}{\Gamma \triangleright \pi_2(M)\colon B} \quad (\textit{projection})$$

$$\frac{\Gamma \triangleright M\colon A}{\Gamma \triangleright \mathtt{inl}(M)\colon A + B} \quad (\textit{injection}) \qquad \frac{\Gamma \triangleright M\colon B}{\Gamma \triangleright \mathtt{inr}(M)\colon A + B} \quad (\textit{injection})$$

$$\frac{\Gamma \triangleright P\colon A + B \quad \Gamma, x\colon A \triangleright M\colon C \quad \Gamma, y\colon B \triangleright N\colon C}{\Gamma \triangleright \mathtt{case}(P, \lambda x\colon A.\ M, \lambda y\colon B.\ N)\colon C} \quad (\textit{by-cases})$$

or

$$\frac{\Gamma \triangleright P\colon A + B \quad \Gamma, x\colon A \triangleright M\colon C \quad \Gamma, y\colon B \triangleright N\colon C}{\Gamma \triangleright (\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon A) \Rightarrow M \mid \mathtt{inr}(y\colon B) \Rightarrow N)\colon C} \quad (\textit{by-cases})$$

$$\frac{\Gamma \triangleright M\colon A[u/t]}{\Gamma \triangleright (\lambda u\colon \iota.\ M)\colon \forall t A} \quad (\forall\textit{-intro})$$

where u does not occur free in Γ or $\forall t A$;

$$\frac{\Gamma \triangleright M\colon \forall t A}{\Gamma \triangleright M\tau\colon A[\tau/t]} \quad (\forall\textit{-elim})$$

$$\frac{\Gamma \triangleright M\colon A[\tau/t]}{\Gamma \triangleright \mathtt{inx}(\tau, M)\colon \exists t A} \quad (\exists\textit{-intro})$$

$$\frac{\Gamma \triangleright M\colon \exists t A \quad \Gamma, x\colon A[u/t] \triangleright N\colon C}{\Gamma \triangleright \mathtt{casex}(M, \lambda u\colon \iota.\ \lambda x\colon A[u/t].\ N)\colon C} \quad (\exists\textit{-elim})$$

where u does not occur free in Γ, $\exists t A$, or C.

In the term $(\lambda u\colon \iota.\ M)$, the type ι stands for the type of individuals. Note that

$$\Gamma \triangleright \lambda u\colon \iota.\ \lambda x\colon A[u/t].\ N\colon \forall u(A[u/t] \to C).$$

The term $\lambda u\colon \iota.\ \lambda x\colon A[u/t].\ N$ contains the type $A[u/t]$ which is a *dependent* type, since it usually contains occurrences of u. Observe that $(\lambda u\colon \iota.\ \lambda x\colon A[u/t].\ N)\tau$ reduces to $\lambda x\colon A[\tau/t].\ N[\tau/u]$, in which the type of x is now $A[\tau/t]$. The term $\mathtt{casex}(M, \lambda u\colon \iota.\ \lambda x\colon A[u/t].\ N)$ is also denoted as $\mathtt{casex}\ M\ \mathtt{of}\ \mathtt{inx}(u\colon \iota, x\colon A[u/t]) \Rightarrow N$, or even $\mathtt{casex}\ M\ \mathtt{of}\ \mathtt{inx}(u, x) \Rightarrow N$, and the $(\exists\textit{-elim})$ rule as

$$\frac{\Gamma \triangleright M\colon \exists t A \quad \Gamma, x\colon A[u/t] \triangleright N\colon C}{\Gamma \triangleright (\mathtt{casex}\ M\ \mathtt{of}\ \mathtt{inx}(u\colon \iota, x\colon A[u/t]) \Rightarrow N)\colon C} \quad (\exists\textit{-elim})$$

where u does not occur free in Γ, $\exists t A$, or C.

Such a formalism can be easily generalized to many sorts (base types), if quantified formulae are written as $\forall t\colon \sigma.\ A$ and $\exists t\colon \sigma.\ A$, where σ is a sort (base type). A further generalization would be to allow higher-order quantification as in Girard's system F_ω (see Girard [9] or Gallier [5]). We also have the following reduction rules.

Definition 4.3 The reduction rules of the system $\lambda^{\rightarrow,\times,+,\forall,\exists,\perp}$ are listed below:

$$
\begin{aligned}
(\lambda x\colon A.\, M)N &\longrightarrow M[N/x],\\
\pi_1(\langle M, N\rangle) &\longrightarrow M,\\
\pi_2(\langle M, N\rangle) &\longrightarrow N,\\
\texttt{case}(\texttt{inl}(P), M, N) &\longrightarrow MP, \quad \text{or}\\
\texttt{case inl}(P)\ \texttt{of inl}(x\colon A) \Rightarrow M \mid \texttt{inr}(y\colon B) \Rightarrow N &\longrightarrow M[P/x],\\
\texttt{case}(\texttt{inr}(P), M, N) &\longrightarrow NP, \quad \text{or}\\
\texttt{case inr}(P)\ \texttt{of inl}(x\colon A) \Rightarrow M \mid \texttt{inr}(y\colon B) \Rightarrow N &\longrightarrow N[P/y],\\
\nabla_{A\rightarrow B}(M)N &\longrightarrow \nabla_B(M),\\
\pi_1(\nabla_{A\times B}(M)) &\longrightarrow \nabla_A(M),\\
\pi_2(\nabla_{A\times B}(M)) &\longrightarrow \nabla_B(M),\\
(\lambda t\colon \iota.\, M)\tau &\longrightarrow M[\tau/t],\\
\nabla_{\forall tA}(M)\tau &\longrightarrow \nabla_{A[\tau/t]}(M),\\
\texttt{case}(\nabla_{A+B}(P), M, N) &\longrightarrow \nabla_C(P),\\
\texttt{casex}(\texttt{inx}(\tau, P), M) &\longrightarrow (M\tau)P, \quad \text{or}\\
\texttt{casex inx}(\tau, P)\ \texttt{of inx}(t\colon \iota, x\colon A) \Rightarrow N &\longrightarrow N[\tau/t, P/x],\\
\texttt{casex}(\nabla_{\exists tA}(P), M) &\longrightarrow \nabla_C(P).
\end{aligned}
$$

A fundamental result about natural deduction is the fact that every proof (term) reduces to a normal form, which is unique up to α-renaming. This result was first proved by Prawitz [17] for the system $\mathcal{N}_i^{\supset,\wedge,\vee,\forall,\exists,\perp}$.

Theorem 4.4 [Church-Rosser property, Prawitz (1971)] *Reduction in $\lambda^{\rightarrow,\times,+,\forall,\exists,\perp}$ (specified in Definition 4.3) is confluent. Equivalently, conversion in $\lambda^{\rightarrow,\times,+,\forall,\exists,\perp}$ is Church-Rosser.*

A proof can be given by adapting the method of Tait and Martin-Löf [15] using a form of parallel reduction (see also Barendregt [1], Hindley and Seldin [11], or Stenlund [19]). We will give another proof in section 8.

Theorem 4.5 [Strong normalization, Prawitz (1971)] *Reduction in $\lambda^{\rightarrow,\times,+,\forall,\exists,\perp}$ is strongly normalizing.*

A proof can be given by adapting Tait's reducibility method [20], [21], as done in Girard [8] (1971), [9] (1972) (see also Gallier [5]). We will give another proof in section 8.

If one looks carefully at the structure of proofs, one realizes that it is not unreasonable to declare other proofs as being redundant, and thus to add some additional reduction rules. For example, the proof term $\langle \pi_1(M), \pi_2(M)\rangle$ can be identified with M itself. Similarly, if x is not free in M, the term $\lambda x\colon A.\,(Mx)$ can be identified with M. Thus, we have the following additional set of reduction rules:

$$
\begin{aligned}
\lambda x\colon A.\,(Mx) &\longrightarrow M, \qquad \text{if } x \notin FV(M),\\
\langle \pi_1(M), \pi_2(M)\rangle &\longrightarrow M,
\end{aligned}
$$

$$\begin{aligned}
\texttt{case}\ M\ \texttt{of}\ \texttt{inl}(x\colon A) \Rightarrow \texttt{inl}(x) \mid \texttt{inr}(y\colon B) \Rightarrow \texttt{inr}(y) &\longrightarrow M, \\
\lambda t\colon \iota.\,(Mt) &\longrightarrow M, \qquad \text{if } t \notin FV(M), \\
\texttt{casex}\ M\ \texttt{of}\ \texttt{inx}(u\colon \iota, x\colon A[u/t]) \Rightarrow \texttt{inx}(u,x) &\longrightarrow M, \qquad \text{if } u \notin FV(M).
\end{aligned}$$

These rules are important in setting up categorical semantics for intuitionistic logic. However, a discussion of this topic would take us far beyond the scope of this paper. Actually, in order to salvage some form of subformula property ruined by the introduction of the connectives $\vee$, $\exists$, and $\perp$, one can add further conversions known as "commuting conversions" (or "permutative conversions"). A lucid discussion of the necessity for such rules can be found in Girard [7]. Theorem 4.4 and theorem 4.5 can be extended to cover the reduction rules of definition 4.3 together with the new reductions rules, but at the cost of rather tedious and rather noninstructive technical complications. Due to the lack of space, we will not elaborate any further on this subject and simply refer the interested reader to Prawitz [16], Girard [9], or Girard [7] for details.

5 $\mathcal{P}$-Candidates for the Arrow Type Constructor $\rightarrow$

We first motivate our version of the reducibility method. The situation is that we have a unary predicate $\mathcal{P}$ describing a property of (typed) λ-terms, and a type-inference system $\mathcal{S}$. For example, $\mathcal{P}$ could be the property of being normalizable, or strongly normalizing, or that confluence holds from any term, and $\mathcal{S}$ could be the system $\lambda^{\rightarrow}$, or $\lambda^{\rightarrow,\times,+,\perp}$, or $\lambda^{\rightarrow,\times,+,\forall,\exists,\perp}$. Our main goal is to find sufficient conditions on the predicate $\mathcal{P}$ so that every term M that type-checks in $\mathcal{S}$ satisfies the predicate $\mathcal{P}$.

As an example of the above general schema, conditions (P1), (P2), (P3) of definition 5.3 together with conditions (P4) and (P5) of definition 5.7 are such conditions on $\mathcal{P}$ with respect to system $\lambda^{\rightarrow}$ (see theorem 5.10). Another example is given by conditions (P1), (P2), (P3) of definition 8.4 together with conditions (P4) and (P5) of definition 8.8 with respect to system $\lambda^{\rightarrow,\times,+,\forall,\exists,\perp}$ (see theorem 8.11). Since the property of being strongly normalizing satisfies properties (P1)-(P5), as a corollary, we have that every term that type-checks in $\lambda^{\rightarrow,\times,+,\forall,\exists,\perp}$ is strongly normalizing (see theorem 8.12). Similarly, we obtain that confluence holds (see theorem 8.13).

The main technique involved is a kind of realizability argument known as *reducibility*. The crux of the reducibility method is to interpret every type σ as a set $[\![\sigma]\!]$ of λ-terms having certain closure properties. One of the crucial properties is that for any type σ, the terms in $[\![\sigma]\!]$ satisfy the predicate $\mathcal{P}$. If the sets $[\![\sigma]\!]$ are defined right, then the following "realizability property" holds (for example, see lemma 5.9):

If $\mathcal{P}$ is a predicate satisfying conditions (P1)-(P5), then for every term M that type-checks in $\lambda^{\rightarrow}$ with type σ, for every substitution φ such that $\varphi(y) \in [\![\gamma]\!]$ for every $y\colon\gamma \in FV(M)$, we have $M[\varphi] \in [\![\sigma]\!]$.

Now, if the properties (P1)-(P5) on the predicate $\mathcal{P}$ are right, every variable is in every $[\![\sigma]\!]$, and thus, by chosing φ to be the identity substitution, we get that $M \in [\![\sigma]\!]$ whenever M type-checks in $\lambda^{\rightarrow}$ with type σ. Furthermore, properties (P1)-(P5) imply that $[\![\sigma]\!] \subseteq \mathcal{P}$, and thus, we have shown that M satisfies the predicate $\mathcal{P}$ whenever M type-checks in $\lambda^{\rightarrow}$.

Other examples of this schema are given by lemma 6.10, lemma 7.10, and lemma 8.10. In order for an argument of this kind to go through, the sets $[\![\sigma]\!]$ must satisfy some inductive invariant. In the literature, this is often referred to as being a *candidate*. Inspired by the paper by Koletsos [13], we use the notion of a $\mathcal{P}$-candidate defined in definition 5.4. This notion has the advantage of not requiring the terms to be strongly normalizing (as in Girard [7]), or to involve rather strange looking terms such as $M[N/x]N_1 \ldots N_k$ (as in Tait, Mitchell, or Krivine). By isolating the dual notions of I-terms and simple terms, we can give a definition that remains *invariant* no matter what the definition of the sets $[\![\sigma]\!]$ is. Also, the definition of a $\mathcal{P}$-candidate only requires that the predicate $\mathcal{P}$ be satisfied, but nothing to do with the properties (P1)-(P5) on $\mathcal{P}$. This separation is helpful in understanding how to derive sufficient properties on $\mathcal{P}$. In other presentations, properties of the predicate $\mathcal{P}$ are often incorporated in the definition of a candidate, and this tends to obscure the argument. Finally, our definition can be easily adapted to other type disciplines (conjunctive types), or to higher-order types. Also, nice proofs of confluence can be obtained (see theorem 8.13). We now proceed with the details.

Let $\mathcal{T}$ denote the set of (simple) types. The presentation will be simplified if we adopt the definition of simply-typed λ-terms where all the variables are explicitly assigned types once and for all. More precisely, we have a family $\mathcal{X} = (X_\sigma)_{\sigma \in \mathcal{T}}$ of variables, where each X_σ is a countably infinite set of variables of type σ, and $X_\sigma \cap X_\tau = \emptyset$ whenever $\sigma \neq \tau$. Using this definition, there is no need to drag contexts along, and the most important feature of the proof, namely the reducibility method, is easier to grasp. The type-checking rules of the system are summarized in the following definition.

Definition 5.1 The terms of the typed λ-calculus $\lambda^{\to}$ are defined by the following rules.

$$x\colon \sigma, \quad \text{when } x \in X_\sigma,$$

(we can also have $c\colon \sigma$, for a set of constants that have been preassigned types).

$$\frac{x\colon \sigma \rhd M\colon \tau}{\rhd (\lambda x\colon \sigma.\, M)\colon \sigma \to \tau} \quad (abstraction)$$

$$\frac{\rhd M\colon \sigma \to \tau \qquad \rhd N\colon \sigma}{\rhd (MN)\colon \tau} \quad (application)$$

From now on, when we refer to a λ-term, we mean a λ-term that type-checks. We let Λ_σ denote the set of λ-terms of type σ. In this section, the only reduction rule considered is β-reduction:

$$(\lambda x\colon \sigma.\, M)N \longrightarrow_\beta M[N/x].$$

It turns out that the behavior of a term depends heavily on the nature of the last typing inference rule used in typing this term. A term created by an introduction rule, or I-term, plays a crucial role, because when combined with another term (or several other terms in the case of disjunctive terms), a new redex is created. On the other hand, for a term created by an elimination rule, or simple term, no new redex is created when this term is combined with another term (or several other terms in the case of disjunctive terms). This motivates the following definition.

Definition 5.2 An *I-term* is a term of the form $\lambda x\colon \sigma.\, M$. A *simple* term (or *neutral* term) is a term that is not an I-term. Thus, a simple term is either a variable x, a constant c, or an application MN. A term M is *stubborn* iff it is simple and, either M is irreducible, or M' is a simple term whenever $M \xrightarrow{+}_\beta M'$ (equivalently, M' is **not** an I-term).

Let $\mathcal{P} = (P_\sigma)_{\sigma \in \mathcal{T}}$ be a family of nonempty sets of simply-typed λ-terms.

Definition 5.3 Properties (P1)-(P3) are defined as follows:

(P1) $x \in P_\sigma$, $c \in P_\sigma$, for every variable x and constant c of type σ.

(P2) If $M \in P_\sigma$ and $M \longrightarrow_\beta N$, then $N \in P_\sigma$.

(P3) If M is simple, $M \in P_{\sigma \to \tau}$, $N \in P_\sigma$, and $(\lambda x\colon \sigma.\, M')N \in P_\tau$ whenever $M \xrightarrow{+}_\beta \lambda x\colon \sigma.\, M'$, then $MN \in P_\tau$.

From now on, we only consider families $\mathcal{P}$ satisfying conditions (P1)-(P3) of definition 5.3.

Definition 5.4 A nonempty set C of terms of type σ is a *$\mathcal{P}$-candidate* iff it satisfies the following conditions:

(R1) $C \subseteq P_\sigma$.

(R2) If $M \in C$ and $M \longrightarrow_\beta N$, then $N \in C$.

(R3) If M is simple, $M \in P_\sigma$, and $\lambda x\colon \gamma.\, M' \in C$ whenever $M \xrightarrow{+}_\beta \lambda x\colon \gamma.\, M'$, then $M \in C$.

Note that (R3) and (P1) imply that for every type σ, any $\mathcal{P}$-candidate C of type σ contains all variables and all constants of type σ. More generally, (R3) implies that C contains all stubborn terms in P_σ, and (P1) guarantees that variables and constants are stubborn terms in P_σ (for every type σ).

By (P3), if $M \in P_{\sigma \to \tau}$ is a stubborn term and $N \in P_\sigma$ is any term, then $MN \in P_\tau$. Furthermore, MN is also stubborn since it is a simple term and since it can only reduce to an I-term (a λ-abstraction) if M itself reduces to a λ-abstraction, i.e. an I-term. Thus, if $M \in P_{\sigma \to \tau}$ is a stubborn term and $N \in P_\sigma$ is any term, then MN is a stubborn term in P_τ. As a consequence, since variables are stubborn, for any terms $N_1, \ldots, N_k$ in $\mathcal{P}$, for every variable x, the term $xN_1 \ldots N_k$ is a stubborn term in $\mathcal{P}$ (assuming appropriate types for x and $N_1, \ldots, N_k$). Instead of (R3), a condition that occurs frequently in reducibility arguments is the following:

(S2) If $N \in P_\gamma$ and $M[N/x]N_1 \ldots N_k \in C$, then $(\lambda x\colon \gamma.\, M)NN_1 \ldots N_k \in C$.

It can be shown easily that (R2) and (R3) imply (S2) (see the proof of lemma 5.8). Terms of the form $xN_1 \ldots N_k$ or $M[N/x]N_1 \ldots N_k$ are known to play a role in reducibility arguments (for example, by Tait, Mitchell, or Krivine), and it is no surprise that they crop up again. However, in contrast with other presentations, we do not have to deal with them explicitly.

Given a family $\mathcal{P}$, for every type σ, we define $[\![\sigma]\!]$ as follows.

Definition 5.5 The sets $[\![\sigma]\!]$ are defined as follows:

$$\begin{aligned} [\![\sigma]\!] &= P_\sigma, \qquad \sigma \text{ a base type}, \\ [\![\sigma \to \tau]\!] &= \{M \mid M \in P_{\sigma \to \tau}, \text{ and for all } N, \text{ if } N \in [\![\sigma]\!] \text{ then } MN \in [\![\tau]\!]\}. \end{aligned}$$

Lemma 5.6 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P3), then each $[\![\sigma]\!]$ is a $\mathcal{P}$-candidate that contains all stubborn terms in P_σ.*

Proof. We proceed by induction on types. If σ is a base type, $[\![\sigma]\!] = P_\sigma$, and obviously, every stubborn term in P_σ is in $[\![\sigma]\!]$. Since $[\![\sigma]\!] = P_\sigma$, (R1) is trivial, (R2) follows from (P2), and (R3) is also trivial.[4]

We now consider the induction step.

(R1). By the definition of $[\![\sigma \to \tau]\!]$, (R1) is trivial.

(R2). Let $M \in [\![\sigma \to \tau]\!]$ and assume that $M \longrightarrow_\beta M'$. Since $M \in P_{\sigma\to\tau}$ by (R1), we have $M' \in P_{\sigma\to\tau}$ by (P2). For any $N \in [\![\sigma]\!]$, since $M \in [\![\sigma \to \tau]\!]$ we have $MN \in [\![\tau]\!]$, and since $M \longrightarrow_\beta M'$ we have $MN \longrightarrow_\beta M'N$. Then, applying the induction hypothesis at type τ, (R2) holds for $[\![\tau]\!]$, and thus $M'N \in [\![\tau]\!]$. Thus, we have shown that $M' \in P_{\sigma\to\tau}$ and that if $N \in [\![\sigma]\!]$, then $M'N \in [\![\tau]\!]$. By the definition of $[\![\sigma \to \tau]\!]$, this shows that $M' \in [\![\sigma \to \tau]\!]$, and (R2) holds at type $\sigma \to \tau$.

(R3). Let $M \in P_{\sigma\to\tau}$ be a simple term, and assume that $\lambda x\colon\sigma.\, M' \in [\![\sigma \to \tau]\!]$ whenever $M \xrightarrow{+}_\beta \lambda x\colon\sigma.\, M'$. We prove that for every N, if $N \in [\![\sigma]\!]$, then $MN \in [\![\tau]\!]$. First, we prove that $MN \in P_\tau$, and for this we use (P3). First, assume that $M \in P_{\sigma\to\tau}$ is stubborn, and let N be in $[\![\sigma]\!]$. By (R1), $N \in P_\sigma$. By the induction hypothesis, all stubborn terms in P_τ are in $[\![\tau]\!]$. Since we have shown that MN is a stubborn term in P_τ whenever $M \in P_{\sigma\to\tau}$ is stubborn and $N \in P_\tau$, we have $M \in [\![\sigma \to \tau]\!]$. Now, consider $M \in P_{\sigma\to\tau}$ non stubborn. If $M \xrightarrow{+}_\beta \lambda x\colon\sigma.\, M'$, then by assumption, $\lambda x\colon\sigma.\, M' \in [\![\sigma \to \tau]\!]$, and for any $N \in [\![\sigma]\!]$, we have $(\lambda x\colon\sigma.\, M')N \in [\![\tau]\!]$. Since by (R1), $N \in P_\sigma$ and $(\lambda x\colon\sigma.\, M')N \in P_\tau$, by (P3), we have $MN \in P_\tau$. Now, there are two cases.

If τ is a base type, then $[\![\tau]\!] = P_\tau$ and $MN \in [\![\tau]\!]$.

If τ is not a base type, the term MN is simple. Thus, we prove that $MN \in [\![\tau]\!]$ using (R3) (which by induction, holds at type τ). The case where MN is stubborn follows from the induction hypothesis. Otherwise, observe that if $MN \xrightarrow{+}_\beta Q$, where $Q = \lambda y\colon\gamma.\, P$ is an I-term, then the reduction is necessarily of the form

$$MN \xrightarrow{+}_\beta (\lambda x\colon\sigma.\, M')N' \longrightarrow_\beta M'[N'/x] \xrightarrow{*}_\beta Q,$$

where $M \xrightarrow{+}_\beta \lambda x\colon\sigma.\, M'$ and $N \xrightarrow{*}_\beta N'$. Since by assumption, $\lambda x\colon\sigma.\, M' \in [\![\sigma \to \tau]\!]$ whenever $M \xrightarrow{+}_\beta \lambda x\colon\sigma.\, M'$, and by the induction hypothesis applied at type σ, by (R2), $N' \in [\![\sigma]\!]$, we conclude that $(\lambda x\colon\sigma.\, M')N' \in [\![\tau]\!]$. By the induction hypothesis applied at type τ, by (R2), we have $Q \in [\![\tau]\!]$, and by (R3), we have $MN \in [\![\tau]\!]$.

Since $M \in P_{\sigma\to\tau}$ and $MN \in [\![\tau]\!]$ whenever $N \in [\![\sigma]\!]$, we conclude that $M \in [\![\sigma \to \tau]\!]$. $\square$

For the proof of the next lemma, we need to add two new conditions (P4) and (P5) to (P1)-(P3).

Definition 5.7 Properties (P4) and (P5) are defined as follows:

(P4) If $M \in P_\tau$, then $\lambda x\colon\sigma.\, M \in P_{\sigma\to\tau}$.

(P5) If $N \in P_\sigma$ and $M[N/x] \in P_\tau$, then $(\lambda x\colon\sigma.\, M)N \in P_\tau$.

Lemma 5.8 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P5) and for every N, ($N \in [\![\sigma]\!]$ implies $M[N/x] \in [\![\tau]\!]$), then $\lambda x\colon\sigma.\, M \in [\![\sigma \to \tau]\!]$.*

[4] In fact, if $[\![\sigma]\!] = P_\sigma$, (R3) holds trivially even at nonbase types. This remark is useful is we allow type variables.

Proof. We prove that $\lambda x{:}\sigma.\, M \in P_{\sigma\to\tau}$ and that for every every N, if $N \in [\![\sigma]\!]$, then $(\lambda x{:}\sigma.M)N \in [\![\tau]\!]$. We will need the fact that the sets of the form $[\![\sigma]\!]$ have the properties (R1)-(R3), but this follows from lemma 5.6, since (P1)-(P3) hold. First, we prove that $\lambda x{:}\sigma.\, M \in P_{\sigma\to\tau}$.

Since by lemma 5.6, $x \in [\![\sigma]\!]$ for every variable of type σ, by the assumption of lemma 5.8, $M[x/x] = M \in [\![\tau]\!]$. Then, by (R1), $M \in P_\tau$, and by (P4), we have $\lambda x{:}\sigma.\, M \in P_{\sigma\to\tau}$.

Next, we prove that for every every N, if $N \in [\![\sigma]\!]$, then $(\lambda x{:}\sigma.M)N \in [\![\tau]\!]$. Let us assume that $N \in [\![\sigma]\!]$. Then, by the assumption of lemma 5.8, $M[N/x] \in [\![\tau]\!]$. Thus, by (R1), we have $N \in P_\sigma$ and $M[N/x] \in P_\tau$. By (P5), we have $(\lambda x{:}\sigma.\, M)N \in P_\tau$. Now, there are two cases.

If τ is a base type, then $[\![\tau]\!] = P_\tau$. Since we just showed that $(\lambda x{:}\sigma.\, M)N \in P_\tau$, we have $(\lambda x{:}\sigma.\, M)N \in [\![\tau]\!]$.

If τ is not a base type, then $(\lambda x{:}\sigma.\, M)N$ is simple. Thus, we prove that $(\lambda x{:}\sigma.\, M)N \in [\![\tau]\!]$ using (R3). The case where $(\lambda x{:}\sigma.\, M)N$ is stubborn is trivial. Otherwise, observe that if $(\lambda x{:}\sigma.\, M)N \xrightarrow{+}_\beta Q$, where $Q = \lambda y{:}\gamma.\, P$ is an I-term, then the reduction is necessarily of the form

$$(\lambda x{:}\sigma.\, M)N \xrightarrow{*}_\beta (\lambda x{:}\sigma.\, M')N' \longrightarrow_\beta M'[N'/x] \xrightarrow{*}_\beta Q,$$

where $M \xrightarrow{*}_\beta M'$ and $N \xrightarrow{*}_\beta N'$. But $M[N/x] \in [\![\tau]\!]$, and since

$$M[N/x] \xrightarrow{*}_\beta M'[N'/x] \xrightarrow{*}_\beta Q,$$

by (R2), we have $Q \in [\![\tau]\!]$. Since $(\lambda x{:}\sigma.\, M)N \in P_\tau$ and $Q \in [\![\tau]\!]$ whenever $(\lambda x{:}\sigma.\, M)N \xrightarrow{+}_\beta Q$, by (R3), we have $(\lambda x{:}\sigma.\, M)N \in [\![\tau]\!]$. $\square$

Lemma 5.9 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P5), then for every term M of type σ, for every substitution φ such that $\varphi(y) \in [\![\gamma]\!]$ for every $y{:}\gamma \in FV(M)$, we have $M[\varphi] \in [\![\sigma]\!]$.*

Proof. We proceed by induction on the structure of M. If M is a variable, then $x[\varphi] = \varphi(x) \in [\![\sigma]\!]$ by the assumption on φ. If c is a constant, then $c[\varphi] = c$, and $c \in [\![\sigma]\!]$ since this is true by lemma 5.6.

If $M = M_1N_1$, where M_1 has type $\sigma \to \tau$ and N_1 has type σ, by the induction hypothesis, $M_1[\varphi] \in [\![\sigma \to \tau]\!]$ and $N_1[\varphi] \in [\![\sigma]\!]$. By the definition of $[\![\sigma \to \tau]\!]$, we get $M_1[\varphi]N_1[\varphi] \in [\![\tau]\!]$, which shows that $(M_1N_1)[\varphi] \in [\![\tau]\!]$, since $M_1[\varphi]N_1[\varphi] = (M_1N_1)[\varphi]$.

If $M = \lambda x{:}\sigma.\, M_1$, consider any $N \in [\![\sigma]\!]$ and any substitution φ such that $\varphi(y) \in [\![\gamma]\!]$ for every $y{:}\gamma \in FV(\lambda x{:}\sigma.\, M_1)$. Thus, the substitution $\varphi[x{:}= N]$ has the property that $\varphi(y) \in [\![\gamma]\!]$ for every $y{:}\gamma \in FV(M_1)$. By suitable α-conversion, we can assume that x does not occur in any $\varphi(y)$ for every $y \in dom(\varphi)$, and that N is substitutable for x in M_1. Then, $M_1[\varphi[x{:}= N]] = M_1[\varphi][N/x]$. By the induction hypothesis applied to M_1 and $\varphi[x{:}= N]$, we have $M_1[\varphi[x{:}= N]] \in [\![\tau]\!]$, that is, $M_1[\varphi][N/x] \in [\![\tau]\!]$. Consequently, by lemma 5.8, $(\lambda x{:}\sigma.\, M_1[\varphi]) \in [\![\sigma \to \tau]\!]$, that is, $(\lambda x{:}\sigma.\, M_1)[\varphi] \in [\![\sigma \to \tau]\!]$, since $(\lambda x{:}\sigma.\, M_1[\varphi]) = (\lambda x{:}\sigma.\, M_1)[\varphi]$. $\square$

Theorem 5.10 *If $\mathcal{P}$ is a family of λ-terms satisfying conditions (P1)-(P5), then $P_\sigma = \Lambda_\sigma$ for every type σ (in other words, every term satisfies the unary predicate defined by $\mathcal{P}$).*

Proof. Apply lemma 5.9 to every term M of type σ and to the identity substitution, which is legitimate since $x \in [\![\sigma]\!]$ for every variable of type σ (by lemma 5.6). Thus, $M \in [\![\sigma]\!]$ for every term of type σ, that is $\Lambda_\sigma \subseteq P_\sigma$. Since obviously $P_\sigma \subseteq \Lambda_\sigma$, we have $P_\sigma = \Lambda_\sigma$. $\square$

6 Adding Product and Sum Types $\times$ and $+$

The type-checking rules of the system are summarized in the following definition.

Definition 6.1 The terms of the typed λ-calculus $\lambda^{\rightarrow,\times,+}$ are defined by the following rules.

$$x\colon\sigma, \quad \text{when } x \in X_\sigma,$$

(we can also have $c\colon\sigma$, for a set of constants that have been preassigned types).

$$\frac{x\colon\sigma \rhd M\colon\tau}{\rhd (\lambda x\colon\sigma.\, M)\colon\sigma\to\tau} \quad (\textit{abstraction})$$

$$\frac{\rhd M\colon\sigma\to\tau \quad \rhd N\colon\sigma}{\rhd (MN)\colon\tau} \quad (\textit{application})$$

$$\frac{\rhd M\colon\sigma \quad \rhd N\colon\tau}{\rhd \langle M,N\rangle\colon\sigma\times\tau} \quad (\textit{pairing})$$

$$\frac{\rhd M\colon\sigma\times\tau}{\rhd \pi_1(M)\colon\sigma} \quad (\textit{projection}) \qquad \frac{\rhd M\colon\sigma\times\tau}{\rhd \pi_2(M)\colon\tau} \quad (\textit{projection})$$

$$\frac{\rhd M\colon\sigma}{\rhd \mathtt{inl}(M)\colon\sigma+\tau} \quad (\textit{injection}) \qquad \frac{\rhd M\colon\tau}{\rhd \mathtt{inr}(M)\colon\sigma+\tau} \quad (\textit{injection})$$

$$\frac{\rhd P\colon\sigma+\tau \quad x\colon\sigma \rhd M\colon\delta \quad y\colon\tau \rhd N\colon\delta}{\rhd (\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon\sigma) \Rightarrow M \mid \mathtt{inr}(y\colon\tau) \Rightarrow N)\colon\delta} \quad (\textit{by-cases})$$

We also recall the reduction rules.

Definition 6.2 The reduction rules of the system $\lambda^{\rightarrow,\times,+}$ are listed below:

$$\begin{aligned}
(\lambda x\colon\sigma.\, M)N &\longrightarrow M[N/x],\\
\pi_1(\langle M,N\rangle) &\longrightarrow M,\\
\pi_2(\langle M,N\rangle) &\longrightarrow N,\\
\mathtt{case}\ \mathtt{inl}(P)\ \mathtt{of}\ \mathtt{inl}(x\colon\sigma) \Rightarrow M \mid \mathtt{inr}(y\colon\tau) \Rightarrow N &\longrightarrow M[P/x],\\
\mathtt{case}\ \mathtt{inr}(P)\ \mathtt{of}\ \mathtt{inl}(x\colon\sigma) \Rightarrow M \mid \mathtt{inr}(y\colon\tau) \Rightarrow N &\longrightarrow N[P/y].
\end{aligned}$$

The reduction relation defined by the rules of definition 6.2 is still denoted as $\longrightarrow_\beta$ (even though there are reductions other that β-reduction). The definition of an I-term is extended as follows.

Definition 6.3 An *I-term* is a term of the form either $\lambda x\colon\sigma.\, M$, $\langle M,N\rangle$, $\mathtt{inl}(M)$, or $\mathtt{inr}(M)$. A *simple* term (or *neutral* term) is a term that is not an I-term. Thus, a simple term is either a variable x, a constant c, an application MN, a projection $\pi_1(M)$ or $\pi_2(M)$, or a conditional term $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon\sigma) \Rightarrow M \mid \mathtt{inr}(y\colon\tau) \Rightarrow N$. A term M is *stubborn* iff it is simple and, either M is irreducible, or M' is a simple term whenever $M \xrightarrow{+}_\beta M'$ (equivalently, M' is **not** an I-term).

Thus, an I-term is a proof-term corresponding to the conclusion of an introduction rule. The beauty of I-terms is that they are just what makes condition (R3) work. We need to extend definition 5.3, definition 5.4, definition 5.5, and definition 5.7, to take into account product types $\sigma \times \tau$ and sum types $\sigma + \tau$.

Definition 6.4 Properties (P1)-(P3) are defined as follows:

(P1) $x \in P_\sigma$, $c \in P_\sigma$, for every variable x and constant c of type σ.

(P2) If $M \in P_\sigma$ and $M \longrightarrow_\beta N$, then $N \in P_\sigma$.

(P3) If M is simple, then:

(1) If $M \in P_{\sigma\to\tau}$, $N \in P_\sigma$, and $(\lambda x{:}\,\sigma.\, M')N \in P_\tau$ whenever $M \xrightarrow{+}_\beta \lambda x{:}\,\sigma.\, M'$, then $MN \in P_\tau$.

(2) If $M \in P_{\sigma\times\tau}$, and $\pi_1(\langle M', N'\rangle) \in P_\sigma$ and $\pi_2(\langle M', N'\rangle) \in P_\tau$ whenever $M \xrightarrow{+}_\beta \langle M', N'\rangle$, then $\pi_1(M) \in P_\sigma$ and $\pi_2(M) \in P_\tau$.

From now on, we only consider families $\mathcal{P}$ satisfying conditions (P1)-(P3) of definition 6.4. Note that (P3) still implies that if $M \in P_{\sigma\to\tau}$ is a stubborn term and $N \in P_\sigma$ is any term, then MN is a stubborn term in P_τ. It also implies that if $M \in P_{\sigma\times\tau}$ is a stubborn term, then $\pi_1(M)$ is a stubborn term in P_σ and $\pi_2(M)$ is a stubborn term in P_τ.

Definition 6.5 A nonempty set C of terms of type σ is a $\mathcal{P}$-*candidate* iff it satisfies the following conditions:

(R1) $C \subseteq P_\sigma$.

(R2) If $M \in C$ and $M \longrightarrow_\beta N$, then $N \in C$.

(R3) If M is simple, $M \in P_\sigma$, and $M' \in C$ whenever $M \xrightarrow{+}_\beta M'$ and M' is an I-term, then $M \in C$.

Note that (R3) and (P1) imply that for every type σ, any $\mathcal{P}$-candidate C of type σ contains all variables and all constants of type σ.

Definition 6.6 The sets $[\![\sigma]\!]$ are defined as follows:

$$
\begin{aligned}
[\![\sigma]\!] &= P_\sigma, \qquad \sigma \text{ a base type}, \\
[\![\sigma \to \tau]\!] &= \{M \mid M \in P_{\sigma\to\tau}, \text{ and for all } N, \text{ if } N \in [\![\sigma]\!] \text{ then } MN \in [\![\tau]\!]\}, \\
[\![\sigma \times \tau]\!] &= \{M \mid M \in P_{\sigma\times\tau},\ \pi_1(M) \in [\![\sigma]\!], \text{ and } \pi_2(M) \in [\![\tau]\!]\}, \\
[\![\sigma + \tau]\!] &= \{M \mid M \in P_{\sigma+\tau}, \text{ either } M' \in [\![\sigma]\!] \text{ whenever } M \xrightarrow{*}_\beta \mathtt{inl}(M'), \text{ or} \\
&\qquad M'' \in [\![\tau]\!] \text{ whenever } M \xrightarrow{*}_\beta \mathtt{inr}(M'')\}.
\end{aligned}
$$

Note that $[\![\sigma \times \tau]\!]$ and $[\![\sigma + \tau]\!]$ can also be defined as follows:

$$
\begin{aligned}
[\![\sigma \times \tau]\!] &= \{M \mid M \in P_{\sigma\times\tau},\ \pi_1(M) \in [\![\sigma]\!]\} \cap \{M \mid M \in P_{\sigma\times\tau},\ \pi_2(M) \in [\![\tau]\!]\}, \\
[\![\sigma + \tau]\!] &= \{M \mid M \in P_{\sigma+\tau},\ M' \in [\![\sigma]\!] \text{ whenever } M \xrightarrow{*}_\beta \mathtt{inl}(M')\} \cup \\
&\qquad \{M \mid M \in P_{\sigma+\tau},\ M'' \in [\![\tau]\!] \text{ whenever } M \xrightarrow{*}_\beta \mathtt{inr}(M'')\}.
\end{aligned}
$$

We now prove a generalization of lemma 5.6.

Lemma 6.7 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P3), then each $[\![\sigma]\!]$ is a $\mathcal{P}$-candidate that contains all stubborn terms in P_σ.*

Proof. We proceed by induction on types. The base case is as in lemma 5.6. The induction step has more cases since we also need to deal with product and sum types.

(R1). This is trivial by the definitions of $[\![\sigma \to \tau]\!]$, $[\![\sigma \times \tau]\!]$, and $[\![\sigma + \tau]\!]$,

(R2). There are three cases depending on the type.

1. Arrow type $\sigma \to \tau$. The proof is as in lemma 5.6, since an I-term of type $\sigma \to \tau$ is necessarily of the form $\lambda x{:}\,\sigma.\, M$.

2. Product type $\sigma \times \tau$. Assume that $M \longrightarrow_\beta M'$ for $M \in [\![\sigma \times \tau]\!]$. We need to prove that $M' \in P_{\sigma\times\tau}$, $\pi_1(M') \in [\![\sigma]\!]$, and $\pi_2(M') \in [\![\tau]\!]$. Since $M \in [\![\sigma \times \tau]\!]$, by (R1), $M \in P_{\sigma\times\tau}$, and by (P2) $M' \in P_{\sigma\times\tau}$. Since $M \in [\![\sigma \times \tau]\!]$, we have $\pi_1(M) \in [\![\sigma]\!]$ and $\pi_2(M) \in [\![\tau]\!]$. But $\pi_1(M) \longrightarrow_\beta \pi_1(M')$ and $\pi_2(M) \longrightarrow_\beta \pi_2(M')$, and by the induction hypothesis, by (R2), we get $\pi_1(M') \in [\![\sigma]\!]$ and $\pi_2(M') \in [\![\tau]\!]$.

3. Sum type $\sigma+\tau$. Assume that $M \longrightarrow_\beta M'$ for $M \in [\![\sigma+\tau]\!]$. We need to prove that $M' \in P_{\sigma+\tau}$, and that either $M_1 \in [\![\sigma]\!]$ whenever $M' \xrightarrow{*}_\beta \mathtt{inl}(M_1)$, or $M_2 \in [\![\tau]\!]$ whenever $M' \xrightarrow{*}_\beta \mathtt{inr}(M_2)$. Since $M \in [\![\sigma + \tau]\!]$, by (R1), $M \in P_{\sigma+\tau}$, and by (P2) $M' \in P_{\sigma+\tau}$. Since $M \longrightarrow_\beta M'$, we have $M \xrightarrow{*}_\beta \mathtt{inl}(M_1)$ whenever $M' \xrightarrow{*}_\beta \mathtt{inl}(M_1)$, and $M \xrightarrow{*}_\beta \mathtt{inr}(M_2)$ whenever $M' \xrightarrow{*}_\beta \mathtt{inr}(M_2)$. However, by definition of $[\![\sigma + \tau]\!]$, either $M_1 \in [\![\sigma]\!]$ whenever $M \xrightarrow{*}_\beta \mathtt{inl}(M_1)$, or $M_2 \in [\![\tau]\!]$ whenever $M \xrightarrow{*}_\beta \mathtt{inr}(M_2)$. Thus, $M_1 \in [\![\sigma]\!]$ whenever $M' \xrightarrow{*}_\beta \mathtt{inl}(M_1)$, or $M_2 \in [\![\tau]\!]$ whenever $M' \xrightarrow{*}_\beta \mathtt{inr}(M_2)$.

(R3). Let M be a simple term. There are three cases depending on the type of M.

1. Arrow type $\sigma \to \tau$. The proof is as in lemma 5.6, since an I-term of type $\sigma \to \tau$ is necessarily of the form $\lambda x{:}\,\sigma.\, M$, and we use (P3)(1).

2. Product type $\sigma \times \tau$. Let $M \in P_{\sigma\times\tau}$ be a simple term, and assume that $M' \in [\![\sigma \times \tau]\!]$ whenever $M \xrightarrow{+}_\beta M'$ and M' is an I-term. We need to show that $\pi_1(M) \in [\![\sigma]\!]$ and $\pi_2(M) \in [\![\tau]\!]$. If $M \in P_{\sigma\times\tau}$ is stubborn, we have shown that $\pi_1(M)$ is a stubborn term in P_σ and that $\pi_2(M)$ is a stubborn term in P_τ. By the induction hypothesis, all stubborn terms in P_σ are in $[\![\sigma]\!]$ and all stubborn terms in P_τ are in $[\![\tau]\!]$. Thus, when M is stubborn, $\pi_1(M) \in [\![\sigma]\!]$ and $\pi_2(M) \in [\![\tau]\!]$. Next, assume that M is not stubborn. Now, an I-term of type $\sigma \times \tau$ is necessarily of the form $\langle M_1, N_1\rangle$, and by the assumption, whenever $M \xrightarrow{+}_\beta \langle M_1, N_1\rangle$, we have $\langle M_1, N_1\rangle \in [\![\sigma \times \tau]\!]$. This implies that $\pi_1(\langle M_1, N_1\rangle) \in [\![\sigma]\!]$ and $\pi_2(\langle M_1, N_1\rangle) \in [\![\tau]\!]$. By (R1), we have $\pi_1(\langle M_1, N_1\rangle) \in P_\sigma$, $\pi_2(\langle M_1, N_1\rangle) \in P_\tau$, and by (P3)(2), we get $\pi_1(M) \in P_\sigma$ and $\pi_2(M) \in P_\tau$. If σ is a base type, then $[\![\sigma]\!] = P_\sigma$ and $\pi_1(M) \in [\![\sigma]\!]$. Similarly, if τ is a base type, then $[\![\tau]\!] = P_\tau$ and $\pi_2(M) \in [\![\tau]\!]$.

Let us now consider the case where σ is not a base type, the case where τ is not a base type being similar. Then, we know that $\pi_1(M) \in P_\sigma$ and $\pi_1(M)$ is a simple term. We use (R3) to prove that $\pi_1(M) \in [\![\sigma]\!]$. The case where $\pi_1(M)$ is stubborn is trivial. Otherwise, we need to show that $M' \in [\![\sigma]\!]$ whenever $\pi_1(M) \xrightarrow{+}_\beta M'$ and M' is an I-term. Then, the reduction $\pi_1(M) \xrightarrow{+}_\beta M'$ must be of the form

$$\pi_1(M) \xrightarrow{+}_\beta \pi_1(\langle M_1, N_1\rangle) \longrightarrow_\beta M_1 \xrightarrow{*}_\beta M',$$

where $M \xrightarrow{+}_\beta \langle M_1, N_1\rangle$. Since $\langle M_1, N_1\rangle$ is an I-term, by the assumption, we have $\langle M_1, N_1\rangle \in [\![\sigma \times \tau]\!]$. This implies that $\pi_1(\langle M_1, N_1\rangle) \in [\![\sigma]\!]$, and by the induction hypothesis and (R2), we have $M' \in [\![\sigma]\!]$. By (R3), we conclude that $\pi_1(M) \in [\![\sigma]\!]$.

3. Sum type $\sigma+\tau$. If $M \in P_{\sigma+\tau}$ is stubborn, then by definition of $[\![\sigma+\tau]\!]$, we have $M \in [\![\sigma+\tau]\!]$. Otherwise, let $M \in P_{\sigma+\tau}$ be a simple term, and assume that $M' \in [\![\sigma+\tau]\!]$ whenever $M \xrightarrow{+}_\beta M'$ and M' is an I-term. We need to show that either $M_1 \in [\![\sigma]\!]$ whenever $M \xrightarrow{*}_\beta \mathtt{inl}(M_1)$, or $M_2 \in [\![\tau]\!]$ whenever $M \xrightarrow{*}_\beta \mathtt{inr}(M_2)$. Assume that $M \xrightarrow{*}_\beta \mathtt{inl}(M_1)$. Since $\mathtt{inl}(M_1)$ is an I-term, by the assumption, we have $\mathtt{inl}(M_1) \in [\![\sigma+\tau]\!]$. By definition of $[\![\sigma+\tau]\!]$, we have either $M_1' \in [\![\sigma]\!]$ whenever $\mathtt{inl}(M_1) \xrightarrow{*}_\beta \mathtt{inl}(M_1')$, or $M_2' \in [\![\tau]\!]$ whenever $\mathtt{inl}(M_1) \xrightarrow{*}_\beta \mathtt{inr}(M_2')$. However, derivations of the form $\mathtt{inl}(M_1) \xrightarrow{*}_\beta \mathtt{inr}(M_2')$ are impossible. Thus, the first case applies, and we have $M_1 \in [\![\sigma]\!]$, since $\mathtt{inl}(M_1) \xrightarrow{*}_\beta \mathtt{inl}(M_1)$. The case where $M \xrightarrow{*}_\beta \mathtt{inr}(M_2)$ is similar. □

Definition 6.8 Properties (P4) and (P5) are defined as follows:

(P4)
(1) If $M \in P_\tau$, then $\lambda x\colon\sigma.\, M \in P_{\sigma\to\tau}$.
(2) If $M \in P_\sigma$ and $N \in P_\tau$, then $\langle M, N\rangle \in P_{\sigma\times\tau}$.
(3) If $M \in P_\sigma$, then $\mathtt{inl}(M) \in P_{\sigma+\tau}$, and if $M \in P_\tau$, then $\mathtt{inr}(M) \in P_{\sigma+\tau}$.

(P5)
(1) If $N \in P_\sigma$ and $M[N/x] \in P_\tau$, then $(\lambda x\colon\sigma.\, M)N \in P_\tau$.
(2) If $M \in P_\sigma$ and $N \in P_\tau$, then $\pi_1(\langle M, N\rangle) \in P_\sigma$ and $\pi_2(\langle M, N\rangle) \in P_\tau$.
(3) If $P \in P_{\sigma+\tau}$, $M \in P_\delta$, $N \in P_\delta$, $M[P_1/x] \in P_\delta$ whenever $P \xrightarrow{*}_\beta \mathtt{inl}(P_1)$, and $N[P_2/y] \in P_\delta$ whenever $P \xrightarrow{*}_\beta \mathtt{inr}(P_2)$, then $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon\sigma) \Rightarrow M \mid \mathtt{inr}(y\colon\tau) \Rightarrow N \in P_\delta$.

It is easy to verify that $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon\sigma) \Rightarrow M \mid \mathtt{inr}(y\colon\tau) \Rightarrow N \in P_\delta$ is a stubborn term in P_δ, if $P \in P_{\sigma+\tau}$ is stubborn, $M \in P_\delta$, and $N \in P_\delta$.

Lemma 6.9 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P5) then the following properties hold: (1) If for every N, ($N \in [\![\sigma]\!]$ implies $M[N/x] \in [\![\tau]\!]$), then $\lambda x\colon\sigma.\, M \in [\![\sigma \to \tau]\!]$; (2) If $M \in [\![\sigma]\!]$ and $N \in [\![\tau]\!]$, then $\langle M, N\rangle \in [\![\sigma\times\tau]\!]$; (3) If $P \in [\![\sigma+\tau]\!]$, for every P_1, ($P_1 \in [\![\sigma]\!]$ implies $M[P_1/x] \in [\![\delta]\!]$), and for every P_2, ($P_2 \in [\![\tau]\!]$ implies $N[P_2/y] \in [\![\delta]\!]$), then $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon\sigma) \Rightarrow M \mid \mathtt{inr}(y\colon\tau) \Rightarrow N \in [\![\delta]\!]$.*

Proof. It is similar to the proof of lemma 5.8, except that we need to prove more clauses. By lemma 6.7, we know that the sets of the form $[\![\sigma]\!]$ have the properties (R1)-(R3).

(1) This has already been proved in lemma 5.8.

(2) We need to prove that $\langle M, N\rangle \in P_{\sigma\times\tau}$, and that $\pi_1(\langle M, N\rangle) \in [\![\sigma]\!]$ and $\pi_2(\langle M, N\rangle) \in [\![\tau]\!]$. Since $M \in [\![\sigma]\!]$ and $N \in [\![\tau]\!]$, by (R1), $M \in P_\sigma$ and $N \in P_\tau$. By (P4)(2), we get $\langle M, N\rangle \in P_{\sigma\times\tau}$. By (P5)(2), we also have $\pi_1(\langle M, N\rangle) \in P_\sigma$ and $\pi_2(\langle M, N\rangle) \in P_\tau$. If σ is a base type then $[\![\sigma]\!] = P_\sigma$ and $\pi_1(\langle M, N\rangle) \in [\![\sigma]\!]$. Similarly, if τ is a base type then $[\![\tau]\!] = P_\tau$ and $\pi_2(\langle M, N\rangle) \in [\![\tau]\!]$.

If both σ and τ are nonbase types, $\pi_1(\langle M, N\rangle) \in P_\sigma$ and $\pi_2(\langle M, N\rangle) \in P_\tau$ are simple terms. We prove that $\pi_1(\langle M, N\rangle) \in [\![\sigma]\!]$ and $\pi_2(\langle M, N\rangle) \in [\![\tau]\!]$ using (R3). We consider the case of $\pi_1(\langle M, N\rangle)$, the case of $\pi_2(\langle M, N\rangle)$ being similar. The case where $\pi_1(\langle M, N\rangle)$ is stubborn is trivial. Otherwise, we need to prove that $Q \in [\![\sigma]\!]$ whenever $\pi_1(\langle M, N\rangle) \xrightarrow{+}_\beta Q$ and Q is an I-term. Then, the reduction must be of the form

$$\pi_1(\langle M, N\rangle) \xrightarrow{*}_\beta \pi_1(\langle M_1, N_1\rangle) \longrightarrow_\beta M_1 \xrightarrow{*}_\beta Q,$$

where $M \xrightarrow{*}_\beta M_1$ and $N \xrightarrow{*}_\beta N_1$. Since $M \in [\![\sigma]\!]$ and

$$M \xrightarrow{*}_\beta M_1 \xrightarrow{*}_\beta Q,$$

by (R2), we have $Q \in [\![\sigma]\!]$.

(3) First, we prove that $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N \in P_\delta$. Assume that the hypothesis of (3) holds. By the assumption, $P \in [\![\sigma + \tau]\!]$, and also $M = M[x/x] \in [\![\delta]\!]$ and $N = N[y/y] \in [\![\delta]\!]$, since by lemma 6.7, $x \in [\![\sigma]\!]$ and $y \in [\![\tau]\!]$. By (R1), we have $P \in P_{\sigma+\tau}$, $M \in P_\delta$, and $N \in P_\delta$. If P is stubborn, we have shown that $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N$ is a stubborn term in P_δ, and thus $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N \in [\![\delta]\!]$ by (R3). Otherwise, if P is not stubborn, and since $P \in [\![\sigma + \tau]\!]$, by (R2), whenever $P \xrightarrow{*}_\beta \mathtt{inl}(P_1)$, we have $\mathtt{inl}(P_1) \in [\![\sigma + \tau]\!]$. By definition of $[\![\sigma + \tau]\!]$, this implies that $P_1 \in [\![\sigma]\!]$. Then, by the assumption, we have $M[P_1/x] \in [\![\delta]\!]$. By (R1), we have $P \in P_{\sigma+\tau}$, $M \in P_\delta$, $N \in P_\delta$, and $M[P_1/x] \in P_\delta$ whenever $P \xrightarrow{*}_\beta \mathtt{inl}(P_1)$. A similar reasoning applies when $P \xrightarrow{*}_\beta \mathtt{inr}(P_2)$, and we have $N[P_2/y] \in P_\delta$. Then, by (P5)(3), we have $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N \in P_\delta$. If δ is a base type, then $[\![\delta]\!] = P_\delta$, and $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N \in [\![\delta]\!]$.

If δ is not a base type, then $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N \in P_\delta$ is a simple term. We use (R3) to prove that $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N \in [\![\delta]\!]$. The case where $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N$ is stubborn is trivial. Otherwise, assume that $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N \xrightarrow{+}_\beta Q$ and Q is an I-term. Then, the reduction is either of the form

$$\begin{aligned}\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N &\xrightarrow{*}_\beta \mathtt{case}\ \mathtt{inl}(P_1)\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M_1 \mid \mathtt{inr}(y{:}\tau) \Rightarrow N_1 \\ &\longrightarrow_\beta M_1[P_1/x] \xrightarrow{*}_\beta Q,\end{aligned}$$

where $P \xrightarrow{*}_\beta \mathtt{inl}(P_1)$, $M \xrightarrow{*}_\beta M_1$, and $N \xrightarrow{*}_\beta N_1$, or

$$\begin{aligned}\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N &\xrightarrow{*}_\beta \mathtt{case}\ \mathtt{inr}(P_2)\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M_1 \mid \mathtt{inr}(y{:}\tau) \Rightarrow N_1 \\ &\longrightarrow_\beta N_1[P_2/y] \xrightarrow{*}_\beta Q,\end{aligned}$$

where $P \xrightarrow{*}_\beta \mathtt{inr}(P_2)$, $M \xrightarrow{*}_\beta M_1$, and $N \xrightarrow{*}_\beta N_1$. Consider the first case, the second one being similar. Since $P \in [\![\sigma + \tau]\!]$, by (R2), $\mathtt{inl}(P_1) \in [\![\sigma + \tau]\!]$. This implies that $P_1 \in [\![\sigma]\!]$. Then, by the assumption, we have $M[P_1/x] \in [\![\delta]\!]$, and since

$$M[P_1/x] \xrightarrow{*}_\beta M_1[P_1/x] \xrightarrow{*}_\beta Q,$$

by (R2), we get $Q \in [\![\delta]\!]$. Finally, by (R3), we have $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\tau) \Rightarrow N \in [\![\delta]\!]$. □

Lemma 6.10 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P5), then for every term M of type σ, for every substitution φ such that $\varphi(y) \in [\![\gamma]\!]$ for every $y{:}\gamma \in FV(M)$, we have $M[\varphi] \in [\![\sigma]\!]$.*

Proof. We proceed by induction on the structure of M. Some of the cases have already been covered in the proof of lemma 5.9, but we also need to handle the new terms.

If $M = \langle M_1, N_1\rangle$, where M_1 has type σ and N_1 has type τ, then by the induction hypothesis, $M_1[\varphi] \in [\![\sigma]\!]$ and $N_1[\varphi] \in [\![\tau]\!]$. By lemma 6.9, we have $\langle M_1[\varphi], N_1[\varphi]\rangle \in [\![\sigma \times \tau]\!]$, i.e. $\langle M_1, N_1\rangle[\varphi] \in [\![\sigma \times \tau]\!]$, since $\langle M_1[\varphi], N_1[\varphi]\rangle = \langle M_1, N_1\rangle[\varphi]$.

If $M = \pi_1(M_1)$ where M_1 has type $\sigma \times \tau$, then by the induction hypothesis, $M_1[\varphi] \in [\![\sigma \times \tau]\!]$. By the definition of $[\![\sigma \times \tau]\!]$, this implies that $\pi_1(M_1)[\varphi] \in [\![\sigma]\!]$, since $\pi_1(M_1)[\varphi] = \pi_1(M_1[\varphi])$. Similarly, we get $\pi_2(M_1)[\varphi] \in [\![\tau]\!]$.

If $M = \mathtt{inl}(M_1)$ where M has type $\sigma + \tau$, then by the induction hypothesis, $M_1[\varphi] \in [\![\sigma]\!]$. By (P4)(3), we have $\mathtt{inl}(M_1[\varphi]) \in P_{\sigma+\tau}$. We need to show that either $N_1 \in [\![\sigma]\!]$ whenever $\mathtt{inl}(M_1[\varphi]) \xrightarrow{*}_\beta \mathtt{inl}(N_1)$, or $N_2 \in [\![\tau]\!]$ whenever $\mathtt{inl}(M_1[\varphi]) \xrightarrow{*}_\beta \mathtt{inr}(N_2)$. The second derivation is impossible, and in the first case, we must have $M_1[\varphi] \xrightarrow{*}_\beta N_1$. Since $M_1[\varphi] \in [\![\sigma]\!]$, by (R2), we have $N_1 \in [\![\sigma]\!]$. The case where $M = \mathtt{inr}(M_1)$ is similar.

If $M = \mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M_1 \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N_1$ is of type δ, consider any $P_1 \in [\![\sigma]\!]$, any $P_2 \in [\![\tau]\!]$, and any substitution φ such that $\varphi(z) \in [\![\gamma]\!]$ for every $z{:}\,\gamma \in (FV(P) \cup FV(M_1) \cup FV(N_1)) - \{x, y\}$. Thus, $\varphi[x{:=}\ P_1, y{:=}\ P_2]$ has the property that $\varphi(z) \in [\![\gamma]\!]$ for every $z{:}\,\gamma \in (FV(P) \cup FV(M_1) \cup FV(N_1))$. By suitable α-conversion, we can assume that x and y do not occur in any $\varphi(z)$ for every $z \in dom(\varphi)$, that P_1 is substitutable for x in M_1, and that P_2 is substitutable for y in N_1. Then, $M_1[\varphi[x{:=}\ P_1, y{:=}\ P_2]] = M_1[\varphi][P_1/x]$, $N_1[\varphi[x{:=}\ P_1, y{:=}\ P_2]] = N_1[\varphi][P_2/y]$, and $P[\varphi[x{:=}\ P_1, y{:=}\ P_2]] = P[\varphi]$, since $x \notin FV(N_1) \cup FV(P)$ and $y \notin FV(M_1) \cup FV(P)$. By the induction hypothesis applied to P, M_1, N_1, and $\varphi[x{:=}\ P_1, y{:=}\ P_2]$ (for any arbitrary $P_1 \in [\![\sigma]\!]$ and $P_2 \in [\![\tau]\!]$), we have $M_1[\varphi[x{:=}\ P_1, y{:=}\ P_2]] \in [\![\delta]\!]$, $N_1[\varphi[x{:=}\ P_1, y{:=}\ P_2]] \in [\![\delta]\!]$, and $P[\varphi[x{:=}\ P_1, y{:=}\ P_2]] \in [\![\sigma + \tau]\!]$, that is, $M_1[\varphi][P_1/x] \in [\![\delta]\!]$, $N_1[\varphi][P_2/y] \in [\![\delta]\!]$, and $P[\varphi] \in [\![\sigma + \tau]\!]$. Thus, by lemma 6.9, we have $\mathtt{case}\ P[\varphi]\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M_1[\varphi] \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N_1[\varphi] \in [\![\delta]\!]$, that is, $(\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M_1 \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N_1)[\varphi] \in [\![\delta]\!]$. $\square$

Theorem 6.11 *If $\mathcal{P}$ is a family of λ-terms satisfying conditions (P1)-(P5), then $P_\sigma = \Lambda_\sigma$ for every type σ (in other words, every term satisfies the unary predicate defined by $\mathcal{P}$).*

Proof. Apply lemma 6.10 to every term M of type σ and to the identity substitution, which is legitimate since $x \in [\![\sigma]\!]$ for every variable of type σ (by lemma 6.7). $\square$

7 Adding the Absurdity Type $\perp$

The type-checking rules of the system are summarized in the following definition.

Definition 7.1 The terms of the typed λ-calculus $\lambda^{\to,\times,+,\perp}$ are defined by the following rules.

$$x{:}\,\sigma, \quad \text{when } x \in X_\sigma,$$

(we can also have $c{:}\,\sigma$, for a set of constants that have been preassigned types).

$$\frac{\triangleright\ M{:}\,\perp}{\triangleright\ \nabla_\sigma\,(M){:}\,\sigma} \quad (\perp\text{-}elim)$$

with $\sigma \neq \perp$,

$$\frac{x\colon \sigma \triangleright M\colon \tau}{\triangleright (\lambda x\colon \sigma.\, M)\colon \sigma \to \tau} \quad (abstraction)$$

$$\frac{\triangleright M\colon \sigma \to \tau \quad \triangleright N\colon \sigma}{\triangleright (MN)\colon \tau} \quad (application)$$

$$\frac{\triangleright M\colon \sigma \quad \triangleright N\colon \tau}{\triangleright \langle M, N\rangle\colon \sigma \times \tau} \quad (pairing)$$

$$\frac{\triangleright M\colon \sigma \times \tau}{\triangleright \pi_1(M)\colon \sigma} \quad (projection) \qquad \frac{\triangleright M\colon \sigma \times \tau}{\triangleright \pi_2(M)\colon \tau} \quad (projection)$$

$$\frac{\triangleright M\colon \sigma}{\triangleright \mathtt{inl}(M)\colon \sigma + \tau} \quad (injection) \qquad \frac{\triangleright M\colon \tau}{\triangleright \mathtt{inr}(M)\colon \sigma + \tau} \quad (injection)$$

$$\frac{\triangleright P\colon \sigma + \tau \quad x\colon \sigma \triangleright M\colon \delta \quad y\colon \tau \triangleright N\colon \delta}{\triangleright (\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon \sigma) \Rightarrow M \mid \mathtt{inr}(y\colon \tau) \Rightarrow N)\colon \delta} \quad (by\text{-}cases)$$

We also recall the reduction rules.

Definition 7.2 The reduction rules of the system $\lambda^{\to,\times,+,\perp}$ are listed below:

$$\begin{aligned}
(\lambda x\colon \sigma.\, M)N &\longrightarrow M[N/x],\\
\pi_1(\langle M, N\rangle) &\longrightarrow M,\\
\pi_2(\langle M, N\rangle) &\longrightarrow N,\\
\mathtt{case}\ \mathtt{inl}(P)\ \mathtt{of}\ \mathtt{inl}(x\colon \sigma) \Rightarrow M \mid \mathtt{inr}(y\colon \tau) \Rightarrow N &\longrightarrow M[P/x],\\
\mathtt{case}\ \mathtt{inr}(P)\ \mathtt{of}\ \mathtt{inl}(x\colon \sigma) \Rightarrow M \mid \mathtt{inr}(y\colon \tau) \Rightarrow N &\longrightarrow N[P/y],\\
\nabla_{\sigma\to\tau}(M)N &\longrightarrow \nabla_\tau(M),\\
\pi_1(\nabla_{\sigma\times\tau}(M)) &\longrightarrow \nabla_\sigma(M),\\
\pi_2(\nabla_{\sigma\times\tau}(M)) &\longrightarrow \nabla_\tau(M),\\
\mathtt{case}\ \nabla_{\sigma+\tau}(P)\ \mathtt{of}\ \mathtt{inl}(x\colon \sigma) \Rightarrow M \mid \mathtt{inr}(y\colon \tau) \Rightarrow N &\longrightarrow \nabla_\delta(P).
\end{aligned}$$

The reduction relation defined by the rules of definition 7.2 is still denoted as $\longrightarrow_\beta$ (even though there are reductions other that β-reduction). Definition 6.3 is extended as follows. Notice that the addition of the type $\perp$ does not change the set of simple terms.

Definition 7.3 An *I-term* is a term of the form either $\lambda x\colon \sigma.\, M$, $\langle M, N\rangle$, $\mathtt{inl}(M)$, or $\mathtt{inr}(M)$, or $\nabla_\sigma(M)$. A *simple* term (or *neutral* term) is a term that is not an I-term. Thus, a simple term is either a variable x, a constant c, an application MN, a projection $\pi_1(M)$ or $\pi_2(M)$, or a conditional term $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon \sigma) \Rightarrow M \mid \mathtt{inr}(y\colon \tau) \Rightarrow N$. A term M is *stubborn* iff it is simple and, either M is irreducible, or M' is a simple term whenever $M \xrightarrow{+}_\beta M'$ (equivalently, M' is **not** an I-term).

Definition 7.4 Properties (P1)-(P3) are defined as follows:

(P1) $x \in P_\sigma$, $c \in P_\sigma$, for every variable x and constant c of type σ.

(P2) If $M \in P_\sigma$ and $M \longrightarrow_\beta N$, then $N \in P_\sigma$.

(P3) If M is simple, then:

(1) If $M \in P_{\sigma\to\tau}$, $N \in P_\sigma$, $(\lambda x\colon\sigma.\, M')N \in P_\tau$ whenever $M \xrightarrow{+}_\beta \lambda x\colon\sigma.\, M'$, and $\nabla_{\sigma\to\tau}(M')N \in P_\tau$ whenever $M \xrightarrow{+}_\beta \nabla_{\sigma\to\tau}(M')$, then $MN \in P_\tau$.

(2) If $M \in P_{\sigma\times\tau}$, $\pi_1(\langle M', N'\rangle) \in P_\sigma$ and $\pi_2(\langle M', N'\rangle) \in P_\tau$ whenever $M \xrightarrow{+}_\beta \langle M', N'\rangle$, and $\pi_1(\nabla_{\sigma\times\tau}(M')) \in P_\sigma$ and $\pi_2(\nabla_{\sigma\times\tau}(M')) \in P_\tau$ whenever $M \xrightarrow{+}_\beta \nabla_{\sigma\times\tau}(M')$, then $\pi_1(M) \in P_\sigma$ and $\pi_2(M) \in P_\tau$.

From now on, we only consider families $\mathcal{P}$ satisfying conditions (P1)-(P3) of definition 7.4. The remarks on stubborn terms made after definition 6.4 also apply here. Definition 6.5 remains the same, except that terms of the form $\nabla_\sigma(M)$ are also I-terms.

Definition 7.5 A nonempty set C of terms of type σ is a *$\mathcal{P}$-candidate* iff it satisfies the following conditions:

(R1) $C \subseteq P_\sigma$.

(R2) If $M \in C$ and $M \longrightarrow_\beta N$, then $N \in C$.

(R3) If M is simple, $M \in P_\sigma$, and $M' \in C$ whenever $M \xrightarrow{+}_\beta M'$ and M' is an I-term, then $M \in C$.

Definition 7.6 The sets $[\![\sigma]\!]$ are defined as follows:

$$\begin{aligned}
[\![\sigma]\!] &= P_\sigma, \qquad \sigma \text{ a base type},\\
[\![\sigma\to\tau]\!] &= \{M \mid M \in P_{\sigma\to\tau},\ \text{and for all } N, \text{ if } N \in [\![\sigma]\!] \text{ then } MN \in [\![\tau]\!]\},\\
[\![\sigma\times\tau]\!] &= \{M \mid M \in P_{\sigma\times\tau},\ \pi_1(M) \in [\![\sigma]\!], \text{ and } \pi_2(M) \in [\![\tau]\!]\},\\
[\![\sigma+\tau]\!] &= \{M \mid M \in P_{\sigma+\tau},\ M' \in [\![\sigma]\!] \text{ whenever } M \xrightarrow{*}_\beta \mathtt{inl}(M')\} \cup\\
&\quad\ \{M \mid M \in P_{\sigma+\tau},\ M'' \in [\![\tau]\!] \text{ whenever } M \xrightarrow{*}_\beta \mathtt{inr}(M'')\} \cup\\
&\quad\ \{M \mid M \in P_{\sigma+\tau},\ M_1 \in P_\perp \text{ whenever } M \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(M_1)\}.
\end{aligned}$$

We now prove a generalization of lemma 6.7.

Lemma 7.7 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P3), then each $[\![\sigma]\!]$ is a $\mathcal{P}$-candidate that contains all stubborn terms in P_σ.*

Proof. We proceed by induction on types. The base case is as in lemma 5.6. The induction step has more cases since for every nonbase type σ, $\nabla_\sigma(M)$ is an I-term of type σ.

(R1). This is trivial by the definitions of $[\![\sigma]\!]$.

(R2). We need to consider the new case when $M \in [\![\sigma+\tau]\!]$. Assume that $M \longrightarrow_\beta M'$. We show that $M' \in P_{\sigma+\tau}$ and $M_1 \in P_\perp$ whenever $M' \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(M_1)$. By (P2), $M' \in P_{\sigma+\tau}$. Since

$M \longrightarrow_\beta M'$, whenever $M' \xrightarrow{*}_\beta \ \triangledown_{\sigma+\tau}(M_1)$, we have $M \xrightarrow{*}_\beta \ \triangledown_{\sigma+\tau}(M_1)$. But then, since $M \in [\![\sigma + \tau]\!]$, we have $M_1 \in P_\perp$, as desired.

(R3). Let $M \in P_\sigma$ be a simple term, and assume that $Q \in [\![\sigma]\!]$ whenever $M \xrightarrow{+}_\beta Q$ and Q is an I-term. There are new cases since $\triangledown_\sigma(M)$ is an I-term for every type σ.

1. Arrow type $\sigma \to \tau$. Let $M \in P_{\sigma\to\tau}$ be a simple term, and assume that $Q \in [\![\sigma \to \tau]\!]$ whenever $M \xrightarrow{+}_\beta Q$ and Q is an I-term. We prove that $MN \in [\![\tau]\!]$ for every $N \in [\![\sigma]\!]$. By (R1), if $N \in [\![\sigma]\!]$ then $N \in P_\sigma$. The case where M is stubborn is handled as in lemma 5.6.

Assume that $M \xrightarrow{+}_\beta Q$ where Q is an I-term. Then, either $Q = \lambda x{:}\,\sigma.M'$ or $Q = \triangledown_{\sigma\to\tau}(M_1)$. If $Q = \lambda x{:}\,\sigma.M'$, since $\lambda x{:}\,\sigma.M' \in [\![\sigma \to \tau]\!]$, we have $(\lambda x{:}\,\sigma.M')N \in [\![\tau]\!]$, and by (R1), $(\lambda x{:}\,\sigma.M')N \in P_\tau$. If $Q = \triangledown_{\sigma\to\tau}(M_1)$, then since $\triangledown_{\sigma\to\tau}(M_1) \in [\![\sigma \to \tau]\!]$, we have $\triangledown_{\sigma\to\tau}(M_1)N \in [\![\tau]\!]$, and by (R1), $\triangledown_{\sigma\to\tau}(M_1)N \in P_\tau$. By (P3)(1), $MN \in P_\tau$.

If τ is a base type, then $[\![\tau]\!] = P_\tau$ and $MN \in [\![\tau]\!]$.

If τ is not a base type, the term MN is simple. Thus, we prove that $MN \in [\![\tau]\!]$ using (R3) (which by induction, holds at type τ). The case where MN is stubborn is trivial. Otherwise, assume that $MN \xrightarrow{+}_\beta Q_1$, where Q_1 is an I-term. Observe that the reduction $MN \xrightarrow{+}_\beta Q_1$ is necessarily either of the form

$$MN \xrightarrow{+}_\beta (\lambda x{:}\,\sigma.\,M_1)N_1 \longrightarrow_\beta M_1[N_1/x] \xrightarrow{*}_\beta Q_1,$$

where $M \xrightarrow{+}_\beta \lambda x{:}\,\sigma.\,M_1$ and $N \xrightarrow{*}_\beta N_1$, or of the form

$$MN \xrightarrow{+}_\beta \ \triangledown_{\sigma\to\tau}(M_1)N_1 \longrightarrow_\beta \triangledown_\tau(M_1) \xrightarrow{*}_\beta Q_1,$$

where $M \xrightarrow{+}_\beta \ \triangledown_{\sigma\to\tau}(M_1)$ and $N \xrightarrow{*}_\beta N_1$.

The first case has already been covered in the proof of lemma 5.6, and $Q_1 \in [\![\tau]\!]$. In the second case, by assumption, $\triangledown_{\sigma\to\tau}(M_1) \in [\![\sigma \to \tau]\!]$. Since by the induction hypothesis applied at type σ, by (R2), $N_1 \in [\![\sigma]\!]$, we have $\triangledown_{\sigma\to\tau}(M_1)N_1 \in [\![\tau]\!]$. By the induction hypothesis applied at type τ, by (R2), we have $Q_1 \in [\![\tau]\!]$. Since $Q_1 \in [\![\tau]\!]$ in all cases, by the induction hypothesis and (R3), we have $MN \in [\![\tau]\!]$. But then, $M \in [\![\sigma \to \tau]\!]$.

2. Product type $\sigma\times\tau$. Let $M \in P_{\sigma\times\tau}$ be a simple term, and assume that $M' \in [\![\sigma\times\tau]\!]$ whenever $M \xrightarrow{+}_\beta M'$ and M' is an I-term. We prove that $\pi_1(M) \in [\![\sigma]\!]$ and $\pi_2(M) \in [\![\tau]\!]$. The case where M is stubborn is handled as in lemma 6.7.

Assume that $M \xrightarrow{+}_\beta M'$ where Q is an I-term. Then, either $M' = \langle M_1, N_1\rangle$ or $M' = \triangledown_{\sigma\times\tau}(M_1)$. If $M' = \langle M_1, N_1\rangle$, then $\langle M_1, N_1\rangle \in [\![\sigma\times\tau]\!]$, and we have $\pi_1(\langle M_1, N_1\rangle) \in [\![\sigma]\!]$ and $\pi_2(\langle M_1, N_1\rangle) \in [\![\tau]\!]$. By (R1), $\pi_1(\langle M_1, N_1\rangle) \in P_\sigma$ and $\pi_2(\langle M_1, N_1\rangle) \in P_\tau$. If $M' = \triangledown_{\sigma\times\tau}(M_1)$, then $\triangledown_{\sigma\times\tau}(M_1) \in [\![\sigma\times\tau]\!]$, and we have $\pi_1(\triangledown_{\sigma\times\tau}(M_1)) \in [\![\sigma]\!]$ and $\pi_2(\triangledown_{\sigma\times\tau}(M_1)) \in [\![\tau]\!]$. By (R1), $\pi_1(\triangledown_{\sigma\times\tau}(M_1)) \in P_\sigma$ and $\pi_2(\triangledown_{\sigma\times\tau}(M_1)) \in P_\tau$. By (P3)(2), we have $\pi_1(M) \in P_\sigma$ and $\pi_2(M) \in P_\tau$.

If σ is a base type, then $[\![\sigma]\!] = P_\sigma$ and $\pi_1(M) \in [\![\sigma]\!]$. Similarly, if τ is a base type, then $[\![\tau]\!] = P_\tau$ and $\pi_2(M) \in [\![\tau]\!]$.

Let us now consider the case where σ is not a base type, the case where τ is not a base type being similar. Then, we know that $\pi_1(M) \in P_\sigma$ and $\pi_1(M)$ is a simple term. We use (R3) to prove that $\pi_1(M) \in [\![\sigma]\!]$. The case where $\pi_1(M)$ is stubborn is trivial. Otherwise, assume that $\pi_1(M) \xrightarrow{+}_\beta Q$ where Q is an I-term. Observe that the reduction $\pi_1(M) \xrightarrow{+}_\beta Q$ is necessarily either of the form

$$\pi_1(M) \xrightarrow{+}_\beta \pi_1(\langle M_1, N_1\rangle) \longrightarrow_\beta M_1 \xrightarrow{*}_\beta Q,$$

where $M \xrightarrow{+}_\beta \langle M_1, N_1\rangle$, or of the form

$$\pi_1(M) \xrightarrow{+}_\beta \pi_1(\nabla_{\sigma\times\tau}(Q_1)) \longrightarrow_\beta \nabla_\sigma(Q_1) \xrightarrow{*}_\beta Q,$$

where $M \xrightarrow{+}_\beta \nabla_{\sigma\times\tau}(Q_1)$.

The first case has already been covered in the proof of lemma 6.7, and $Q \in [\![\sigma]\!]$. In the second case, by assumption, $\nabla_{\sigma\times\tau}(Q_1) \in [\![\sigma \times \tau]\!]$. Thus, $\pi_1(\nabla_{\sigma\times\tau}(Q_1)) \in [\![\sigma]\!]$, and by the induction hypothesis and (R2), we have $Q \in [\![\sigma]\!]$. Since $Q \in [\![\sigma]\!]$ in all cases, by the induction hypothesis and (R3), we have $\pi_1(M) \in [\![\sigma]\!]$. Similarly, we show that $\pi_2(M) \in [\![\tau]\!]$. But then, $M \in [\![\sigma \times \tau]\!]$.

3. Sum type $\sigma + \tau$. The case where M is stubborn is handled as in lemma 6.7. Otherwise, let $M \in P_{\sigma+\tau}$ be a simple term, and assume that $M' \in [\![\sigma + \tau]\!]$ whenever $M \xrightarrow{+}_\beta M'$ and M' is an I-term. We need to show that either $M_1 \in [\![\sigma]\!]$ whenever $M \xrightarrow{*}_\beta \mathtt{inl}(M_1)$, or $M_2 \in [\![\tau]\!]$ whenever $M \xrightarrow{*}_\beta \mathtt{inr}(M_2)$, or $M_3 \in P_\perp$ whenever $M \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(M_3)$. The first two kinds of derivations have already been covered in the proof of lemma 6.7. Assume that $M \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(M_3)$. Since $\nabla_{\sigma+\tau}(M_3)$ is an I-term, by the assumption, we have $\nabla_{\sigma+\tau}(M_3) \in [\![\sigma + \tau]\!]$. By definition of $[\![\sigma + \tau]\!]$, we have either $M_1' \in [\![\sigma]\!]$ whenever $\nabla_{\sigma+\tau}(M_3) \xrightarrow{*}_\beta \mathtt{inl}(M_1')$, or $M_2' \in [\![\tau]\!]$ whenever $\nabla_{\sigma+\tau}(M_3) \xrightarrow{*}_\beta \mathtt{inr}(M_2')$, or $M_3' \in P_\perp$ whenever $\nabla_{\sigma+\tau}(M_3) \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(M_3')$. However, the first two kinds of derivations are impossible. Thus, the third case applies, and we have $M_3 \in P_\perp$. □

Definition 7.8 Properties (P4) and (P5) are defined as follows:

(P4)

(1) If $M \in P_\tau$, then $\lambda x{:}\,\sigma.\, M \in P_{\sigma\to\tau}$.
(2) If $M \in P_\sigma$ and $N \in P_\tau$, then $\langle M, N\rangle \in P_{\sigma\times\tau}$.
(3) If $M \in P_\sigma$, then $\mathtt{inl}(M) \in P_{\sigma+\tau}$, and if $M \in P_\tau$, then $\mathtt{inr}(M) \in P_{\sigma+\tau}$.
(4) If $M \in P_\perp$, then $\nabla_\sigma(M) \in P_\sigma$.

(P5)

(1) If $N \in P_\sigma$ and $M[N/x] \in P_\tau$, then $(\lambda x{:}\,\sigma.\, M)N \in P_\tau$.
(2) If $M \in P_\sigma$ and $N \in P_\tau$, then $\pi_1(\langle M, N\rangle) \in P_\sigma$ and $\pi_2(\langle M, N\rangle) \in P_\tau$.
(3) If $P \in P_{\sigma+\tau}$, $M \in P_\delta$, $N \in P_\delta$, $M[P_1/x] \in P_\delta$ whenever $P \xrightarrow{*}_\beta \mathtt{inl}(P_1)$, $N[P_2/y] \in P_\delta$ whenever $P \xrightarrow{*}_\beta \mathtt{inr}(P_2)$, and $P_1 \in P_\perp$ whenever $P \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(P_1)$, then $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N \in P_\delta$.
(4) If $M_1 \in P_\perp$ and $N \in P_\sigma$, then $\nabla_{\sigma\to\tau}(M_1)N \in P_\tau$. If $M_1 \in P_\perp$, then $\pi_1(\nabla_{\sigma\times\tau}(M_1)) \in P_\sigma$ and $\pi_2(\nabla_{\sigma\times\tau}(M_1)) \in P_\tau$.

It is still the case that $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N \in P_\delta$ is a stubborn term in P_δ, if $P \in P_{\sigma+\tau}$ is stubborn, $M \in P_\delta$, and $N \in P_\delta$.

Lemma 7.9 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P5) then the following properties hold: (1) If for every N, ($N \in [\![\sigma]\!]$ implies $M[N/x] \in [\![\tau]\!]$), then $\lambda x{:}\,\sigma.\, M \in [\![\sigma \to \tau]\!]$; (2) If $M \in [\![\sigma]\!]$ and $N \in [\![\tau]\!]$, then $\langle M, N\rangle \in [\![\sigma \times \tau]\!]$; (3) If $P \in [\![\sigma + \tau]\!]$, for every P_1, ($P_1 \in [\![\sigma]\!]$ implies $M[P_1/x] \in [\![\delta]\!]$), and for every P_2, ($P_2 \in [\![\tau]\!]$ implies $N[P_2/y] \in [\![\delta]\!]$), then* $\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N \in [\![\delta]\!]$; *(4) If $M \in P_\perp$, then $\nabla_\sigma(M) \in [\![\sigma]\!]$ for every type σ.*

Proof. It is similar to the proof of lemma 6.9, except that we need to treat the case where $P \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(P_1)$ in (3), and we need to prove (4). By lemma 7.7, we know that the sets of the form $[\![\sigma]\!]$ have the properties (R1)-(R3).

(1) This has already been proved in lemma 6.9.

(2) This has already been proved in lemma 6.9.

(3) Assume that the hypothesis of (3) holds. First, we prove that $\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N \in P_\delta$. The case where P is stubborn is handled as in lemma 6.9. We need to consider the new case where $P \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(P')$. Since $P \in [\![\sigma + \tau]\!]$, by (R2), we have $\nabla_{\sigma+\tau}(P') \in [\![\sigma + \tau]\!]$. By definition of $[\![\sigma + \tau]\!]$, this implies that $P' \in P_\perp$. Then, by the assumption, we have $M = M[x/x] \in [\![\delta]\!]$, and $N = N[y/y] \in [\![\delta]\!]$, since by lemma 7.7, $x \in [\![\sigma]\!]$ and $y \in [\![\tau]\!]$. By (R1), we have $P \in P_{\sigma+\tau}$, $M \in P_\delta$, $N \in P_\delta$, and $P' \in P_\perp$ whenever $P \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(P')$. Thus, by (P5)(3), we have $\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N \in P_\delta$.

If δ is a base type, then $[\![\delta]\!] = P_\delta$, and $\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N \in [\![\delta]\!]$.

If δ is not a base type, then $\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N \in P_\delta$ is a simple term. We use (R3) to prove that $\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N \in [\![\delta]\!]$. The case where $\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N$ is stubborn is trivial. Otherwise, assume that $\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N \xrightarrow{+}_\beta Q$ and Q is an I-term. Then, the reduction is either of the form

$$\begin{aligned}\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N &\xrightarrow{*}_\beta \texttt{case}\ \texttt{inl}(P_1)\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M_1 \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N_1\\ &\longrightarrow_\beta M_1[P_1/x] \xrightarrow{*}_\beta Q,\end{aligned}$$

where $P \xrightarrow{*}_\beta \texttt{inl}(P_1)$, $M \xrightarrow{*}_\beta M_1$, and $N \xrightarrow{*}_\beta N_1$, or

$$\begin{aligned}\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N &\xrightarrow{*}_\beta \texttt{case}\ \texttt{inr}(P_2)\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M_1 \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N_1\\ &\longrightarrow_\beta N_1[P_2/y] \xrightarrow{*}_\beta Q,\end{aligned}$$

where $P \xrightarrow{*}_\beta \texttt{inr}(P_2)$, $M \xrightarrow{*}_\beta M_1$, and $N \xrightarrow{*}_\beta N_1$, or

$$\begin{aligned}&\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N\\ &\qquad\xrightarrow{*}_\beta \texttt{case}\ \nabla_{\sigma+\tau}(P_1)\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M_1 \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N_1 \longrightarrow_\beta \nabla_\delta(P_1) \xrightarrow{*}_\beta Q,\end{aligned}$$

where $P \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(P_1)$, $M \xrightarrow{*}_\beta M_1$, and $N \xrightarrow{*}_\beta N_1$. The first two cases have already been treated in the proof of lemma 6.9.

In the third case, since $P \in [\![\sigma + \tau]\!]$, by (R2), $\nabla_{\sigma+\tau}(P_1) \in [\![\sigma + \tau]\!]$. This implies that $P_1 \in P_\perp$. Then, by (4) (of this lemma), $\nabla_\delta(P_1) \in [\![\delta]\!]$. By (R2), we get $Q \in [\![\delta]\!]$. Finally, by (R3), we have $\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N \in [\![\delta]\!]$.

(4) We prove it by induction on σ. When σ is a base type, since $\nabla_\sigma(M) \in P_\sigma$ by (P4)(4) and since $[\![\sigma]\!] = P_\sigma$, we have $\nabla_\sigma(M) \in [\![\sigma]\!]$.

1. Arrow type $\sigma \to \tau$. We prove that $\nabla_{\sigma\to\tau}(M)N \in [\![\tau]\!]$ for every $N \in [\![\sigma]\!]$. Since $M \in P_\perp$ and by (R1) $N \in P_\sigma$, by (P5)(4), we have $\nabla_{\sigma\to\tau}(M)N \in P_\tau$. If τ is a base type, $[\![\tau]\!] = P_\tau$ and $\nabla_{\sigma\to\tau}(M)N \in [\![\tau]\!]$. Otherwise, $\nabla_{\sigma\to\tau}(M)N \in P_\tau$ is a simple term and we use (R3). The case where $\nabla_{\sigma\to\tau}(M)N$ is stubborn is trivial. Otherwise, a reduction $\nabla_{\sigma\to\tau}(M)N \xrightarrow{+}_\beta Q$ where Q is an I-term must be of the form

$$\nabla_{\sigma\to\tau}(M)N \xrightarrow{*}_\beta \nabla_{\sigma\to\tau}(M_1)N_1 \longrightarrow_\beta \nabla_\tau(M_1) \xrightarrow{*}_\beta Q,$$

where $M \xrightarrow{*}_\beta M_1$ and $N \xrightarrow{*}_\beta N_1$. By the induction hypothesis, $\nabla_\tau(M_1) \in [\![\tau]\!]$, and by (R2), we have $Q \in [\![\tau]\!]$. Thus, by (R3), we have $\nabla_{\sigma\to\tau}(M)N \in [\![\tau]\!]$.

2. Product type $\sigma \times \tau$. We prove that $\pi_1(\nabla_{\sigma\times\tau}(M)) \in [\![\sigma]\!]$ and $\pi_2(\nabla_{\sigma\times\tau}(M)) \in [\![\tau]\!]$. Since $M \in P_\perp$, by (P5)(4), we have $\pi_1(\nabla_{\sigma\times\tau}(M)) \in P_\sigma$ and $\pi_2(\nabla_{\sigma\times\tau}(M)) \in P_\tau$. If σ is a base type, then $[\![\sigma]\!] = P_\sigma$ and $\pi_1(\nabla_{\sigma\times\tau}(M)) \in [\![\sigma]\!]$. Similarly, if τ is a base type, then $[\![\tau]\!] = P_\tau$ and $\pi_2(\nabla_{\sigma\times\tau}(M)) \in [\![\tau]\!]$.

If σ is not a base type, then $\pi_1(\nabla_{\sigma\times\tau}(M)) \in P_\sigma$ is a simple term and we use (R3). The case where $\pi_1(\nabla_{\sigma\times\tau}(M))$ is stubborn is trivial. Otherwise, a reduction $\pi_1(\nabla_{\sigma\times\tau}(M)) \xrightarrow{+}_\beta Q$ where Q is an I-term must be of the form

$$\pi_1(\nabla_{\sigma\times\tau}(M)) \xrightarrow{*}_\beta \pi_1(\nabla_{\sigma\times\tau}(M_1)) \longrightarrow_\beta \nabla_\sigma(M_1) \xrightarrow{*}_\beta Q,$$

where $M \xrightarrow{*}_\beta M_1$. Since by the induction hypothesis, $\nabla_\sigma(M_1) \in [\![\sigma]\!]$, by (R2), we have $Q \in [\![\sigma]\!]$. By (R3), we have $\pi_1(\nabla_{\sigma\times\tau}(M)) \in [\![\sigma]\!]$. A similar argument applies to $\pi_2(\nabla_{\sigma\times\tau}(M))$.

3. Sum type $\sigma + \tau$. By (P4)(4), since $M \in P_\perp$, we have $\nabla_{\sigma+\tau}(M) \in P_{\sigma+\tau}$. The case where $\nabla_{\sigma+\tau}(M)$ is stubborn is trivial. Otherwise, by the definition of the third component in the union constituting $[\![\sigma + \tau]\!]$, since $M \in P_\perp$, we have $\nabla_{\sigma+\tau}(M) \in [\![\sigma + \tau]\!]$. □

Lemma 7.10 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P5), then for every term M of type σ, for every substitution φ such that $\varphi(y) \in [\![\gamma]\!]$ for every $y{:}\,\gamma \in FV(M)$, we have $M[\varphi] \in [\![\sigma]\!]$.*

Proof. We proceed by induction on the structure of M. If $M = M_1N_1$, $M = \pi_1(M_1)$, $M = \pi_2(M_1)$, $M = \langle M_1, N_1\rangle$, $M = \lambda x{:}\,\sigma.\, M_1$, or $M = \texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M_1 \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N_1$, the proof remains the same and uses lemma 7.9.

If $M = \texttt{inl}(M_1)$ where M has type $\sigma + \tau$, then by the induction hypothesis, $M_1[\varphi] \in [\![\sigma]\!]$. By (P4)(3), we have $\texttt{inl}(M_1[\varphi]) \in P_{\sigma+\tau}$. We need to show that either $N_1 \in [\![\sigma]\!]$ whenever $\texttt{inl}(M_1[\varphi]) \xrightarrow{*}_\beta \texttt{inl}(N_1)$, or $N_2 \in [\![\tau]\!]$ whenever $\texttt{inl}(M_1[\varphi]) \xrightarrow{*}_\beta \texttt{inr}(N_2)$, or $N_3 \in P_\perp$ whenever $\texttt{inl}(M_1[\varphi]) \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(N_3)$. The second and third derivations are impossible, and in the first case, we must have $M_1[\varphi] \xrightarrow{*}_\beta N_1$. Since $M_1[\varphi] \in [\![\sigma]\!]$, by (R2), we have $N_1 \in [\![\sigma]\!]$. The case where $M = \texttt{inr}(M_1)$ is similar.

If $M = \nabla_\sigma(M_1)$, then by the induction hypothesis, $M_1[\varphi] \in [\![\perp]\!] = P_\perp$. By lemma 7.9 (4), we get $\nabla_\sigma(M_1)[\varphi] \in [\![\sigma]\!]$. □

Theorem 7.11 *If $\mathcal{P}$ is a family of λ-terms satisfying conditions (P1)-(P5), then $P_\sigma = \Lambda_\sigma$ for every type σ (in other words, every term satisfies the unary predicate defined by $\mathcal{P}$).*

Proof. Apply lemma 7.10 to every term M of type σ and to the identity substitution, which is legitimate since $x \in [\![\sigma]\!]$ for every variable of type σ (by lemma 7.7). $\square$

8 Adding First-Order Quantifiers $\forall$ and $\exists$

The type-checking rules of the system are summarized in the following definition.

Definition 8.1 The terms of the typed λ-calculus $\lambda^{\to,\times,+,\forall,\exists,\perp}$ are defined by the following rules.

$$x : \sigma, \quad \text{when } x \in X_\sigma,$$

(we can also have $c : \sigma$, for a set of constants that have been preassigned types).

$$\frac{\triangleright M : \perp}{\triangleright \nabla_\sigma(M) : \sigma} \quad (\perp\textit{-elim})$$

with $\sigma \neq \perp$,

$$\frac{x : \sigma \triangleright M : \tau}{\triangleright (\lambda x : \sigma.\, M) : \sigma \to \tau} \quad (\textit{abstraction})$$

$$\frac{\triangleright M : \sigma \to \tau \quad \triangleright N : \sigma}{\triangleright (MN) : \tau} \quad (\textit{application})$$

$$\frac{\triangleright M : \sigma \quad \triangleright N : \tau}{\triangleright \langle M, N\rangle : \sigma \times \tau} \quad (\textit{pairing})$$

$$\frac{\triangleright M : \sigma \times \tau}{\triangleright \pi_1(M) : \sigma} \quad (\textit{projection}) \qquad \frac{\triangleright M : \sigma \times \tau}{\triangleright \pi_2(M) : \tau} \quad (\textit{projection})$$

$$\frac{\triangleright M : \sigma}{\triangleright \mathtt{inl}(M) : \sigma + \tau} \quad (\textit{injection}) \qquad \frac{\triangleright M : \tau}{\triangleright \mathtt{inr}(M) : \sigma + \tau} \quad (\textit{injection})$$

$$\frac{\triangleright P : \sigma + \tau \quad x : \sigma \triangleright M : \delta \quad y : \tau \triangleright N : \delta}{\triangleright (\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x : \sigma) \Rightarrow M \mid \mathtt{inr}(y : \tau) \Rightarrow N) : \delta} \quad (\textit{by-cases})$$

$$\frac{\triangleright M : \sigma[u/t]}{\triangleright (\lambda u : \iota.\, M) : \forall t.\, \sigma} \quad (\forall\textit{-intro})$$

where u does not occur free in the type of any term variable free in M, or in $\forall t.\, \sigma$;

$$\frac{\triangleright M : \forall t.\, \sigma}{\triangleright M\tau : \sigma[\tau/t]} \quad (\forall\textit{-elim})$$

$$\frac{\triangleright M : \sigma[\tau/t]}{\triangleright \mathtt{inx}(\tau, M) : \exists t.\, \sigma} \quad (\exists\textit{-intro})$$

$$\frac{\triangleright M : \exists t.\, \sigma \quad x : \sigma[u/t] \triangleright N : \delta}{\triangleright (\mathtt{casex}\ M\ \mathtt{of}\ \mathtt{inx}(u : \iota, x : \sigma[u/t]) \Rightarrow N) : \delta} \quad (\exists\textit{-elim})$$

where u does not occur free in the type of any term variable free in M, or in $\exists t.\, \sigma$, or in δ.

We also recall the reduction rules.

Definition 8.2 The reduction rules of the system $\lambda^{\rightarrow,\times,+,\forall,\exists,\perp}$ are listed below:

$$\begin{aligned}
(\lambda x\colon\sigma.\, M)N &\longrightarrow M[N/x],\\
\pi_1(\langle M, N\rangle) &\longrightarrow M,\\
\pi_2(\langle M, N\rangle) &\longrightarrow N,\\
\texttt{case inl}(P)\ \texttt{of inl}(x\colon\sigma) \Rightarrow M \mid \texttt{inr}(y\colon\tau) \Rightarrow N &\longrightarrow M[P/x],\\
\texttt{case inr}(P)\ \texttt{of inl}(x\colon\sigma) \Rightarrow M \mid \texttt{inr}(y\colon\tau) \Rightarrow N &\longrightarrow N[P/y],\\
\nabla_{\sigma\rightarrow\tau}(M)N &\longrightarrow \nabla_\tau(M),\\
\pi_1(\nabla_{\sigma\times\tau}(M)) &\longrightarrow \nabla_\sigma(M),\\
\pi_2(\nabla_{\sigma\times\tau}(M)) &\longrightarrow \nabla_\tau(M),\\
(\lambda t\colon\iota.\, M)\tau &\longrightarrow M[\tau/t],\\
\nabla_{\forall t.\,\sigma}(M)\tau &\longrightarrow \nabla_{\sigma[\tau/t]}(M),\\
\texttt{case}\ \nabla_{\sigma+\tau}(P)\ \texttt{of inl}(x\colon\sigma) \Rightarrow M \mid \texttt{inr}(y\colon\tau) \Rightarrow N &\longrightarrow \nabla_\delta(P),\\
\texttt{casex inx}(\tau, P)\ \texttt{of inx}(t\colon\iota, x\colon\sigma) \Rightarrow N &\longrightarrow N[\tau/t, P/x],\\
\texttt{casex}\ \nabla_{\exists t.\,\sigma}(P)\ \texttt{of inx}(t\colon\iota, x\colon\sigma) \Rightarrow M &\longrightarrow \nabla_\delta(P).
\end{aligned}$$

The reduction relation defined by the rules of definition 8.2 is still denoted as $\longrightarrow_\beta$ (even though there are reductions other that β-reduction). For notational convenience, we assume that there is a single sort ι and that all type variables (which are first-order) are of this sort. The generalization to the many-sorted case is straightforward, but would require writing $\forall t\colon s.\,\sigma$ and $\exists t\colon s.\,\sigma$. We simply write $\forall t.\,\sigma$ and $\exists t.\,\sigma$.

The definition of an I-term is extended as follows.

Definition 8.3 An *I-term* is a term of the form either $\lambda x\colon\sigma.M$, $\langle M, N\rangle$, $\texttt{inl}(M)$, $\texttt{inr}(M)$, $\nabla_\sigma(M)$, $\lambda t\colon\iota.\, M$, or $\texttt{inx}(\tau, M)$. A *simple* term (or *neutral* term) is a term that is not an I-term. Thus, a simple term is either a variable x, a constant c, an application MN, a projection $\pi_1(M)$ or $\pi_2(M)$, a conditional term $\texttt{case}\ P\ \texttt{of inl}(x\colon\sigma) \Rightarrow M \mid \texttt{inr}(y\colon\tau) \Rightarrow N$, a type application $M\tau$, or a term $\texttt{casex}\ P\ \texttt{of inx}(t\colon\iota, x\colon\sigma) \Rightarrow N$. A term M is *stubborn* iff it is simple and, either M is irreducible, or M' is a simple term whenever $M \xrightarrow{+}_\beta M'$ (equivalently, M' is **not** an I-term).

Actually, the universal type $\forall t.\,\sigma$ behaves much like the arrow type $\sigma \rightarrow \tau$, and the existential type $\exists x.\sigma$ behaves much like the sum type $\sigma + \tau$. This will be reflected in the conditions (P1)-(P5) and in the definition of $[\![\forall t.\,\sigma]\!]$ and $[\![\exists t.\,\sigma]\!]$. Furthermore, the proofs are also practically identical, and since we have already given complete proofs, we will only give brief sketches. Recall that $\mathcal{T}$ denotes the set of all types.

Definition 8.4 Properties (P1)-(P3) are defined as follows:

(P1) $x \in P_\sigma$, $c \in P_\sigma$, for every variable x and constant c of type σ.

(P2) If $M \in P_\sigma$ and $M \longrightarrow_\beta N$, then $N \in P_\sigma$.

(P3) If M is simple, then:

(1) If $M \in P_{\sigma\to\tau}$, $N \in P_\sigma$, $(\lambda x{:}\,\sigma.\, M')N \in P_\tau$ whenever $M \xrightarrow{+}_\beta \lambda x{:}\,\sigma.\, M'$, and $\nabla_{\sigma\to\tau}(M')N \in P_\tau$ whenever $M \xrightarrow{+}_\beta \nabla_{\sigma\to\tau}(M')$, then $MN \in P_\tau$.
(2) If $M \in P_{\sigma\times\tau}$, $\pi_1(\langle M', N'\rangle) \in P_\sigma$ and $\pi_2(\langle M', N'\rangle) \in P_\tau$ whenever $M \xrightarrow{+}_\beta \langle M', N'\rangle$, and $\pi_1(\nabla_{\sigma\times\tau}(M')) \in P_\sigma$ and $\pi_2(\nabla_{\sigma\times\tau}(M')) \in P_\tau$ whenever $M \xrightarrow{+}_\beta \nabla_{\sigma\times\tau}(M')$, then $\pi_1(M) \in P_\sigma$ and $\pi_2(M) \in P_\tau$.
(3) If $M \in P_{\forall t.\,\sigma}$, $\tau \in \mathcal{T}$, $(\lambda t{:}\,\iota.\, M')\tau \in P_{\sigma[\tau/t]}$ whenever $M \xrightarrow{+}_\beta \lambda t{:}\,\iota.\, M'$, and $\nabla_{\forall t.\,\sigma}(M')\tau \in P_{\sigma[\tau/t]}$ whenever $M \xrightarrow{+}_\beta \nabla_{\forall t.\,\sigma}(M')$, then $M\tau \in P_{\sigma[\tau/t]}$.

The remarks on stubborn terms made after definition 7.4 also apply here. Furthermore, if $M \in P_{\forall t.\,\sigma}$ is stubborn, then $M\tau$ is a stubborn term in $P_{\sigma[\tau/t]}$. Definition 7.5 remains the same, except that terms of the form $\lambda t{:}\,\iota.\, M$ or $\mathtt{inx}(\tau, M)$ are also I-terms.

Definition 8.5 A nonempty set C of terms of type σ is a $\mathcal{P}$-*candidate* iff it satisfies the following conditions:

(R1) $C \subseteq P_\sigma$.

(R2) If $M \in C$ and $M \longrightarrow_\beta N$, then $N \in C$.

(R3) If M is simple, $M \in P_\sigma$, and $M' \in C$ whenever $M \xrightarrow{+}_\beta M'$ and M' is an I-term, then $M \in C$.

Definition 8.6 The sets $[\![\sigma]\!]$ are defined as follows:

$$\begin{aligned}
[\![\sigma]\!] &= P_\sigma, \qquad \sigma \text{ a base type},\\
[\![\sigma\to\tau]\!] &= \{M \mid M \in P_{\sigma\to\tau},\ \text{and for all } N, \text{ if } N \in [\![\sigma]\!] \text{ then } MN \in [\![\tau]\!]\},\\
[\![\sigma\times\tau]\!] &= \{M \mid M \in P_{\sigma\times\tau},\ \pi_1(M) \in [\![\sigma]\!],\ \text{and } \pi_2(M) \in [\![\tau]\!]\},\\
[\![\sigma+\tau]\!] &= \{M \mid M \in P_{\sigma+\tau},\ M' \in [\![\sigma]\!] \text{ whenever } M \xrightarrow{*}_\beta \mathtt{inl}(M')\} \cup\\
&\quad\ \{M \mid M \in P_{\sigma+\tau},\ M'' \in [\![\tau]\!] \text{ whenever } M \xrightarrow{*}_\beta \mathtt{inr}(M'')\} \cup\\
&\quad\ \{M \mid M \in P_{\sigma+\tau},\ M_1 \in P_\perp \text{ whenever } M \xrightarrow{*}_\beta \nabla_{\sigma+\tau}(M_1)\},\\
[\![\forall t.\,\sigma]\!] &= \{M \mid M \in P_{\forall t.\,\sigma},\ \text{and } \forall\tau \in \mathcal{T},\ M\tau \in [\![\sigma[\tau/t]]\!]\},\\
[\![\exists t.\,\sigma]\!] &= \{M \mid M \in P_{\exists t.\,\sigma},\ \text{and } \exists\tau \in \mathcal{T},\ M' \in [\![\sigma[\tau/t]]\!] \text{ whenever } M \xrightarrow{*}_\beta \mathtt{inx}(\tau, M')\} \cup\\
&\quad\ \{M \mid M \in P_{\exists t.\,\sigma},\ M_1 \in P_\perp \text{ whenever } M \xrightarrow{*}_\beta \nabla_{\exists t.\,\sigma}(M_1)\}.
\end{aligned}$$

We now prove a generalization of lemma 7.7.

Lemma 8.7 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P3), then each $[\![\sigma]\!]$ is a $\mathcal{P}$-candidate that contains all stubborn terms in P_σ.*

Proof. The types $\forall t.\,\sigma$ and $\exists t.\,\sigma$ need to be handled. However, as we already remarked earlier, the proof for the type $\forall t.\,\sigma$ is almost exactly identical to the proof for the type $\sigma \to \tau$, and the proof for the type $\exists t.\,\sigma$ is almost exactly identical to the proof for the type $\sigma + \tau$ (see the proof of lemma 5.6 and lemma 7.7). We trust that the reader can fill in the details. $\square$

Definition 8.8 Properties (P4) and (P5) are defined as follows:

(P4)

(1) If $M \in P_\tau$, then $\lambda x\colon \sigma.\, M \in P_{\sigma\to\tau}$.
(2) If $M \in P_\sigma$ and $N \in P_\tau$, then $\langle M, N\rangle \in P_{\sigma\times\tau}$.
(3) If $M \in P_\sigma$, then $\mathtt{inl}(M) \in P_{\sigma+\tau}$, and if $M \in P_\tau$, then $\mathtt{inr}(M) \in P_{\sigma+\tau}$.
(4) If $M \in P_\perp$, then $\bigtriangledown_\sigma(M) \in P_\sigma$.
(5) If $M \in P_\sigma$, then $\lambda t\colon \iota.\, M \in P_{\forall t.\,\sigma}$.
(6) If $M \in P_{\sigma[\tau/t]}$, then $\mathtt{inx}(\tau, M) \in P_{\exists t.\,\sigma}$.

(P5)

(1) If $N \in P_\sigma$ and $M[N/x] \in P_\tau$, then $(\lambda x\colon \sigma.\, M)N \in P_\tau$.
(2) If $M \in P_\sigma$ and $N \in P_\tau$, then $\pi_1(\langle M, N\rangle) \in P_\sigma$ and $\pi_2(\langle M, N\rangle) \in P_\tau$.
(3) If $P \in P_{\sigma+\tau}$, $M \in P_\delta$, $N \in P_\delta$, $M[P_1/x] \in P_\delta$ whenever $P \xrightarrow{*}_\beta \mathtt{inl}(P_1)$, $N[P_2/y] \in P_\delta$ whenever $P \xrightarrow{*}_\beta \mathtt{inr}(P_2)$, and $P_1 \in P_\perp$ whenever $P \xrightarrow{*}_\beta \bigtriangledown_{\sigma+\tau}(P_1)$, then $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon \sigma) \Rightarrow M \mid \mathtt{inr}(y\colon \tau) \Rightarrow N \in P_\delta$.
(4) If $M_1 \in P_\perp$ and $N \in P_\sigma$, then $\bigtriangledown_{\sigma\to\tau}(M_1)N \in P_\tau$. If $M_1 \in P_\perp$, then $\pi_1(\bigtriangledown_{\sigma\times\tau}(M_1)) \in P_\sigma$ and $\pi_2(\bigtriangledown_{\sigma\times\tau}(M_1)) \in P_\tau$. If $M_1 \in P_\perp$ and $\tau \in \mathcal{T}$, then $\bigtriangledown_{\forall t.\,\sigma}(M_1)\tau \in P_{\sigma[\tau/t]}$.
(5) If $\tau \in \mathcal{T}$ and $M[\tau/t] \in P_{\sigma[\tau/t]}$, then $(\lambda t\colon \iota.\, M)\tau \in P_{\sigma[\tau/t]}$.
(6) If $P \in P_{\exists t.\,\sigma}$, $N \in P_\delta$, $N[P_1/x, \tau/t] \in P_\delta$ whenever $P \xrightarrow{*}_\beta \mathtt{inx}(\tau, P_1)$, and $P_1 \in P_\perp$ whenever $P \xrightarrow{*}_\beta \bigtriangledown_{\exists t.\,\sigma}(P_1)$, then $\mathtt{casex}\ P\ \mathtt{of}\ \mathtt{inx}(t\colon \iota, x\colon \sigma) \Rightarrow N \in P_\delta$.

The remark on stubborn terms made after definition 7.8 also applies here. Furthermore, if $P \in P_{\exists t.\,\sigma}$ is stubborn and $N \in P_\delta$, then $\mathtt{casex}\ P\ \mathtt{of}\ \mathtt{inx}(t\colon \iota, x\colon \sigma) \Rightarrow N$ is a stubborn term in P_δ.

Lemma 8.9 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P5) then the following properties hold: (1) If for every N, ($N \in [\![\sigma]\!]$ implies $M[N/x] \in [\![\tau]\!]$), then $\lambda x\colon \sigma.\, M \in [\![\sigma \to \tau]\!]$; (2) If $M \in [\![\sigma]\!]$ and $N \in [\![\tau]\!]$, then $\langle M, N\rangle \in [\![\sigma \times \tau]\!]$; (3) If $P \in [\![\sigma + \tau]\!]$, for every P_1, ($P_1 \in [\![\sigma]\!]$ implies $M[P_1/x] \in [\![\delta]\!]$), and for every P_2, ($P_2 \in [\![\tau]\!]$ implies $N[P_2/y] \in [\![\delta]\!]$), then* $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon \sigma) \Rightarrow M \mid \mathtt{inr}(y\colon \tau) \Rightarrow N \in [\![\delta]\!]$*; (4) If $M \in P_\perp$, then $\bigtriangledown_\sigma(M) \in [\![\sigma]\!]$ for every type σ. (5) If for every τ, ($\tau \in \mathcal{T}$ implies $M[\tau/t] \in [\![\sigma[\tau/t]]\!]$), then $\lambda t\colon \iota.\, M \in [\![\forall t.\, \sigma]\!]$; (6) If $P \in [\![\exists t.\, \sigma]\!]$, and for every P_1, for every $\tau \in \mathcal{T}$, ($P_1 \in [\![\sigma[\tau/t]]\!]$ implies $N[P_1/x, \tau/t] \in [\![\delta]\!]$), then* $\mathtt{casex}\ P\ \mathtt{of}\ \mathtt{inx}(t\colon \iota, x\colon \sigma) \Rightarrow N \in [\![\delta]\!]$.

Proof. It is similar to the proof of lemma 7.9, but we need to cover (5) and (6). Actually, the proof of (5) is almost exactly identical to the proof of (1), and the proof of (6) is almost exactly identical to the proof of (3) (see the proof of lemma 7.9). We trust that the reader can fill in the details. $\square$

For the next lemma, we need to consider substitutions φ whose domain is the union of a finite set of term variables and a finite set of type variables. Such substitutions assign types to type variables and terms to term variables. We let $FV(M)$ denote the set of free type and term variables in the term M.

Lemma 8.10 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P5), then for every term M of type σ, for every substitution φ such that $\varphi(y) \in [\![\gamma]\!]$ for every term variable $y\colon \gamma \in FV(M)$, we have $M[\varphi] \in [\![\sigma[\varphi]]\!]$.*

Proof. A minor difference with the proof of lemma 7.10 is that the substitution φ is applied to the type σ in $[\![\sigma[\varphi]]\!]$ (actually, the type-substitution part of φ is applied to σ). The proof that $(\lambda t{:}\,\iota.\ M)[\varphi] \in [\![(\forall t.\ \sigma)[\varphi]]\!]$ is very similar to the proof that $(\lambda x{:}\,\sigma.\ M)[\varphi] \in [\![(\sigma \to \tau)[\varphi]]\!]$, and the proof that $(M\tau)[\varphi] \in [\![\sigma[\tau/t][\varphi]]\!]$ is very similar to the proof that $(MN)[\varphi] \in [\![\tau[\varphi]]\!]$. The only (minor) difference is that we consider substitutions $\varphi[t{:=}\ \tau]$ (instead of $\varphi[x{:=}\ N]$). The proof that $\mathtt{inx}(\tau, M)[\varphi] \in [\![(\exists t.\ \sigma)[\varphi]]\!]$ is very similar to the proof that $\mathtt{inl}(M)[\varphi] \in [\![(\sigma + \tau)[\varphi]]\!]$ and $\mathtt{inr}(M)[\varphi] \in [\![(\sigma + \tau)[\varphi]]\!]$. The proof that $(\mathtt{casex}\ P\ \mathtt{of}\ \mathtt{inx}(t{:}\,\iota, x{:}\,\sigma) \Rightarrow N)[\varphi] \in [\![\delta[\varphi]]\!]$ is very similar to the proof that $(\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N)[\varphi] \in [\![\delta[\varphi]]\!]$. The only (minor) difference is that we consider substitutions $\varphi[t{:=}\ \tau, x{:=}\ P_1]$ (instead of $\varphi[x{:=}\ P_1, y{:=}\ P_2]$). We trust that the reader can fill in the details. $\square$

Theorem 8.11 *If $\mathcal{P}$ is a family of λ-terms satisfying conditions (P1)-(P5), then $P_\sigma = \Lambda_\sigma$ for every type σ (in other words, every term satisfies the unary predicate defined by $\mathcal{P}$).*

Proof. Apply lemma 8.10 to every term M of type σ and to the identity substitution, which is legitimate since $x \in [\![\sigma]\!]$ for every variable of type σ (by lemma 8.7). $\square$

As a consequence of theorem 8.11, we can prove that reduction in the system $\lambda^{\to,\times,+,\forall,\exists,\perp}$ is strongly normalizing (SN) and confluent. These are nontrivial results.

Theorem 8.12 *The reduction relation $\xrightarrow{*}_\beta$ of the system $\lambda^{\to,\times,+,\forall,\exists,\perp}$ is strongly normalizing.*

Proof. Let $\mathcal{P}$ be the family defined such that $P_\sigma = SN_\sigma$ is the set of strongly normalizing terms of type σ. By theorem 8.11, we just have to check that $\mathcal{P}$ satisfies the 17 conditions of (P1)-(P5)! Actually, this is quite easy, as we shall see. First, we make the following observation that will simplify the proof. Since there is only a finite number of redexes in any term, for any term M, the reduction tree[5] for M is finitely branching. Thus, if M is any strongly normalizing term (abbreviated as *SN term* from now on), every path in its reduction tree is finite, and since this tree is finite branching, by König's lemma, this reduction tree is finite. Thus, for any SN term M, the depth[6] of its reduction tree is a natural number, and we will denote it as $d(M)$. We now check the conditions (P1)-(P5). (P1) and (P2) are obvious.

(P3)(1) Since $M \in SN_{\sigma\to\tau}$ and $N \in SN_\sigma$, $d(M)$ and $d(N)$ are finite. We prove by induction on $d(M) + d(N)$ that MN is SN. We consider all possible ways that $MN \longrightarrow_\beta P$. Since M is simple, MN itself is not a redex, and so $P = M_1N_1$ where either $N = N_1$ and $M \longrightarrow_\beta M_1$, or $M = M_1$ and $N \longrightarrow_\beta N_1$.

If M_1 is simple or $M_1 = M$, $d(M_1) + d(N_1) < d(M) + d(N)$, and by the induction hypothesis, $P = M_1N_1$ is SN. Otherwise, there are two cases. If $M_1 = \lambda x{:}\,\sigma.\ M'$, $N_1 = N$, by assumption $(\lambda x{:}\,\sigma.\ M')N$ is SN, and so P is SN. If $M_1 = \nabla_{\sigma\to\tau}(M')$, $N_1 = N$, by assumption, $\nabla_{\sigma\to\tau}(M')N$ is SN, and so is P. Thus, $P = M_1N_1$ is SN in all cases, and MN is SN.

(P3)(2) Since $M \in P_{\sigma\times\tau}$ is SN, $d(M)$ is finite. We prove by induction on $d(M)$ that $\pi_1(M)$ is SN (and that $\pi_2(M)$ is SN). Since M is simple, $\pi_1(M)$ itself is not a redex, and if $\pi_1(M) \longrightarrow_\beta P$, then $P = \pi_1(M_1)$ and $M \longrightarrow_\beta M_1$. If M_1 is simple, then $d(M_1) < d(M)$, and by the induction

[5] the tree of reduction sequences from M

[6] the length of a longest path in the tree, counting the number of edges

hypothesis, $\pi_1(M_1)$ is SN. Otherwise, there are two cases. If $M_1 = \langle M', N' \rangle$, by assumption, $P = \pi_1(\langle M', N' \rangle)$ is SN. If $M_1 = \bigtriangledown_{\sigma\times\tau}(M')$, by assumption, $P = \pi_1(\bigtriangledown_{\sigma\times\tau}(\langle M', N' \rangle))$ is SN. Then, in all cases, P is SN, and so $\pi_1(M)$ is SN. A similar argument applies to $\pi_2(M)$.

(P3)(3) This case is quite similar to (P3)(1). Since $M \in SN_{\sigma\to\tau}$, $d(M)$ is finite. We prove by induction on $d(M)$ that $M\tau$ is SN. We consider all possible ways that $M\tau \longrightarrow_\beta P$. Since M is simple, $M\tau$ itself is not a redex, and so $P = M_1\tau$ where $M \longrightarrow_\beta M_1$. If M_1 is simple, $d(M_1) < d(M)$, and by the induction hypothesis, $P' = M_1\tau$ is SN. Otherwise, there are two cases. If $M_1 = \lambda t{:}\,\iota.\ M'$, by assumption, $P = (\lambda t{:}\,\iota.\ M')\tau$ is SN. If $M_1 = \bigtriangledown_{\forall t.\,\sigma}(M')$, by assumption, $P = \bigtriangledown_{\forall t.\,\sigma}(M')\tau$ is SN. But then, $P = M_1\tau$ is SN in all cases, and so $M\tau$ is SN.

(P4) These cases are all similar, and hold because a reduction cannot apply at the outermost level.

(P4)(1) Any reduction from $\lambda x{:}\,\sigma.\ M$ must be of the form $\lambda x{:}\,\sigma.\ M \xrightarrow{+}_\beta \lambda x{:}\,\sigma.\ M'$ where $M \xrightarrow{+}_\beta M'$. We use a simple induction on $d(M)$.

(P4)(2) Any reduction from $\langle M, N \rangle$ is of the form $\langle M, N \rangle \xrightarrow{*}_\beta \langle M', N' \rangle$ where $M \xrightarrow{*}_\beta M'$ and $N \xrightarrow{*}_\beta N'$. We use a simple induction on $d(M) + d(N)$.

(P4)(3) Any reduction from $\mathtt{inl}(M)$ is of the form $\mathtt{inl}(M) \xrightarrow{+}_\beta \mathtt{inl}(M')$ where $M \xrightarrow{+}_\beta M'$. We use a simple induction on $d(M)$. The case of $\mathtt{inr}(M)$ is similar.

(P4)(4) Similar to (P4)(3).

(P4)(5) Similar to (P4)(1).

(P4)(6) Similar to (P4)(3).

(P5) The proof of these cases is rather similar to the proof used in (P3).

(P5)(1) Since $N \in SN_\sigma$ and $M[N/x] \in SN_\tau$, the term M itself is SN. Thus, $d(M)$ and $d(N)$ are finite. We prove by induction on $d(M) + d(N)$ that $(\lambda x{:}\,\sigma.\,M)N$ is SN. We consider all possible ways that $(\lambda x{:}\,\sigma.\,M)N \longrightarrow_\beta P$. Either $P = (\lambda x{:}\,\sigma.\,M_1)N$ where $M \longrightarrow_\beta M_1$, or $P = (\lambda x{:}\,\sigma.\,M)N_1$ where $N \longrightarrow_\beta N_1$, or $P = M[N/x]$. In the first two cases, $d(M_1) + d(N) < d(M) + d(N)$, $d(M) + d(N_1) < d(M) + d(N)$, and by the induction hypothesis, P is SN. In the third case, by assumption $M[N/x]$ is SN. But then, P is SN in all cases, and so $(\lambda x{:}\,\sigma.\ M)N$ is SN.

(P5)(2) Since $M \in SN_\sigma$ and $N \in SN_\sigma$, then $d(M)$ and $d(N)$ are finite. We prove by induction on $d(M) + d(N)$ that $\pi_1(\langle M, N \rangle) \in SN_\sigma$ and $\pi_2(\langle M, N \rangle) \in SN_\tau$. If $\pi_1(\langle M, N \rangle) \longrightarrow_\beta P$, then either $P = \pi_1(\langle M_1, N \rangle)$ and $M \longrightarrow_\beta M_1$, or $P = \pi_1(\langle M, N_1 \rangle)$ and $N \longrightarrow_\beta N_1$, or $P = M$.

In the first two cases, $d(M_1) + d(N) < d(M) + d(N)$, $d(M) + d(N_1) < d(M) + d(N)$, and by the induction hypothesis, P is SN. In the third case, by assumption M is SN. But then, P is SN in all cases, and so $\pi_1(\langle M, N \rangle)$ is SN. A similar argument applies to $\pi_2(\langle M, N \rangle)$.

(P5)(3) Since $P \in SN_{\sigma+\tau}$, $M \in SN_\delta$, and $N \in SN_\delta$, $d(P)$, $d(M)$, and $d(N)$ are finite. We prove by induction on $d(P) + d(M) + d(N)$ that $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N$ is SN. If $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N \longrightarrow_\beta Q$, then either $Q = \mathtt{case}\ P_1\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N$ and $P \longrightarrow_\beta P_1$, or $Q = \mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M_1 \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N$ and $M \longrightarrow_\beta M_1$, or $Q = \mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N_1$ and $N \longrightarrow_\beta N_1$, or $P = \mathtt{inl}(P_1)$ and $Q = M[P_1/x]$, or $P = \mathtt{inr}(P_2)$ and $Q = N[P_2/y]$, or $P = \bigtriangledown_{\sigma+\tau}(P_1)$ and $Q = \bigtriangledown_\delta(P_1)$.

In the first three cases, $d(P_1) + d(M) + d(N) < d(P) + d(M) + d(N)$, $d(P) + d(M_1) + d(N) < d(P) + d(M) + d(N)$, and $d(P) + d(M) + d(N_1) < d(P) + d(M) + d(N)$, and by the induction hypothesis, Q is SN. In the fourth case, by the assumption $M[P_1/x] = Q$ is SN. In the fifth case, by the assumption $N[P_2/y] = Q$ is SN. In the sixth case, by the assumption, P_1 is SN, which implies that $Q = \nabla_\delta(P_1)$ is SN. In all cases, Q is SN, and thus $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x{:}\,\sigma) \Rightarrow M \mid \mathtt{inr}(y{:}\,\tau) \Rightarrow N$ is SN.

(P5)(4) Since $M_1 \in SN_\perp$ and $N \in SN_\sigma$, $d(M_1)$ and $d(N)$ are finite. We prove by induction on $d(M_1) + d(N)$ that $\nabla_{\sigma\to\tau}(M_1)N$ is SN. If $\nabla_{\sigma\to\tau}(M_1)N \longrightarrow_\beta P$, then either $M_1 \longrightarrow_\beta M_2$, or $N \longrightarrow_\beta N_1$, or $P = \nabla_\tau(M_1)$. In the first two cases, since $d(M_2) + d(N) < d(M_1) + d(N)$ and $d(M_1) + d(N_1) < d(M_1) + d(N)$, we conclude by applying the induction hypothesis. When $P = \nabla_\tau(M_1)$, since M_1 is SN and reductions cannot apply at the outermost level, P must be SN too. Thus, P is SN in all cases, and $\nabla_{\sigma\to\tau}(M_1)N$ is SN.

If M_1 is SN, then $d(M_1)$ is finite. We prove by induction on $d(M_1)$ that $\pi_1(\nabla_{\sigma\times\tau}(M_1))$ and $\pi_2(\nabla_{\sigma\times\tau}(M_1))$ are SN. If $\pi_1(\nabla_{\sigma\times\tau}(M_1)) \longrightarrow_\beta P$, then either $M_1 \longrightarrow_\beta M_2$, or $P = \nabla_\sigma(M_1)$. In the first case, $d(M_2) < d(M_1)$ and we apply the induction hypothesis. When $P = \nabla_\sigma(M_1)$, since M_1 is SN, so is $P = \nabla_\sigma(M_1)$. Thus, P is SN in all cases, and $\pi_1(\nabla_{\sigma\times\tau}(M_1))$ is SN. A similar proof applies to $\pi_2(\nabla_{\sigma\times\tau}(M_1))$.

If $M_1 \in SN_\perp$ then $d(M_1)$ is finite. We prove by induction on $d(M_1)$ that $\nabla_{\forall t.\,\sigma}(M_1)\tau$ is SN. If $\nabla_{\forall t.\,\sigma}(M_1)\tau \longrightarrow_\beta P$, then either $M_1 \longrightarrow_\beta M_2$, or $P = \nabla_{\sigma[\tau/t]}(M_1)$. In the first case, $d(M_2) < d(M_1)$ and we apply the induction hypothesis. When $P = \nabla_{\sigma[\tau/t]}(M_1)$, since M_1 is SN, so is $P = \nabla_{\sigma[\tau/t]}(M_1)$. Thus, P is SN in all cases, and so is $\nabla_{\forall t.\,\sigma}(M_1)\tau$.

(P5)(5) This case is quite similar to (P5)(1). Since $M[\tau/t] \in SN_{\sigma[\tau/t]}$, the term M itself is SN. Thus, $d(M)$ is finite. We prove by induction on $d(M)$ that $(\lambda t{:}\,\iota.\, M)\tau$ is SN. We consider all possible ways that $(\lambda t{:}\,\iota.\, M)\tau \longrightarrow_\beta P$. Either $P = (\lambda t{:}\,\iota.\, M_1)\tau$ where $M \longrightarrow_\beta M_1$, or $P = M[\tau/t]$. In the first case, $d(M_1) < d(M)$, and by the induction hypothesis, P is SN. In the second case, by assumption $M[\tau/t]$ is SN. But then, P is SN in all cases, and so $(\lambda t{:}\,\iota.\, M)\tau$ is SN.

(P5)(6) This case is quite similar to (P5)(3). Since $P \in SN_{\exists t.\,\sigma}$ and $N \in SN_\delta$, $d(P)$ and $d(N)$ are finite. We prove by induction on $d(P) + d(N)$ that $\mathtt{casex}\ P\ \mathtt{of}\ \mathtt{inx}(t{:}\,\iota, x{:}\,\sigma) \Rightarrow N$ is SN. If $\mathtt{casex}\ P\ \mathtt{of}\ \mathtt{inx}(t{:}\,\iota, x{:}\,\sigma) \Rightarrow N \longrightarrow_\beta Q$, then either $Q = \mathtt{casex}\ P_1\ \mathtt{of}\ \mathtt{inx}(t{:}\,\iota, x{:}\,\sigma) \Rightarrow N$ and $P \longrightarrow_\beta P_1$, or $Q = \mathtt{casex}\ P\ \mathtt{of}\ \mathtt{inx}(t{:}\,\iota, x{:}\,\sigma) \Rightarrow N_1$ and $N \longrightarrow_\beta N_1$, or $P = \mathtt{inx}(\tau, P_1)$ and $Q = N[P_1/x, \tau/t]$, or $P = \nabla_{\exists t.\,\sigma}(P_1)$ and $Q = \nabla_\delta(P_1)$.

In the first two cases, $d(P_1) + d(N) < d(P) + d(N)$ and $d(P) + d(N_1) < d(P) + d(N)$, and by the induction hypothesis, Q is SN. In the third case, by the assumption $N[P_1/x, \tau/t] = Q$ is SN. In the fourth case, by the assumption, P_1 is SN, which implies that $Q = \nabla_\delta(P_1)$ is SN. In all cases, Q is SN, and thus $\mathtt{casex}\ P\ \mathtt{of}\ \mathtt{inx}(t{:}\,\iota, x{:}\,\sigma) \Rightarrow N$ is SN.

This concludes all 17 cases, and the proof! $\square$

Theorem 8.13 *The reduction relation $\xrightarrow{*}_\beta$ of the system $\lambda^{\to,\times,+,\forall,\exists,\perp}$ is confluent.*

Proof. Let $\mathcal{P}$ be the family defined such that P_σ is the set of terms of type σ from which confluence holds, i.e., terms M such that if $M \xrightarrow{*}_\beta M_1$ and $M \xrightarrow{*}_\beta M_2$, then there is some M_3 such that $M_1 \xrightarrow{*}_\beta M_3$ and $M_2 \xrightarrow{*}_\beta M_3$. By theorem 8.11, we just have to check that $\mathcal{P}$ satisfies the 17 conditions of (P1)-(P5)! Conditions (P1) and (P2) are trivial.

(P3)(1) A reduction $MN \xrightarrow{*}_\beta Q$ either has the property that $Q = M_1N_1$, $M \xrightarrow{*}_\beta M_1$ and $N \xrightarrow{*}_\beta N_1$, in which case we say that M and N have independent reductions, or that

$$MN \xrightarrow{+}_\beta (\lambda x{:}\,\sigma.\, M_1)N \xrightarrow{*}_\beta (\lambda x{:}\,\sigma.\, M_1)N_1 \longrightarrow_\beta M_1[N_1/x] \xrightarrow{*}_\beta Q,$$

or

$$MN \xrightarrow{+}_\beta \nabla_{\sigma\to\tau}\,(M_1)N \xrightarrow{*}_\beta \nabla_{\sigma\to\tau}\,(M_1)N_1 \longrightarrow_\beta \nabla_\tau(M_1) \xrightarrow{*}_\beta Q,$$

in which case we say that there is a top level redex. By assumption, confluence holds from M and N. This implies that we cannot have "mixed" reductions $M \xrightarrow{+}_\beta \nabla_{\sigma\to\tau}\,(M_1)$ and $M \xrightarrow{+}_\beta \lambda x{:}\,\sigma.\, M_2$. There are seven subcases.

(1) Two reductions in which M and N have independent reductions: $MN \xrightarrow{*}_\beta M_1N_1$ and $MN \xrightarrow{*}_\beta M_2N_2$.

Since confluence holds from M and N, there are M_3 and N_3 such that $M_1 \xrightarrow{*}_\beta M_3$, $M_2 \xrightarrow{*}_\beta M_3$, $N_1 \xrightarrow{*}_\beta N_3$, and $N_2 \xrightarrow{*}_\beta N_3$. Then M_3N_3 is such that $M_1N_1 \xrightarrow{*}_\beta M_3N_3$ and $M_2N_2 \xrightarrow{*}_\beta M_3N_3$.

(2) Two reductions, each with a top level redex:

$$MN \xrightarrow{+}_\beta (\lambda x{:}\,\sigma.\, M_1)N \xrightarrow{*}_\beta (\lambda x{:}\,\sigma.\, M_1)N_1 \longrightarrow_\beta M_1[N_1/x] \xrightarrow{*}_\beta Q_1$$

and

$$MN \xrightarrow{+}_\beta (\lambda x{:}\,\sigma.\, M_2)N \xrightarrow{*}_\beta (\lambda x{:}\,\sigma.\, M_2)N_2 \longrightarrow_\beta M_2[N_2/x] \xrightarrow{*}_\beta Q_2.$$

Since confluence holds from M, there is an M_3 such that $\lambda x{:}\,\sigma.M_1 \xrightarrow{*}_\beta M_3$, and $\lambda x{:}\,\sigma.M_2 \xrightarrow{*}_\beta M_3$. Then,

$$(\lambda x{:}\,\sigma.\, M_1)N \xrightarrow{*}_\beta P \quad \text{and} \quad (\lambda x{:}\,\sigma.\, M_2)N \xrightarrow{*}_\beta P,$$

with $P = M_3N$. Thus, we have reductions

$$(\lambda x{:}\,\sigma.\, M_1)N \xrightarrow{*}_\beta Q_1 \quad \text{and} \quad (\lambda x{:}\,\sigma.\, M_1)N \xrightarrow{*}_\beta P.$$

By assumption, confluence holds from $(\lambda x{:}\,\sigma.\, M_1)N$, and there is some Q_3 such that $Q_1 \xrightarrow{*}_\beta Q_3$ and $P \xrightarrow{*}_\beta Q_3$. Now, we also have reductions

$$(\lambda x{:}\,\sigma.\, M_2)N \xrightarrow{*}_\beta Q_2 \quad \text{and} \quad (\lambda x{:}\,\sigma.\, M_2)N \xrightarrow{*}_\beta P \xrightarrow{*}_\beta Q_3.$$

By assumption, confluence holds from $(\lambda x{:}\,\sigma.M_2)N$, and there is some Q_4 such that $Q_2 \xrightarrow{*}_\beta Q_4$ and $Q_3 \xrightarrow{*}_\beta Q_4$. Putting the reductions $Q_1 \xrightarrow{*}_\beta Q_3$ and $Q_3 \xrightarrow{*}_\beta Q_4$ together, and have a reduction $Q_1 \xrightarrow{*}_\beta Q_4$, and we see that there is conluence in Q_4 since $Q_1 \xrightarrow{*}_\beta Q_4$ and $Q_2 \xrightarrow{*}_\beta Q_4$.

The above reductions are indicated in the following diagram.

$$
\begin{tikzcd}[column sep=small]
 & MN \arrow[dl] \arrow[dr] & & \\
(\lambda x\colon \sigma.\, M_1)N \arrow[dd] \arrow[dr] & & (\lambda x\colon \sigma.\, M_2)N \arrow[dl] \arrow[dr] & \\
 & P \arrow[ddd] & & (\lambda x\colon \sigma.\, M_2)N_2 \arrow[ddd] \\
(\lambda x\colon \sigma.\, M_1)N_1 \arrow[d] & & & \\
Q_1 \arrow[dr] & & & \\
 & Q_3 \arrow[dr] & & Q_2 \arrow[dl] \\
 & & Q_4 &
\end{tikzcd}
$$

(3) Two reductions, one with a top level redex, the other with independence:

$$MN \xrightarrow{+}_{\beta} (\lambda x\colon \sigma.\, M_1)N \xrightarrow{*}_{\beta} (\lambda x\colon \sigma.\, M_1)N_1 \longrightarrow_{\beta} M_1[N_1/x] \xrightarrow{*}_{\beta} Q_1$$

and

$$MN \xrightarrow{*}_{\beta} M_2N_2 = Q_2.$$

As in case (2), using confluence from M and N, we get a P such that

$$(\lambda x\colon \sigma.\, M_1)N \xrightarrow{*}_{\beta} P \quad \text{and} \quad Q_2 = M_2N_2 \xrightarrow{*}_{\beta} P.$$

Since by assumption, confluence holds from $(\lambda x\colon \sigma.\, M_1)N$, there is a Q_3 such that $Q_1 \xrightarrow{*}_{\beta} Q_3$ and $P \xrightarrow{*}_{\beta} Q_3$, which yields confluence.

The above reductions are indicated in the following diagram.

$$
\begin{tikzcd}
 & MN \arrow[dl] \arrow[dr] & \\
(\lambda x\colon\sigma.\, M_1)N \arrow[dr] \arrow[dd] & & Q_2 = M_2N_2 \arrow[dl] \\
 & P \arrow[ddd] & \\
(\lambda x\colon\sigma.\, M_1)N_1 \arrow[d] & & \\
Q_1 \arrow[dr] & & \\
 & Q_3 &
\end{tikzcd}
$$

(4) Symmetric to case (3).

(5)

$$MN \xrightarrow{+}_\beta \ \bigtriangledown_{\sigma\to\tau}(M_1)N \xrightarrow{*}_\beta \ \bigtriangledown_{\sigma\to\tau}(M_1)N_1 \longrightarrow_\beta \bigtriangledown_\tau(M_1) \xrightarrow{*}_\beta Q_1,$$

and

$$MN \xrightarrow{+}_\beta \ \bigtriangledown_{\sigma\to\tau}(M_2)N \xrightarrow{*}_\beta \ \bigtriangledown_{\sigma\to\tau}(M_2)N_2 \longrightarrow_\beta \bigtriangledown_\tau(M_2) \xrightarrow{*}_\beta Q_2.$$

Since confluence holds from M, there is some M_3 such that

$$\bigtriangledown_{\sigma\to\tau}(M_1) \xrightarrow{*}_\beta M_3 \quad \text{and} \quad \bigtriangledown_{\sigma\to\tau}(M_2) \xrightarrow{*}_\beta M_3.$$

Then, letting $P = M_3N$, we have

$$\bigtriangledown_{\sigma\to\tau}(M_1)N \xrightarrow{*}_\beta P \quad \text{and} \quad \bigtriangledown_{\sigma\to\tau}(M_2)N \xrightarrow{*}_\beta P.$$

Since we also have $\bigtriangledown_{\sigma\to\tau}(M_1)N \xrightarrow{*}_\beta Q_1$, and by assumption, confluence holds from $\bigtriangledown_{\sigma\to\tau}(M_1)N$, there is some Q_3 such that $Q_1 \xrightarrow{*}_\beta Q_3$ and $P \xrightarrow{*}_\beta Q_3$. But now,

$$\bigtriangledown_{\sigma\to\tau}(M_2)N \xrightarrow{*}_\beta P \xrightarrow{*}_\beta Q_3 \quad \text{and} \quad \bigtriangledown_{\sigma\to\tau}(M_2)N \xrightarrow{*}_\beta Q_2.$$

Since by assumption, confluence holds from $\bigtriangledown_{\sigma\to\tau}(M_2)N$, there is some Q_4 such that $Q_2 \xrightarrow{*}_\beta Q_4$ and $Q_3 \xrightarrow{*}_\beta Q_4$, and we have confluence in Q_4.

The above reductions are indicated in the following diagram.

$$
\begin{tikzcd}
 & MN \arrow[dl] \arrow[dr] & & & \\
\nabla_{\sigma\to\tau}(M_1)N \arrow[d] \arrow[dr] & & \nabla_{\sigma\to\tau}(M_2)N \arrow[dl] \arrow[dr] & & \\
\nabla_{\sigma\to\tau}(M_1)N_1 \arrow[d] & P \arrow[dd] & & \nabla_{\sigma\to\tau}(M_2)N_2 \arrow[dd] & \\
Q_1 \arrow[dr] & & & & \\
 & Q_3 \arrow[dr] & & Q_2 \arrow[dl] & \\
 & & Q_4 & &
\end{tikzcd}
$$

(6)

$$MN \xrightarrow{+}_\beta \nabla_{\sigma\to\tau}(M_1)N \xrightarrow{*}_\beta \nabla_{\sigma\to\tau}(M_1)N_1 \longrightarrow_\beta \nabla_\tau(M_1) \xrightarrow{*}_\beta Q_1,$$

and

$$MN \xrightarrow{*}_\beta M_2N_2 = Q_2.$$

Since confluence holds from M, there is some M_3 such that

$$\nabla_{\sigma\to\tau}(M_1) \xrightarrow{*}_\beta M_3 \quad \text{and} \quad M_2 \xrightarrow{*}_\beta M_3.$$

Then, letting $P = M_3N$, we have

$$\nabla_{\sigma\to\tau}(M_1)N \xrightarrow{*}_\beta P \quad \text{and} \quad Q_2 = M_2N_2 \xrightarrow{*}_\beta P.$$

Since by assumption, confluence holds from $\nabla_{\sigma\to\tau}(M_1)N$, there is some Q_3 such that $Q_1 \xrightarrow{*}_\beta Q_3$ and $P \xrightarrow{*}_\beta Q_3$.

The above reductions are indicated in the following diagram.

$$
\begin{tikzcd}
 & MN \arrow[dl] \arrow[dr] & \\
\nabla_{\sigma\to\tau}(M_1)N \arrow[d] \arrow[dr] & & Q_2 = M_2N_2 \arrow[dl] \\
\nabla_{\sigma\to\tau}(M_1)N_1 \arrow[d] & P \arrow[dd] & \\
Q_1 \arrow[dr] & & \\
 & Q_3 &
\end{tikzcd}
$$

(7) Symmetric to case (6).

By now, a pattern of proof should have emerged. There are four possibilities. Let M be some compound simple term.

(1) $M \xrightarrow{*}_\beta Q_1$ and $M \xrightarrow{*}_\beta Q_2$ contain no top level reductions. In this case, the reductions from the maximal subterms forming M are independent, and we easily obtain confluence using the induction hypothesis.

(2) $M \xrightarrow{*}_\beta Q_1$ and $M \xrightarrow{*}_\beta Q_2$ both contain a top level reduction. In this case, we must have

$$M \xrightarrow{+}_\beta R_1 \xrightarrow{*}_\beta R_1' \longrightarrow_\beta S_1 \xrightarrow{*}_\beta Q_1,$$

and

$$M \xrightarrow{+}_\beta R_2 \xrightarrow{*}_\beta R_2' \longrightarrow_\beta S_2 \xrightarrow{*}_\beta Q_2,$$

where R_1 and R_2 are the first occurrences of top level redexes, R_1' and R_2' the top level redexes that are actually reduced, and S_1 and S_2 the results of these top level reductions.

In this case, the reductions $M \xrightarrow{+}_\beta R_1$ and $M \xrightarrow{+}_\beta R_2$ are as in case 1, and by the induction hypothesis, we can find a P such that

$$R_1 \xrightarrow{*}_\beta P \quad \text{and} \quad R_2 \xrightarrow{*}_\beta P.$$

But then, because R_1 is a top level redex, by the assumption, confluence holds from R_1, and we get some Q_3 such that

$$Q_1 \xrightarrow{*}_\beta Q_3 \quad \text{and} \quad P \xrightarrow{*}_\beta Q_3.$$

Then, $R_2 \xrightarrow{*}_\beta Q_2$ and $R_2 \xrightarrow{*}_\beta P \xrightarrow{*}_\beta Q_3$. Again, because R_2 is a top level redex, by the assumption, confluence holds from R_2, and we get some Q_4 such that

$$Q_2 \xrightarrow{*}_\beta Q_4 \quad \text{and} \quad Q_3 \xrightarrow{*}_\beta Q_4.$$

We have confluence in Q_4.

The above reductions are indicated in the following diagram.

$$
\begin{tikzcd}
 & MN \arrow[dl] \arrow[dr] & & \\
R_1 \arrow[dd] \arrow[dr] & & R_2 \arrow[dl] \arrow[dr] & \\
 & P \arrow[ddd] & & R_2' \arrow[ddd] \\
R_1' \arrow[d] & & & \\
Q_1 \arrow[dr] & & & \\
 & Q_3 \arrow[dr] & & Q_2 \arrow[dl] \\
 & & Q_4 &
\end{tikzcd}
$$

(3) $M \xrightarrow{*}_\beta Q_1$ and $M \xrightarrow{*}_\beta Q_2$, where the first reduction has a top level reduction but the second one does not. In this case, we must have

$$M \xrightarrow{+}_\beta R_1 \xrightarrow{*}_\beta R_1' \longrightarrow_\beta S_1 \xrightarrow{*}_\beta Q_1,$$

and

$$M \xrightarrow{*}_\beta Q_2,$$

where R_1 is the first occurrence of a top level redex, R_1' is the top level redex that is actually reduced, and S_1 the result of this top level reduction.

In this case, the reductions $M \xrightarrow{+}_\beta R_1$ and $M \xrightarrow{*}_\beta Q_2$ are as in case 1, and by the induction hypothesis, we can find a P such that

$$R_1 \xrightarrow{*}_\beta P \quad \text{and} \quad Q_2 \xrightarrow{*}_\beta P.$$

But then, because R_1 is a top level redex, by the assumption, confluence holds from R_1, and we get some Q_3 such that

$$Q_1 \xrightarrow{*}_\beta Q_3 \quad \text{and} \quad P \xrightarrow{*}_\beta Q_3.$$

We have confluence in Q_3.

The above reductions are indicated in the following diagram.

$$
\begin{tikzcd}
 & MN \arrow[dl] \arrow[dr] & \\
R_1 \arrow[d] \arrow[dr] & & Q_2 \arrow[dl] \\
R_1' \arrow[d] & P \arrow[dd] & \\
Q_1 \arrow[dr] & & \\
 & Q_3 &
\end{tikzcd}
$$

(4) $M \xrightarrow{*}_\beta Q_1$ and $M \xrightarrow{*}_\beta Q_2$, where the first reduction does not have a top level reduction but the second one does. This case is the symmetric of (3).

The reader will easily verify that the above pattern applies to (P3)(2) and (P3)(3).

(P4) These cases are all similar, and hold because a reduction cannot apply at the top level. For example, asuming that confluence holds from M, note that we have $\lambda x\colon\sigma.\, M \xrightarrow{*}_\beta \lambda x\colon\sigma.\, M'$ iff $M \xrightarrow{*}_\beta M'$, and thus confluence holds from $\lambda x\colon\sigma.\, M$.

(P5) There is a similar pattern for (P5)(1), (P5)(2), (P5)(4), and (P5)(5). There are four possibilities.

(1) $M \xrightarrow{*}_\beta Q_1$ and $M \xrightarrow{*}_\beta Q_2$ contain no top level reduction. In this case, Q_1 and Q_2 are top level redexes, and we can extend the above reductions by actually reducing Q_1 and Q_2: $M \xrightarrow{*}_\beta Q_1 \longrightarrow_\beta S_1$ and $M \xrightarrow{*}_\beta Q_2 \longrightarrow_\beta S_2$.

(2) $M \xrightarrow{*}_\beta Q_1$ and $M \xrightarrow{*}_\beta Q_2$ both contain a top level reduction. In this case, we must have

$$M \xrightarrow{*}_\beta R_1 \longrightarrow_\beta S_1 \xrightarrow{*}_\beta Q_1,$$

and

$$M \xrightarrow{*}_\beta R_2 \longrightarrow_\beta S_2 \xrightarrow{*}_\beta Q_2,$$

where R_1 and R_2 are the first occurrences of top level reductions and S_1 and S_2 the results of these top level reductions.

(3) $M \xrightarrow{*}_\beta Q_1$ and $M \xrightarrow{*}_\beta Q_2$ where the first reduction has a top level reduction but the second one does not. In this case, we must have

$$M \xrightarrow{*}_\beta R_1 \longrightarrow_\beta S_1 \xrightarrow{*}_\beta Q_1,$$

and

$$M \xrightarrow{*}_\beta Q_2,$$

where R_1 is the first occurrence of a top level reduction, and S_1 the result of this top level reduction. We can extend the second reduction by actually reducing the top level redex Q_2: $M \xrightarrow{*}_\beta Q_2 \longrightarrow_\beta S_2$.

(4) $M \xrightarrow{*}_\beta Q_1$ and $M \xrightarrow{*}_\beta Q_2$, where the first reduction does not have a top level reduction but the second one does. This case is the symmetric of (3).

Thus, in all cases, we can assume that we have reductions as in case (2). Then, because M itself is a top level redex, we have the reduction $M \longrightarrow_\beta M'$, and the crucial fact is that because of the structure of the redexes M, R_1 and R_2, we have reductions

$$M' \xrightarrow{*}_\beta S_1 \xrightarrow{*}_\beta Q_1 \quad \text{and} \quad M' \xrightarrow{*}_\beta S_2 \xrightarrow{*}_\beta Q_2.$$

However, by assumption, confluence holds from M', and we get a Q_3 such that

$$Q_1 \xrightarrow{*}_\beta Q_3 \quad \text{and} \quad Q_2 \xrightarrow{*}_\beta Q_3.$$

The above reductions are indicated in the following diagram.

$$\begin{tikzcd}
& M \arrow[dl] \arrow[d] \arrow[dr] & \\
R_1 \arrow[d] & M' \arrow[dl] \arrow[dr] & R_2 \arrow[d] \\
S_1 \arrow[d] & & S_2 \arrow[d] \\
Q_1 \arrow[dr] & & Q_2 \arrow[dl] \\
& Q_3 &
\end{tikzcd}$$

We illustrate the above scheme in the case of $M = (\lambda x\colon \sigma.\, M_1)N_1$, leaving the remaining cases to the reader. Then, $M' = M_1[N_1/x]$, $S_1 = M_2[N_2/x]$, and $S_2 = M_3[N_3/x]$, where $M_1 \xrightarrow{*}_\beta M_2$, $M_1 \xrightarrow{*}_\beta M_3$, $N_1 \xrightarrow{*}_\beta N_2$, $N_1 \xrightarrow{*}_\beta N_3$.

(P5)(3) and (P5)(6). These two cases are very similar, and we only treat (P5)(3). There are four main cases.

(1) The reductions

$$\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x\colon \sigma) \Rightarrow M \mid \texttt{inr}(y\colon \tau) \Rightarrow N \xrightarrow{*}_\beta Q_1$$

and

$$\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x\colon \sigma) \Rightarrow M \mid \texttt{inr}(y\colon \tau) \Rightarrow N \xrightarrow{*}_\beta Q_2$$

contain no top level reductions.

Then, $Q_1 = \texttt{case}\ P_1\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M_1 \mid \texttt{inr}(y{:}\tau) \Rightarrow N_1$ and $Q_2 = \texttt{case}\ P_2\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M_2 \mid \texttt{inr}(y{:}\tau) \Rightarrow N_2$, where $P \xrightarrow{*}_\beta P_1$, $P \xrightarrow{*}_\beta P_2$, $M \xrightarrow{*}_\beta M_1$, $M \xrightarrow{*}_\beta M_2$, $N \xrightarrow{*}_\beta N_1$, and $N \xrightarrow{*}_\beta N_2$. Since confluence holds from P, M, and N, there are some P_3, M_3, and N_3 that achieve confluence, and thus we have confluence in $Q_3 = \texttt{case}\ P_3\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M_3 \mid \texttt{inr}(y{:}\tau) \Rightarrow N_3$.

(2) The reductions

$$\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\tau) \Rightarrow N \xrightarrow{*}_\beta Q_1$$

and

$$\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\tau) \Rightarrow N \xrightarrow{*}_\beta Q_2$$

both contain top level reductions.

In this case, P reduces to a term of the form $\texttt{inl}(P')$, or $\texttt{inr}(P')$, or $\nabla_{\sigma+\tau}(P')$. We treat the first case, the others being similar. We must have

$$\begin{aligned}
&\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\tau) \Rightarrow N\\
&\qquad\qquad \xrightarrow{*}_\beta \texttt{case}\ \texttt{inl}(P_1)\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\tau) \Rightarrow N\\
&\qquad\qquad \xrightarrow{*}_\beta \texttt{case}\ \texttt{inl}(P_1)\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M_1 \mid \texttt{inr}(y{:}\tau) \Rightarrow N_1\\
&\qquad\qquad \longrightarrow_\beta M_1[P_1/x] \xrightarrow{*}_\beta Q_1,
\end{aligned}$$

and

$$\begin{aligned}
&\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\tau) \Rightarrow N\\
&\qquad\qquad \xrightarrow{*}_\beta \texttt{case}\ \texttt{inl}(P_2)\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\tau) \Rightarrow N\\
&\qquad\qquad \xrightarrow{*}_\beta \texttt{case}\ \texttt{inl}(P_2)\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M_2 \mid \texttt{inr}(y{:}\tau) \Rightarrow N_2\\
&\qquad\qquad \longrightarrow_\beta M_2[P_2/x] \xrightarrow{*}_\beta Q_2.
\end{aligned}$$

Since confluence holds from P, there is some P_3 such that $P_1 \xrightarrow{*}_\beta P_3$ and $P_2 \xrightarrow{*}_\beta P_3$. Then, we have

$$M[P_1/x] \xrightarrow{*}_\beta M[P_3/x] \quad \text{and} \quad M[P_2/x] \xrightarrow{*}_\beta M[P_3/x],$$

and also

$$M[P_1/x] \xrightarrow{*}_\beta M_1[P_1/x] \xrightarrow{*}_\beta Q_1 \quad \text{and} \quad M[P_2/x] \xrightarrow{*}_\beta M_2[P_2/x] \xrightarrow{*}_\beta Q_2.$$

Since by the assumption, confluence holds from $M[P_1/x]$, there is some Q_3 such that

$$Q_1 \xrightarrow{*}_\beta Q_3 \quad \text{and} \quad M[P_3/x] \xrightarrow{*}_\beta Q_3.$$

Then, we have $M[P_2/x] \xrightarrow{*}_\beta M[P_3/x] \xrightarrow{*}_\beta Q_3$, and since by the assumption, confluence holds from $M[P_2/x]$, there is some Q_4 such that $Q_2 \xrightarrow{*}_\beta Q_4$ and $Q_3 \xrightarrow{*}_\beta Q_4$.

(3) The reduction

$$\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\tau) \Rightarrow N \xrightarrow{*}_\beta Q_1$$

contains a top level reduction, but

$$\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M \mid \texttt{inr}(y\colon\tau) \Rightarrow N \xrightarrow{*}_\beta Q_2$$

does not.

In this case, P reduces to a term of the form $\texttt{inl}(P')$, or $\texttt{inr}(P')$, or $\nabla_{\sigma+\tau}(P')$. We treat the first case, the others being similar. In this case, we have

$$\begin{aligned}
&\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M \mid \texttt{inr}(y\colon\tau) \Rightarrow N \\
&\qquad\qquad \xrightarrow{*}_\beta \texttt{case}\ \texttt{inl}(P_1)\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M \mid \texttt{inr}(y\colon\tau) \Rightarrow N \\
&\qquad\qquad \xrightarrow{*}_\beta \texttt{case}\ \texttt{inl}(P_1)\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M_1 \mid \texttt{inr}(y\colon\tau) \Rightarrow N_1 \\
&\qquad\qquad \longrightarrow_\beta M_1[P_1/x] \xrightarrow{*}_\beta Q_1,
\end{aligned}$$

and

$$\begin{aligned}
&\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M \mid \texttt{inr}(y\colon\tau) \Rightarrow N \\
&\qquad\qquad \xrightarrow{*}_\beta \texttt{case}\ P_2\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M \mid \texttt{inr}(y\colon\tau) \Rightarrow N \\
&\qquad\qquad \xrightarrow{*}_\beta Q_2 = \texttt{case}\ P_2\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M_2 \mid \texttt{inr}(y\colon\tau) \Rightarrow N_2.
\end{aligned}$$

The rest of the proof is similar to the previous case, but is simpler. Since confluence holds from P, there is some P_3 such that $P_1 \xrightarrow{*}_\beta P_3$ and $P_2 \xrightarrow{*}_\beta \texttt{inl}(P_3)$. Then the reduction

$$\begin{aligned}
&\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M \mid \texttt{inr}(y\colon\tau) \Rightarrow N \\
&\qquad\qquad \xrightarrow{*}_\beta Q_2 = \texttt{case}\ P_2\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M_2 \mid \texttt{inr}(y\colon\tau) \Rightarrow N_2
\end{aligned}$$

can be extended to

$$\begin{aligned}
&\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M \mid \texttt{inr}(y\colon\tau) \Rightarrow N \\
&\qquad\qquad \xrightarrow{*}_\beta Q_2 = \texttt{case}\ P_2\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M_2 \mid \texttt{inr}(y\colon\tau) \Rightarrow N_2 \\
&\qquad\qquad \xrightarrow{*}_\beta \texttt{case}\ \texttt{inl}(P_3)\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow M_2 \mid \texttt{inr}(y\colon\tau) \Rightarrow N_2 \\
&\qquad\qquad \xrightarrow{*}_\beta M_2[P_3/x].
\end{aligned}$$

As in the previous case, we use the fact that confluence holds from $M[P_1/x]$.

(4) This is the symmetric of case 3.

This concludes all the cases, and the proof. $\square$

9 Adding η-like Reduction Rules

We now show that the method extends without difficulties to η-like reduction rules.

Definition 9.1 The set of *η-like reduction rules* is defined as follows.

$$\begin{aligned}
\lambda x\colon\sigma.\,(Mx) &\longrightarrow M, && \text{if } x \notin FV(M),\\
\langle \pi_1(M), \pi_2(M)\rangle &\longrightarrow M, &&\\
\texttt{case}\ M\ \texttt{of}\ \texttt{inl}(x\colon\sigma) \Rightarrow \texttt{inl}(x) \mid \texttt{inr}(y\colon\tau) \Rightarrow \texttt{inr}(y) &\longrightarrow M, &&\\
\lambda t\colon\iota.\,(Mt) &\longrightarrow M, && \text{if } t \notin FV(M),\\
\texttt{casex}\ M\ \texttt{of}\ \texttt{inx}(u\colon\iota, x\colon\sigma[u/t]) \Rightarrow \texttt{inx}(u,x) &\longrightarrow M, && \text{if } u \notin FV(M).
\end{aligned}$$

We will denote the reduction relation defined by the union of the rules of definition 8.2 and of definition 9.1 as $\longrightarrow_{\beta\eta}$ (even though there are reductions other that β-reduction and η-reduction). The definition of an I-term remains identical to that given in definition 8.3, and similarly for stubborn terms. Properties (P1)-(P3) also remain the same, but they are stated with respect to the new reduction relation $\xrightarrow{+}_{\beta\eta}$.

Definition 9.2 Properties (P1)-(P3) are defined as follows:

(P1) $x \in P_\sigma$, $c \in P_\sigma$, for every variable x and constant c of type σ.

(P2) If $M \in P_\sigma$ and $M \longrightarrow_{\beta\eta} N$, then $N \in P_\sigma$.

(P3) If M is simple, then:

(1) If $M \in P_{\sigma\to\tau}$, $N \in P_\sigma$, $(\lambda x\colon \sigma.\, M')N \in P_\tau$ whenever $M \xrightarrow{+}_{\beta\eta} \lambda x\colon \sigma.\, M'$, and $\nabla_{\sigma\to\tau}(M')N \in P_\tau$ whenever $M \xrightarrow{+}_{\beta\eta} \nabla_{\sigma\to\tau}(M')$, then $MN \in P_\tau$.

(2) If $M \in P_{\sigma\times\tau}$, $\pi_1(\langle M', N'\rangle) \in P_\sigma$ and $\pi_2(\langle M', N'\rangle) \in P_\tau$ whenever $M \xrightarrow{+}_{\beta\eta} \langle M', N'\rangle$, and $\pi_1(\nabla_{\sigma\times\tau}(M')) \in P_\sigma$ and $\pi_2(\nabla_{\sigma\times\tau}(M')) \in P_\tau$ whenever $M \xrightarrow{+}_{\beta\eta} \nabla_{\sigma\times\tau}(M')$, then $\pi_1(M) \in P_\sigma$ and $\pi_2(M) \in P_\tau$.

(3) If $M \in P_{\forall t.\, \sigma}$, $\tau \in \mathcal{T}$, $(\lambda t\colon \iota.\, M')\tau \in P_{\sigma[\tau/t]}$ whenever $M \xrightarrow{+}_{\beta\eta} \lambda t\colon \iota.\, M'$, and $\nabla_{\forall t.\, \sigma}(M')\tau \in P_{\sigma[\tau/t]}$ whenever $M \xrightarrow{+}_{\beta\eta} \nabla_{\forall t.\, \sigma}(M')$, then $M\tau \in P_{\sigma[\tau/t]}$.

Definition 8.5 remains the same, except that it uses the new reduction relation $\longrightarrow_{\beta\eta}$.

Definition 9.3 A nonempty set C of terms of type σ is a *$\mathcal{P}$-candidate* iff it satisfies the following conditions:

(R1) $C \subseteq P_\sigma$.

(R2) If $M \in C$ and $M \longrightarrow_{\beta\eta} N$, then $N \in C$.

(R3) If M is simple, $M \in P_\sigma$, and $M' \in C$ whenever $M \xrightarrow{+}_{\beta\eta} M'$ and M' is an I-term, then $M \in C$.

Definition 8.6 is now stated in terms of the reduction relation $\longrightarrow_{\beta\eta}$.

Definition 9.4 The sets $[\![\sigma]\!]$ are defined as follows:

$$
\begin{aligned}
[\![\sigma]\!] &= P_\sigma, \qquad \sigma \text{ a base type},\\
[\![\sigma \to \tau]\!] &= \{M \mid M \in P_{\sigma\to\tau}, \text{ and for all } N, \text{ if } N \in [\![\sigma]\!] \text{ then } MN \in [\![\tau]\!]\},\\
[\![\sigma \times \tau]\!] &= \{M \mid M \in P_{\sigma\times\tau},\ \pi_1(M) \in [\![\sigma]\!], \text{ and } \pi_2(M) \in [\![\tau]\!]\},\\
[\![\sigma + \tau]\!] &= \{M \mid M \in P_{\sigma+\tau},\ M' \in [\![\sigma]\!] \text{ whenever } M \xrightarrow{*}_{\beta\eta} \mathtt{inl}(M')\} \,\cup\\
&\ \{M \mid M \in P_{\sigma+\tau},\ M'' \in [\![\tau]\!] \text{ whenever } M \xrightarrow{*}_{\beta\eta} \mathtt{inr}(M'')\} \,\cup\\
&\ \{M \mid M \in P_{\sigma+\tau},\ M_1 \in P_\perp \text{ whenever } M \xrightarrow{*}_{\beta\eta} \nabla_{\sigma+\tau}(M_1)\},\\
[\![\forall t.\, \sigma]\!] &= \{M \mid M \in P_{\forall t.\, \sigma}, \text{ and } \forall \tau \in \mathcal{T},\ M\tau \in [\![\sigma[\tau/t]]\!]\},\\
[\![\exists t.\, \sigma]\!] &= \{M \mid M \in P_{\exists t.\, \sigma}, \text{ and } \exists \tau \in \mathcal{T},\ M' \in [\![\sigma[\tau/t]]\!] \text{ whenever } M \xrightarrow{*}_{\beta\eta} \mathtt{inx}(\tau, M')\} \,\cup\\
&\ \{M \mid M \in P_{\exists t.\, \sigma},\ M_1 \in P_\perp \text{ whenever } M \xrightarrow{*}_{\beta\eta} \nabla_{\exists t.\, \sigma}(M_1)\}.
\end{aligned}
$$

Lemma 8.7 still holds.

Lemma 9.5 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P3), then each $[\![\sigma]\!]$ is a $\mathcal{P}$-candidate that contains all stubborn terms in P_σ.*

Proof. Careful inspection reveals that the proof of lemma 8.7 remains unchanged. This is because, for a simple term M:

(1) If $M \in P_{\sigma\to\tau}$ and there is a reduction $MN \xrightarrow{+}_{\beta\eta} Q$ where Q is an I-term, we must have either

$$M \xrightarrow{+}_{\beta\eta} \lambda x\colon\sigma.\, M_1,$$

or

$$M \xrightarrow{+}_{\beta\eta} \nabla_{\sigma\to\tau}(M_1),$$

even w.r.t. the reduction relation $\xrightarrow{+}_{\beta\eta}$.

(2) If $M \in P_{\sigma\times\tau}$ and there is a reduction $\pi_1(M) \xrightarrow{+}_{\beta\eta} Q$ where Q is an I-term, we must have either

$$M \xrightarrow{+}_{\beta\eta} \langle M_1, N_1\rangle,$$

or

$$M \xrightarrow{+}_{\beta\eta} \nabla_{\sigma\times\tau}(Q_1).$$

The case of the type $\sigma+\tau$ is also unchanged. □

Properties (P4), (P5) are unchanged, but they are stated for the reduction relation $\xrightarrow{+}_{\beta\eta}$.

Definition 9.6 Properties (P4) and (P5) are defined as follows:

(P4)
1. If $M \in P_\tau$, then $\lambda x\colon\sigma.\, M \in P_{\sigma\to\tau}$.
2. If $M \in P_\sigma$ and $N \in P_\tau$, then $\langle M, N\rangle \in P_{\sigma\times\tau}$.
3. If $M \in P_\sigma$, then $\mathtt{inl}(M) \in P_{\sigma+\tau}$, and if $M \in P_\tau$, then $\mathtt{inr}(M) \in P_{\sigma+\tau}$.
4. If $M \in P_\perp$, then $\nabla_\sigma(M) \in P_\sigma$.
5. If $M \in P_\sigma$, then $\lambda t\colon\iota.\, M \in P_{\forall t.\,\sigma}$.
6. If $M \in P_{\sigma[\tau/t]}$, then $\mathtt{inx}(\tau, M) \in P_{\exists t.\,\sigma}$.

(P5)
1. If $N \in P_\sigma$ and $M[N/x] \in P_\tau$, then $(\lambda x\colon\sigma.\, M)N \in P_\tau$.
2. If $M \in P_\sigma$ and $N \in P_\tau$, then $\pi_1(\langle M, N\rangle) \in P_\sigma$ and $\pi_2(\langle M, N\rangle) \in P_\tau$.
3. If $P \in P_{\sigma+\tau}$, $M \in P_\delta$, $N \in P_\delta$, $M[P_1/x] \in P_\delta$ whenever $P \xrightarrow{*}_{\beta\eta} \mathtt{inl}(P_1)$, $N[P_2/x] \in P_\delta$ whenever $P \xrightarrow{*}_{\beta\eta} \mathtt{inr}(P_2)$, and $P_1 \in P_\perp$ whenever $P \xrightarrow{*}_{\beta\eta} \nabla_{\sigma+\tau}(P_1)$, then $\mathtt{case}\ P\ \mathtt{of}\ \mathtt{inl}(x\colon\sigma) \Rightarrow M \mid \mathtt{inr}(y\colon\tau) \Rightarrow N \in P_\delta$.
4. If $M_1 \in P_\perp$ and $N \in P_\sigma$, then $\nabla_{\sigma\to\tau}(M_1)N \in P_\tau$. If $M_1 \in P_\perp$, then $\pi_1(\nabla_{\sigma\times\tau}(M_1)) \in P_\sigma$ and $\pi_2(\nabla_{\sigma\times\tau}(M_1)) \in P_\tau$. If $M_1 \in P_\perp$ and $\tau \in \mathcal{T}$, then $\nabla_{\forall t.\,\sigma}(M_1)\tau \in P_{\sigma[\tau/t]}$.
5. If $\tau \in \mathcal{T}$ and $M[\tau/t] \in P_{\sigma[\tau/t]}$, then $(\lambda t\colon\iota.\, M)\tau \in P_{\sigma[\tau/t]}$.
6. If $P \in P_{\exists t.\,\sigma}$, $N \in P_\delta$, $N[P_1/x, \tau/t] \in P_\delta$ whenever $P \xrightarrow{*}_{\beta\eta} \mathtt{inx}(\tau, P_1)$, and $P_1 \in P_\perp$ whenever $P \xrightarrow{*}_{\beta\eta} \nabla_{\exists t.\,\sigma}(P_1)$, then $\mathtt{casex}\ P\ \mathtt{of}\ \mathtt{inx}(t\colon\iota, x\colon\sigma) \Rightarrow N \in P_\delta$.

Lemma 9.7 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P5) then the following properties hold: (1) If for every N, ($N \in [\![\sigma]\!]$ implies $M[N/x] \in [\![\tau]\!]$), then $\lambda x{:}\,\sigma.\, M \in [\![\sigma \to \tau]\!]$; (2) If $M \in [\![\sigma]\!]$ and $N \in [\![\tau]\!]$, then $\langle M, N\rangle \in [\![\sigma \times \tau]\!]$; (3) If $P \in [\![\sigma + \tau]\!]$, for every P_1, ($P_1 \in [\![\sigma]\!]$ implies $M[P_1/x] \in [\![\delta]\!]$), and for every P_2, ($P_2 \in [\![\tau]\!]$ implies $N[P_2/y] \in [\![\delta]\!]$), then $\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N \in [\![\delta]\!]$; (4) If $M \in P_\perp$, then $\nabla_\sigma(M) \in [\![\sigma]\!]$ for every type σ. (5) If for every τ, ($\tau \in \mathcal{T}$ implies $M[\tau/t] \in [\![\sigma[\tau/t]]\!]$), then $\lambda t{:}\,\iota.\, M \in [\![\forall t.\, \sigma]\!]$; (6) If $P \in [\![\exists t.\, \sigma]\!]$, and for every P_1, for every $\tau \in \mathcal{T}$, ($P_1 \in [\![\sigma[\tau/t]]\!]$ implies $N[P_1/x, \tau/t] \in [\![\delta]\!]$), then $\texttt{casex}\ P\ \texttt{of}\ \texttt{inx}(t{:}\,\iota, x{:}\,\sigma) \Rightarrow N \in [\![\delta]\!]$.*

Proof. This time, a few changes to the proof of lemma 8.9 have to be made to take the reduction rules of definition 9.1 into account.

(1) We need to reexamine the case where

$$(\lambda x{:}\,\sigma.\, M)N \xrightarrow{+}_{\beta\eta} Q$$

and Q is an I-term. The reduction is necessarily of the form either

$$(\lambda x{:}\,\sigma.\, M)N \xrightarrow{*}_{\beta\eta} (\lambda x{:}\,\sigma.\, M')N' \longrightarrow_{\beta\eta} M'[N'/x] \xrightarrow{*}_{\beta\eta} Q,$$

where $M \xrightarrow{*}_{\beta\eta} M'$ and $N \xrightarrow{*}_{\beta\eta} N'$, or

$$(\lambda x{:}\,\sigma.\, M)N \xrightarrow{*}_{\beta\eta} (\lambda x{:}\,\sigma.\, (M'x))N' \longrightarrow_{\beta\eta} M'N' \xrightarrow{*}_{\beta\eta} Q,$$

where $M \xrightarrow{*}_{\beta\eta} M'x$, with $x \notin FV(M')$, and $N \xrightarrow{*}_{\beta\eta} N'$.

The first case is as in lemma 8.9. In the second case, since $x \notin FV(M')$, note that $M'N' = (M'x)[N'/x]$. Since $M \xrightarrow{*}_{\beta\eta} M'x$ and $N \xrightarrow{*}_{\beta\eta} N'$, we have

$$M[N/x] \xrightarrow{*}_{\beta\eta} (M'x)[N'/x] = M'N' \xrightarrow{*}_{\beta\eta} Q,$$

and by (R2), we have $Q \in [\![\tau]\!]$.

(2) We need to reexamine the case where

$$\pi_1(\langle M, N\rangle) \xrightarrow{+}_{\beta\eta} Q$$

and Q is an I-term. The reduction is necessarily of the form either

$$\pi_1(\langle M, N\rangle) \xrightarrow{*}_{\beta\eta} \pi_1(\langle M_1, N_1\rangle) \longrightarrow_{\beta\eta} M_1 \xrightarrow{*}_{\beta\eta} Q,$$

where $M \xrightarrow{*}_{\beta\eta} M_1$ and $N \xrightarrow{*}_{\beta\eta} N_1$, or

$$\pi_1(\langle M, N\rangle) \xrightarrow{*}_{\beta\eta} \pi_1(\langle \pi_1(P), \pi_2(P)\rangle) \longrightarrow_{\beta\eta} \pi_1(P) \xrightarrow{*}_{\beta\eta} Q,$$

where $M \xrightarrow{*}_{\beta\eta} \pi_1(P)$ and $N \xrightarrow{*}_{\beta\eta} \pi_2(P)$.

The first case is as in lemma 8.9. In the second case, we get $M \xrightarrow{*}_{\beta\eta} Q$, and since $M \in [\![\sigma]\!]$, we have $Q \in [\![\sigma]\!]$.

(3) We need to reexamine the case where

$$\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N \xrightarrow{+}_{\beta\eta} Q$$

and Q is an I-term. The reduction is necessarily of the form either

$$\begin{aligned}\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N &\xrightarrow{*}_{\beta\eta} \texttt{case}\ \texttt{inl}(P_1)\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M_1 \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N_1\\ &\longrightarrow_{\beta\eta} M_1[P_1/x] \xrightarrow{*}_{\beta\eta} Q,\end{aligned}$$

where $P \xrightarrow{*}_{\beta\eta} \texttt{inl}(P_1)$, $M \xrightarrow{*}_{\beta\eta} M_1$, and $N \xrightarrow{*}_{\beta\eta} N_1$, or

$$\begin{aligned}\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N &\xrightarrow{*}_{\beta\eta} \texttt{case}\ \texttt{inr}(P_2)\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M_1 \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N_1\\ &\longrightarrow_{\beta\eta} N_1[P_2/y] \xrightarrow{*}_{\beta\eta} Q,\end{aligned}$$

where $P \xrightarrow{*}_{\beta\eta} \texttt{inr}(P_2)$, $M \xrightarrow{*}_{\beta\eta} M_1$, and $N \xrightarrow{*}_{\beta\eta} N_1$, or

$$\begin{aligned}&\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N\\ &\qquad\xrightarrow{*}_{\beta\eta} \texttt{case}\ \nabla_{\sigma+\tau}(P_1)\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M_1 \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N_1 \longrightarrow_{\beta\eta} \nabla_\delta(P_1) \xrightarrow{*}_{\beta\eta} Q,\end{aligned}$$

where $P \xrightarrow{*}_{\beta\eta} \nabla_{\sigma+\tau}(P_1)$, $M \xrightarrow{*}_{\beta\eta} M_1$, and $N \xrightarrow{*}_{\beta\eta} N_1$, or

$$\begin{aligned}&\texttt{case}\ P\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow M \mid \texttt{inr}(y{:}\,\tau) \Rightarrow N\\ &\qquad\xrightarrow{*}_{\beta\eta} \texttt{case}\ P_1\ \texttt{of}\ \texttt{inl}(x{:}\,\sigma) \Rightarrow \texttt{inl}(x) \mid \texttt{inr}(y{:}\,\tau) \Rightarrow \texttt{inr}(y) \longrightarrow_{\beta\eta} P_1 \xrightarrow{*}_{\beta\eta} Q,\end{aligned}$$

where $P \xrightarrow{*}_{\beta\eta} P_1$, $M \xrightarrow{*}_{\beta\eta} \texttt{inl}(x)$, and $N \xrightarrow{*}_{\beta\eta} \texttt{inr}(y)$ (and $\delta = \sigma + \tau$).

The first three cases are as in lemma 8.9. In the last case, we have $P \xrightarrow{*}_{\beta\eta} Q$, and since $P \in [\![\sigma + \tau]\!]$, by (R2), $Q \in [\![\sigma + \tau]\!]$.

(4) The proof is exactly as in lemma 8.9.

(5) This case is very similar to case (1).

(6) This case is very similar to case (3). □

Since lemma 9.5 and lemma 9.7 hold, so does the extension of lemma 8.10 to the reduction relation $\longrightarrow_{\beta\eta}$.

Lemma 9.8 *If $\mathcal{P}$ is a family satisfying conditions (P1)-(P5), then for every term M of type σ, for every substitution φ such that $\varphi(y) \in [\![\gamma]\!]$ for every term variable $y{:}\,\gamma \in FV(M)$, we have $M[\varphi] \in [\![\sigma[\varphi]]\!]$.*

Finally, since lemma 9.7 and lemma 9.8 hold, our main theorem holds for the reduction relation including η-like rules.

Theorem 9.9 *If $\mathcal{P}$ is a family of λ-terms satisfying conditions (P1)-(P5), then $P_\sigma = \Lambda_\sigma$ for every type σ (in other words, every term satisfies the unary predicate defined by $\mathcal{P}$).*

As a consequence of theorem 9.9, we can extend theorem 8.12 and theorem 8.13 to the reduction relation $\xrightarrow{*}_{\beta\eta}$ in the system $\lambda^{\rightarrow,\times,+,\forall,\exists,\perp}$. For strong normalization, this is a fairly trivial extension, but for confluence, this requires a little bit of work (but it it still less work that checking local confluence). In both cases, it is the verification of (P4) that requires more work.

Theorem 9.10 *The reduction relation* $\xrightarrow{*}_{\beta\eta}$ *of the system* $\lambda^{\to,\times,+,\forall,\exists,\perp}$ *is strongly normalizing.*

Proof. (P1) and (P2) are still trivial. One can easily verify that the proof for (P3) given in theorem 8.12 remains unchanged. For (P4) and (P5), we need to consider η-like reductions. The reader will verify that the proof for (P5) given in lemma 8.12 can easily be adpated using the technique of theorem 9.7 to handle η-like reductions. It remains to check (P4).

(P4)(1) If M is SN then $d(M)$ is finite. We prove by induction on $d(M)$ that $\lambda x\colon\sigma.\, M$ is SN. Note that $\lambda x\colon\sigma.\, M \longrightarrow_{\beta\eta} P$ if either $P = \lambda x\colon\sigma.\, M_1$ and $M \longrightarrow_{\beta\eta} M_1$, or $M = M'x$ where $x \notin FV(M')$ and $P = M'$. In the first case, $d(M_1) < d(M)$, and by the induction hypothesis, P is SN. In the second case, since $M = M'x$ is SN, so is $M' = P$. Thus, P is SN in all cases, and so is $\lambda x\colon\sigma.\, M$

(P4)(2) If M and N are SN, then $d(M)$ and $d(N)$ are finite. We prove by induction on $d(M) + d(N)$ that $\langle M, N\rangle$ is SN. Note that $\langle M, N\rangle \longrightarrow_{\beta\eta} P$ if either $P = \langle M_1, N\rangle$ and $M \longrightarrow_{\beta\eta} M_1$, or $P = \langle M, N_1\rangle$ and $N \longrightarrow_{\beta\eta} N_1$, or $M = \pi_1(Q)$, $N = \pi_2(Q)$, and $P = Q$. In the first two cases, $d(M_1) + d(N) < d(M) + d(N)$ and $d(M) + d(N_1) < d(M) + d(N)$, and by the induction hypothesis, P is SN. In the third case, since $M = \pi_1(Q)$ is SN, so is $P = Q$. Thus, P is SN in all cases, and so is $\langle M, N\rangle$.

(P4)(3) If M is SN, by an obvious induction on $d(M)$, $\mathtt{inl}(M)$ and $\mathtt{inr}(M)$ are SN.

(P4)(4) If M is SN, by an obvious induction on $d(M)$, $\bigtriangledown_\sigma(M)$ is SN.

(P4)(5) Similar to (P4)(1).

(P4)(6) Similar to (P4)(3). □

Theorem 9.11 *The reduction relation* $\xrightarrow{*}_{\beta\eta}$ *of the system* $\lambda^{\to,\times,+,\forall,\exists,\perp}$ *is confluent.*

Proof. (P1) and (P2) are still trivial. One can easily verify that the proof for (P3) and (P5) given in theorem 8.13 can easily be adpated using the technique of theorem 9.7 to handle η-like reductions. It remains to check that (P4) holds. This requires a little bit of work. For example, assuming that confluence holds from M, we need to show that confluence holds from $\lambda x\colon\sigma. M$. The complication caused by η-like reductions is that we can have reductions

$$\lambda x\colon\sigma.\, M \xrightarrow{*}_{\beta\eta} \lambda x\colon\sigma.\, (M_1 x) \longrightarrow_{\beta\eta} M_1 \xrightarrow{*}_{\beta\eta} Q_1,$$

where $M \xrightarrow{*}_{\beta\eta} M_1 x$ and $x \notin FV(M_1)$. The problem is that it is not immediately obvious that confluence from M implies confluence from M_1. Actually, because $x \notin FV(M_1)$ in such situations, it is possible to prove that confluence holds from $\lambda x\colon\sigma.\, M$. Such a verification is carried out in Appendix 2 (page 196-198) of Gallier [5]. The other cases can also be handled, and are left to the (perseverant) reader (in fact, they are easier!). □

One should realize that the Church-Rosser property in the presence of η-like reductions fails for terms that do not type-check. For example, the term $M = \lambda x\colon\sigma.\, ((\lambda y\colon\tau.\, y)x)$ where $\sigma \neq \tau$ reduces to $\lambda x\colon\sigma.\, x$ under β-reduction and to $\lambda y\colon\tau.\, y$ under η-reduction. Both terms are in normal form, but since $\sigma \neq \tau$, they are not α-equivalent. The reason for the failure of confluence is that the term M does **not** type-check. This shows that one cannot use the fact that the Church-Rosser property holds for untyped terms under $\beta\eta$-reduction to prove the Church-Rosser property for typed λ-terms under $\beta\eta$-reduction. In our approach, terms must type-check, and the above problem does not arise.

The reducibility method presented in this paper immediately extends to the second-order λ-calculus, or to Girard's system F_ω (as presented in [5]). It can also easily be adapted to the systems of conjunctive types due to Coppo and Dezani as presented in Krivine [14] (system $\mathcal{D}\Omega$ and system $\mathcal{D}$ for pure λ-terms). However, we will now grant our reader a well deserved break, and treat such extensions elsewhere.

References

[1] H.P. Barendregt. *The Lambda Calculus*, volume 103 of *Studies in Logic*. North-Holland, second edition, 1984.

[2] H.B. Curry and R. Feys. *Combinatory Logic, Vol. I.* Studies in Logic. North-Holland, third edition, 1974.

[3] Jean Gallier. Constructive Logics. Part I: A Tutorial on Proof Systems and Typed λ-Calculi. *Theoretical Computer Science*, 1993.

[4] Jean H. Gallier. *Logic for Computer Science.* Harper and Row, New York, 1986.

[5] Jean H. Gallier. On Girard's "candidats de reductibilités". In P. Odifreddi, editor, *Logic And Computer Science*, pages 123–203. Academic Press, London, New York, May 1990.

[6] G. Gentzen. Investigations into logical deduction. In M.E. Szabo, editor, *The Collected Papers of Gerhard Gentzen.* North-Holland, 1969.

[7] J.-Y. Girard, Y. Lafont, and P. Taylor. *Proofs and Types*, volume 7 of *Cambridge Tracts in Theoretical Computer Science.* Cambridge University Press, 1989.

[8] Jean-Yves Girard. Une extension de l'interprétation de Gödel à l'analyse, et son application à l'élimination des coupures dans l'analyse et la théorie des types. In J.E. Fenstad, editor, *Proc. 2nd Scand. Log. Symp.*, pages 63–92. North-Holland, 1971.

[9] Jean-Yves Girard. *Interprétation fonctionnelle et élimination des coupures de l'arithmétique d'ordre supérieur.* PhD thesis, Université de Paris VII, June 1972. Thèse de Doctorat d'Etat.

[10] Jean-Yves Girard. Geometry of interaction I: Interpretation of system F. In Ferro Bonotto, Valentini, and Zanardo, editors, *Logic Colloquium '88*, pages 221–260. North-Holland, Elsevier, 1989.

[11] J.R. Hindley and J.P. Seldin. *Introduction to Combinators and λ-Calculus*, volume 1 of *London Mathematical Society Student texts.* Cambridge University Press, 1986.

[12] W. A. Howard. The formulae-as-types notion of construction. In J. P. Seldin and J. R. Hindley, editors, *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, pages 479–490. Academic Press, London, 1980. Reprint of manuscript first published in 1969.

[13] G. Koletsos. Church-rosser theorem for typed functional systems. *J. Symbolic Logic*, 50(3):782–790, 1985.

[14] J.L. Krivine. *Lambda-Calcul, types et modèles*. Etudes et recherches en informatique. Masson, 1990.

[15] P. Martin-Löf. An intuitionistic theory of types. Technical report, University of Stokholm, Stockholm, Sweden, 1972. Privately circulated manuscript.

[16] D. Prawitz. *Natural deduction, a proof-theoretical study.* Almquist & Wiksell, Stockholm, 1965.

[17] D. Prawitz. Ideas and results in proof theory. In J.E. Fenstad, editor, *Proc. 2nd Scand. Log. Symp.*, pages 235–307. North-Holland, 1971.

[18] R. Statman. Logical Relations and the Typed λ-calculus. *Information and Control*, 65(2/3):85–97, 1985.

[19] S. Stenlund. *Combinators, Lambda Terms, and Proof Theory.* D. Reidel, Dordrecht, Holland, 1972.

[20] W.W. Tait. Intensional interpretation of functionals of finite type I. *J. Symbolic Logic*, 32:198–212, 1967.

[21] W.W. Tait. A realizability interpretation of the theory of species. In R. Parikh, editor, *Logic Colloquium*, volume 453 of *Lecture Notes in Math.*, pages 240–251. Springer Verlag, 1975.

[22] A.S. Troelstra and D. van Dalen. *Constructivism in Mathematics: An Introduction, Vol. I and II*, volume 123 of *Studies in Logic.* North-Holland, 1988.

[23] D. van Dalen. *Logic and Structure.* Universitext. Springer Verlag, second edition, 1980.