Hypothetical Logic of Proofs

Eduardo Bonelli & Gabriela Steren

Logica Universalis

ISSN 1661-8297
Volume 8
Number 1

Log. Univers. (2014) 8:103-140
DOI 10.1007/s11787-014-0098-0

Log. Univers. 8 (2014), 103–140
© 2014 Springer Basel
1661-8297/14/010103-38, *published online* March 4, 2014
DOI 10.1007/s11787-014-0098-0

Logica Universalis

Hypothetical Logic of Proofs

Eduardo Bonelli and Gabriela Steren

Abstract. The logic of proofs is a refinement of modal logic introduced by Artemov in 1995 in which the modality $\Box A$ is revisited as $[\![t]\!]A$ where t is an expression that bears witness to the validity of A. It enjoys arithmetical soundness and completeness and is capable of reflecting its own proofs ($\vdash A$ implies $\vdash [\![t]\!]A$, for some t). We develop the Hypothetical Logic of Proofs, a reformulation of LP based on judgemental reasoning.

Mathematics Subject Classification (2010). 68N18, 68Q42, 03B40, 03B45, 03B70.

Keywords. Modal logic, logic of proofs, natural deduction, Curry-Howard isomorphism, lambda calculus, lambda Mu-calculus.

Contents

Birkhäuser

1. Introduction

We propose a presentation of LP based on hypothetical reasoning with the aim of contributing towards a novel reading of this logic in relation to programming languages and type theory. We begin by explaining: (1) what LP is (Sect. 1.1); (2) why it is worthwhile to explore its applications to programming languages and type theory (Sect. 1.2); and (3) what we mean by a hypothetical presentation (Sect. 1.3).

1.1. LP

The logic of proofs LP [5,6] is a logic in which the usual propositional connectives are augmented by a new one: given a proof polynomial s and a proposition A, build $[\![s]\!]A$. The intended reading is: "s is a proof of A". A proof s is represented as combinatory term (proof polynomial), constructed from proof variables and constants using the operations: application "$\cdot$", proof-checker "!" and plus "+". More precisely, formulae and proof polynomials are given by the following grammar:

$$\begin{aligned} A, B &::= P \,|\, \bot \,|\, A \supset B \,|\, [\![s]\!]A \\ s, t &::= x^A \,|\, c \,|\, s \cdot t \,|\, !s \,|\, s + t \end{aligned}$$

A **formula** $(A, B, \ldots)$ is either a propositional variable $(P, Q, \ldots)$, the constant for falsehood $(\bot)$, an implication $(A \supset B)$ or a modality $([\![s]\!]A)$. The axioms are specified by means of the following axiom schemes:

A0. Axioms of classical propositional logic in the language of LP
A1. $[\![s]\!]A \supset A$ (*"verification"*)
A2. $[\![s]\!](A \supset B) \supset ([\![t]\!]A \supset [\![s \cdot t]\!]B)$ (*"application"*)
A3. $[\![s]\!]A \supset [\![!s]\!][\![s]\!]A$ (*"proof checker"*)
A4. $[\![s]\!]A \supset [\![s + t]\!]A$ (*"plus"*)
A5. $[\![t]\!]A \supset [\![s + t]\!]A$

For verification one reads:"if s is a proof of A, then A holds". For application one reads: "if s is a proof of $A \supset B$ and t is a proof of A, then $s \cdot t$ is a proof of B". Thus "$\cdot$" represents composition of proofs. For proof checking one reads: "if s is a proof of A, then $!s$ is a proof of the sentence 's is a proof of A' ". Thus $!s$ is seen as a computation that verifies $[\![s]\!]A$. For plus one reads: "if s is a proof of A, then so is $s + t$, regardless of the form of t". The inference schemes of LP are:

R1. If $\vdash A \supset B$ and $\vdash A$ then $\vdash B$ (modus ponens).
R2. If A is an axiom **A0-A5**, and c is a proof constant, then $\vdash [\![c]\!]A$ (necessitation).

A **constant specification** (CS) is a finite set of formulas $[\![c_1]\!]A_1, \ldots, [\![c_n]\!]A_n$ such that c_i is a constant, and A_i an axiom **A0**–**A5**. Each derivation in LP naturally generates the CS consisting of all formulas introduced in this derivation by the necessitation rule.

Among the notable properties of LP we find that of arithmetical soundness and completeness [5,6]. This result was later extended to a fragment of LP capturing provability in HA [4,10].

1.2. LP and Programming Languages

The fact that proof polynomials and formulae coexist suggest that there may be computational interpretations of LP in which type derivations (certificates, computation trails, etc.) may be combined with programs that manipulate them in a uniform setting. Some steps in exploring this idea have already been taken.

In [2] proof polynomials are seen to encode intentional information stating how a result is obtained. A lambda calculus is synthesized from the Curry–Howard isomorphism applied to a hypothetical presentation of an intuitionistic fragment of LP (this paper, in contrast, studies classical LP and also deals with the plus, thus encompassing full LP). Each reduction step in this lambda calculus generates a trail. Confluence for this enriched lambda calculus then not only states that computation is deterministic in terms of the standard joinability condition, but also that joinability may be reached by means of essentially performing the same amount of work. Indeed, if these trails are seen as Lévy labels, then we obtain a fresh view on the standard strong confluence result of the lambda calculus [14].

A different proposal is developed in [8] where proof polynomials are interpreted as certificates of typability for mobile code. Essentially, the well-known Curry-Howard correspondence between IS4 and mobile computation (see [8] for references) is extended to an intuitionistic fragment of LP obtaining a lambda calculus that operates over certified mobile units, pairs consisting of mobile code accompanied with a certificate. The type system also guarantees well-formedness of certificate construction (see Sect. 8).

Another property of LP worthy of mention is that it is capable of internalising its own proofs: $\vdash A$ implies there exists a proof polynomial s s.t. $\vdash [\![s]\!]A$. Here s essentially reifies the derivation of $\vdash A$ into the object-logic. This suggests that proof polynomials may be interpreted as the computation history. The reason is that when such proof polynomials are internalized in our hypothetical presentation, proof normalisation steps must also be reflected in order to preserve subject reduction. If we additionally empower the programmer to have access to these proof polynomials, then we can model history-based access control, history-based information flow analysis and other security formalisms [7].

Finally, an intuitionistic fragment of LP with disjunction and plus is studied in [20] in terms of the Curry–Howard isomorphism. From that work we draw our analysis of the typing schemes for the plus. That work, however, does not address classical LP.

1.3. Hypothetical Reasoning for LP

Following [18] we distinguish the following judgements: "A is a proposition" ("A proposition" for short), "s is a proof witness", "A is true" and "A is valid". We also add the judgements "A is false" and "A is true with proof witness s". In the case of the last three judgements we assume that it is already known that "A proposition"; likewise, in the last judgement, we assume that it is already known that "s is a proof witness". The inference schemes defining the meaning of "A proposition" are the usual well-formedness conditions and hence are omitted. For example, in the case of "$A \supset B$ proposition" we have the inference scheme:

$$\frac{A\ \mathit{proposition} \quad B\ \mathit{proposition}}{A \supset B\ \mathit{proposition}}$$

Our interest lies in providing meaning to the following hypothetical judgements with proof witnesses:

$$\begin{array}{l} v_1 : A_1\ \mathit{valid}, \ldots, v_n : A_n\ \mathit{valid}; \\ x_1 : B_1\ \mathit{true}, \ldots, x_m : B_m\ \mathit{true}; \vdash A\ \mathit{true\ with\ proof\ witness}\ s \\ \alpha_1 : C_1\ \mathit{false}, \ldots, \alpha_p : C_p\ \mathit{false} \end{array}$$

by a set of axiom and inference schemes, where v_i (for $i \in 1..n$), x_j (for $j \in 1..m$) and α_k (for $k \in 1..p$) range over some given some set of validity, truth and falsehood variables, resp. For the sake of readability, we drop the qualifiers "*valid*", "*true*" , "*false*" and "*true with proof witness*". Consequently, these judgements take the form:

$$v_1 : A_1, \ldots, v_n : A_n; a_1 : B_1, \ldots, a_m : B_m; \alpha_1 : C_1, \ldots, \alpha_p : C_p \vdash A \,|\, s$$

Section 2 gives meaning to these judgements by introducing appropriate axiom and inference schemes. This will provide a natural deduction presentation, whose fundamental properties we study in this paper.

Structure of the paper. Section 2 introduces the Hypothetical Logic of Proofs or HLP. We then establish the precise correspondence between LP and HLP. A term assignment for HLP is presented in Sect. 4. This is followed by a study of the fundamental properties of reduction for that term assignment, namely strong normalisation (Sect. 5) and confluence (Sect. 6). Section 7 considers additional permutative rules. After a brief overview of related work (Sect. 8) we conclude in Sect. 9. In the sequel, unless otherwise stated, LP will refer to the presentation based on classical logic, as given above.

2. HLP

This section introduces the syntax and inference schemes of HLP.

2.1. Formulae and Proof Witnesses

A *formula* in HLP is the same as in LP, except that $r, s, \dots$ range over proof witnesses rather than proof polynomials.

$$r, s, t ::= x^A \mid v^A \mid \lambda x^A.s \mid s \cdot t \mid !s \mid t\langle v^A{:=}r, s\rangle \mid s + t \mid [\alpha^A]s \mid \mu\alpha^A.s$$

A *proof witness* is either a truth hypothesis (x^A); a validity hypothesis (v^A); an abstraction ($\lambda x^A.s$); an application ($s \cdot t$); a "bang" ($!s$); an "unbox" ($t\langle v^A{:=}r, s\rangle$); a "plus" ($s + t$); a name application ($[\alpha^A]s$); or a name abstraction ($\mu\alpha^A.s$). In $\lambda x^A.s$, the scope of the bound variable x^A is s; in $t\langle v^A{:=}r, s\rangle$ the scope of the bound variable v^A is t and in $\mu\alpha^A.s$ the scope of the bound variable α^A is s. Also, $!s$ binds all free occurrences of truth and falsehood variables in s; likewise $t\langle v^A{:=}r, s\rangle$ binds all free occurrences of truth and falsehood variables in r. A *truth context* (Γ) is a set of truth hypotheses $\{x_1^{A_1}, \dots, x_n^{A_n}\}$; a *validity context* ($\Theta$) is a set of validity variables $\{v_1^{A_1}, \dots, v_m^{A_m}\}$; a *falsehood context* (Δ) is a set of falsehood variables $\{\alpha_1^{A_1}, \dots, \alpha_k^{A_k}\}$. We write $\cdot$ for the empty context. A *judgement* is an expression of the form $\Theta; \Gamma; \Delta \vdash A \mid s$.

We assume the following *variable convention*: all bound variable names are different from each other, and different from all free variables. We also assume that application "$\cdot$" and sum "$+$" are left-associative, and implication "$\supset$" is right-associative. We use $\neg A$ as an abbreviation for $A \supset \bot$. The operators $!$, $\neg$ and $[\![\ ]\!]$ have precedence over $\cdot$, $+$ and $\supset$, which in turn have precedence over λ, μ and $[\ ]$. For example, $[\alpha^{([\![r]\!]A)\supset((\neg B)\supset C)}]((!s) + t)$ may be written $[\alpha^{[\![r]\!]A\supset\neg B\supset C}]!s + t$.

The set of *free variables of validity, truth and falsehood* in a formula A are denoted $\mathsf{FVT}(A)$, $\mathsf{FVV}(A)$ and $\mathsf{FVF}(A)$, resp. The definition of $\mathsf{FVT}(A)$ is as follows ($\mathsf{FVV}(A)$ and $\mathsf{FVF}(A)$ are similar and hence omitted), where $\mathsf{FVT}(A, B)$ abbreviates $\mathsf{FVT}(A) \cup \mathsf{FVT}(B)$:

$$\begin{aligned}
\mathsf{FVT}(P) &\triangleq \emptyset\\
\mathsf{FVT}(\bot) &\triangleq \emptyset\\
\mathsf{FVT}(A \supset B) &\triangleq \mathsf{FVT}(A, B)\\
\mathsf{FVT}([\![t]\!]A) &\triangleq \mathsf{FVT}(t, A)
\end{aligned}$$

The set of free variables of validity, truth and falsehood in a proof witness s, denoted $\mathsf{FVT}(s)$, $\mathsf{FVV}(s)$ and $\mathsf{FVF}(s)$, resp., are defined as follows:

$$\begin{aligned}
\mathsf{FVT}(x^A) &\triangleq \{x^A\}\\
\mathsf{FVT}(v^A) &\triangleq \emptyset\\
\mathsf{FVT}(\lambda x^A.s) &\triangleq \mathsf{FVT}(s)\backslash\{x^A\}\\
\mathsf{FVT}(s \cdot t) &\triangleq \mathsf{FVT}(s, t)\\
\mathsf{FVT}(!s) &\triangleq \emptyset\\
\mathsf{FVT}(t\langle v^A{:=}r, s\rangle) &\triangleq \mathsf{FVT}(t, s)\\
\mathsf{FVT}(s + t) &\triangleq \mathsf{FVT}(s, t)\\
\mathsf{FVT}([\alpha^A]s^A) &\triangleq \mathsf{FVT}(s^A)\\
\mathsf{FVT}(\mu\alpha^A.s) &\triangleq \mathsf{FVT}(s^A)
\end{aligned}$$

$$\begin{aligned}
\mathsf{FVV}(x^A) &\triangleq \emptyset\\
\mathsf{FVV}(v^A) &\triangleq \{v^A\}\\
\mathsf{FVV}(\lambda x^A.s) &\triangleq \mathsf{FVV}(s)\\
\mathsf{FVV}(s \cdot t) &\triangleq \mathsf{FVV}(s, t)\\
\mathsf{FVV}(!s) &\triangleq \mathsf{FVV}(s)\\
\mathsf{FVV}(t\langle v^A{:=}r, s\rangle) &\triangleq (\mathsf{FVV}(t)\backslash\{v^A\})\\
&\quad \cup \mathsf{FVV}(r, s)\\
\mathsf{FVV}(s + t) &\triangleq \mathsf{FVV}(s, t)\\
\mathsf{FVV}([\alpha^A]s^A) &\triangleq \mathsf{FVV}(s^A)\\
\mathsf{FVV}(\mu\alpha^A.s) &\triangleq \mathsf{FVV}(s^A)
\end{aligned}$$

$$\begin{aligned}
\mathsf{FVF}(x^A) &\triangleq \emptyset\\
\mathsf{FVF}(v^A) &\triangleq \emptyset\\
\mathsf{FVF}(\lambda x^A.s) &\triangleq \mathsf{FVF}(s)\\
\mathsf{FVF}(s\cdot t) &\triangleq \mathsf{FVF}(s,t)\\
\mathsf{FVF}(!s) &\triangleq \emptyset\\
\mathsf{FVF}(t\langle v^A{:=}r,s\rangle) &\triangleq \mathsf{FVF}(t,s)\\
\mathsf{FVF}(s+t) &\triangleq \mathsf{FVF}(s,t)\\
\mathsf{FVF}([\alpha^A]s^A) &\triangleq \mathsf{FVF}(s^A)\cup\{\alpha^A\}\\
\mathsf{FVF}(\mu\alpha^A.s) &\triangleq \mathsf{FVF}(s^A)\backslash\{\alpha^A\}
\end{aligned}$$

Remark 2.1. In a judgement $\Theta;\Gamma;\Delta\vdash A\,|\,s$ we shall assume the following *freshness condition*: all v_i with $i\in 1..m$, x_i with $i\in 1..n$ and α_i with $i\in 1..k$ are assumed distinct and moreover *fresh* (*i.e.* that they do not occur in the A_i, B_i and C_i). More precisely, for every pair of formulas A, B such that $x^A\in\Gamma$, $v^A\in\Theta$ or $\alpha^A\in\Delta$:

- if $y^B\in\Gamma$, then $y^B\notin\mathsf{FVT}(A)$;
- if $w^B\in\Theta$, then $w^B\notin\mathsf{FVV}(A)$; and
- if $\beta^B\in\Delta$, then $\beta^B\notin\mathsf{FVF}(A)$.

2.2. Axiom and Inference Schemes

The axiom and inference schemes of HLP are depicted in Fig. 1. We write $\rhd_{\mathsf{HLP}}\,\Theta;\Gamma;\Delta\vdash A\,|\,s$ to indicate that the judgement $\Theta;\Gamma;\Delta\vdash A\,|\,s$ is derivable using these schemes. A brief informal explanation of some of these schemes follows. The axiom scheme Var states that the judgement $\Theta;\Gamma,x^A;\Delta\vdash A\,|\,x^A$ is evident in itself. Indeed, if we assume that x^A is a witness that proposition A is true, then we immediately conclude that A is true with proof witness x^A. The introduction scheme for the $[\![t]\!]$ modality internalises metalevel evidence into the object logic. It states that if s is unconditional evidence that A is true, then A is in fact valid with proof witness s, or more generally, any proof term t equivalent to s (in a sense to be made precise shortly, cf. Sect. 2.3). Evidence for the truth of $[\![t]\!]A$ is constructed from the (verified) evidence that A is unconditionally true by prefixing it with a bang constructor. Finally, $\Box$E allows the discharging of validity hypotheses. In order to discharge the validity hypothesis v^A, a proof of the validity of A is required. In this system, this requires proving that $[\![r]\!]A$ is true with proof witness s, for some proof witness r and s. Note that r is a witness that A is unconditionally true (i.e. valid) whereas s is witness to the truth of $[\![r]\!]A$. The former is then substituted in the place of all free occurrences of v in the proposition C. This construction is recorded with proof witness $t\langle v^A{:=}r,s\rangle$ in the conclusion. The expression $C\{v^A\leftarrow r\}$ denotes the substitution of v^A by r in C. This and other forms of substitution will be explained in detail in Sect. 4.1. A final remark on $\Box$E, its witness includes r since this is required for the proof that derivable HLP formulae are also derivable in LP (Sect. 3.2) and also for Subject Reduction (see validity variable substitution and its use in the reduction rule γ in Sect. 4.3).

Regarding the schemes for plus we comment on PlusL, the case of PlusR being similar. Informally, the proof witness $s+t$ testifies that either s or t is

$$\dfrac{}{\Theta; \Gamma, x^A; \Delta \vdash A \mid x^A}\,\mathsf{Var}$$

$$\dfrac{\Theta; \Gamma, x^A; \Delta \vdash B \mid s}{\Theta; \Gamma; \Delta \vdash A \supset B \mid \lambda x^A.s}\,\supset\!\mathsf{I} \qquad \dfrac{\Theta; \Gamma; \Delta \vdash A \supset B \mid s \quad \Theta; \Gamma; \Delta \vdash A \mid t}{\Theta; \Gamma; \Delta \vdash B \mid s \cdot t}\,\supset\!\mathsf{E}$$

$$\dfrac{\Theta; \cdot; \cdot \vdash B \mid s \quad \Theta; \cdot; \cdot \vdash s \equiv t \colon B}{\Theta; \Gamma; \Delta \vdash \llbracket t \rrbracket B \mid\, !t}\,\Box\mathsf{I} \qquad \dfrac{\Theta; \Gamma; \Delta \vdash \llbracket r \rrbracket A \mid s \quad \Theta, v^A; \Gamma; \Delta \vdash C \mid t}{\Theta; \Gamma; \Delta \vdash C\{v^A \leftarrow r\} \mid t\langle v^A{:=}r, s\rangle}\,\Box\mathsf{E}$$

$$\dfrac{}{\Theta, v^A; \Gamma; \Delta \vdash A \mid v^A}\,\mathsf{VarM}$$

$$\dfrac{\Theta; \Gamma; \Delta \vdash A \mid s}{\Theta; \Gamma; \Delta \vdash A \mid s + t}\,\mathsf{PlusL} \qquad \dfrac{\Theta; \Gamma; \Delta \vdash A \mid t}{\Theta; \Gamma; \Delta \vdash A \mid s + t}\,\mathsf{PlusR}$$

$$\dfrac{\Theta; \Gamma; \Delta, \alpha^A \vdash A \mid s}{\Theta; \Gamma; \Delta, \alpha^A \vdash \bot \mid [\alpha^A]s}\,\mathsf{Name} \qquad \dfrac{\Theta; \Gamma; \Delta, \alpha^A \vdash \bot \mid s}{\Theta; \Gamma; \Delta \vdash A \mid \mu\alpha^A.s}\,\mathsf{NAbs}$$

FIGURE 1. Axiom and inference schemes of HLP

witness to the truth of A *without* supplying details on which of the two. Note that t is any proof witness whatsoever. Indeed, it may even contain variables not included in Θ, Γ nor Δ (see also Example 2.4). The reason is that we seek to preserve the *theorems* of LP in HLP, in particular $\llbracket s \rrbracket A \supset \llbracket s + t \rrbracket A$, which places no restriction on t. An alternative scheme requiring that the variables in t occur in the respective contexts:

$$\dfrac{\Theta; \Gamma; \Delta \vdash A \mid s \quad \mathsf{FVV}(t) \subseteq \Theta \quad \mathsf{FVT}(t) \subseteq \Gamma \quad \mathsf{FVF}(t) \subseteq \Delta}{\Theta; \Gamma; \Delta \vdash A \mid s + t}\,\mathsf{PlusL}'$$

would not allow this preservation to hold.

Finally, the schemes Name and NAbs were introduced by Parigot [16,17]. The intuition behind them is that hypotheses in Δ must be considered negated. Under this reading, the scheme Name states that from $\neg A$ and A we may deduce $\bot$. Likewise, the scheme NAbs is the classical negation rule stating that if we arrive at a contradiction from the hypothesis $\neg A$, then we may discharge this hypothesis and obtain A.

Some sample derivations follow.

Example 2.2. We prove $\cdot; \cdot; \cdot \vdash \llbracket s \rrbracket A \supset \llbracket !s \rrbracket \llbracket s \rrbracket A \mid \lambda x^{\llbracket s \rrbracket A}.!!v^A\langle v^A{:=}s, x^{\llbracket s \rrbracket A}\rangle$.

$$\dfrac{\dfrac{\dfrac{}{\cdot; x^{\llbracket s \rrbracket A}; \cdot \vdash \llbracket s \rrbracket A \mid x^{\llbracket s \rrbracket A}}\,\mathsf{Var} \qquad \dfrac{\dfrac{\dfrac{}{v^A; \cdot; \cdot \vdash A \mid v^A}\,\mathsf{VarM}}{v^A; \cdot; \cdot \vdash \llbracket v^A \rrbracket A \mid\, !v^A}\,\Box\mathsf{I}}{v^A; x^{\llbracket s \rrbracket A}; \cdot \vdash \llbracket !v^A \rrbracket \llbracket v^A \rrbracket A \mid\, !!v^A}\,\Box\mathsf{I}}{\cdot; x^{\llbracket s \rrbracket A}; \cdot \vdash \llbracket !s \rrbracket \llbracket s \rrbracket A \mid\, !!v^A\langle v^A{:=}s, x^{\llbracket s \rrbracket A}\rangle}\,\Box\mathsf{E}}{\cdot; \cdot; \cdot \vdash \llbracket s \rrbracket A \supset \llbracket !s \rrbracket \llbracket s \rrbracket A \mid \lambda x^{\llbracket s \rrbracket A}.!!v^A\langle v^A{:=}s, x^{\llbracket s \rrbracket A}\rangle}\,\supset\!\mathsf{I}$$

Example 2.3. The following judgement is easily seen to be derivable: $\cdot;\cdot;\cdot \vdash \llbracket x^A \cdot x^A \rrbracket B \supset \llbracket x^A \cdot x^A \rrbracket B \mid \lambda y^{\llbracket x^A \cdot x^A \rrbracket B}.y$. Note that the proof witness $x^A \cdot x^A$ does not denote any valid derivation in HLP. In fact, for any proof witness s, $\rhd_{\mathsf{HLP}} \cdot;\cdot;\cdot \vdash \llbracket s \rrbracket B \supset \llbracket s \rrbracket B \mid \lambda y^{\llbracket s \rrbracket B}.y$.

Example 2.4. The following example illustrates the $+$ operator, for which it is convenient to extend HLP with conjunction and disjunction [20]. We seek to prove the formula $\llbracket s \rrbracket A \vee \llbracket t \rrbracket B \supset \llbracket \mathsf{inl}(s) + \mathsf{inr}(t) \rrbracket (A \vee B)$.

$$\dfrac{\Theta;\Gamma;\Delta \vdash A \mid s \quad \Theta;\Gamma;\Delta \vdash B \mid t}{\Theta;\Gamma;\Delta \vdash A \wedge B \mid \mathsf{pair}(s,t)}\,\wedge_{\mathsf{I}} \qquad \dfrac{\Theta;\Gamma;\Delta \vdash A \wedge B \mid s}{\Theta;\Gamma;\Delta \vdash A \mid \mathsf{fst}(s)}\,\wedge_{\mathsf{E1}} \qquad \dfrac{\Theta;\Gamma;\Delta \vdash A \wedge B \mid s}{\Theta;\Gamma;\Delta \vdash B \mid \mathsf{snd}(s)}\,\wedge_{\mathsf{E2}}$$

$$\dfrac{\Theta;\Gamma;\Delta \vdash A \mid s}{\Theta;\Gamma;\Delta \vdash A \vee B \mid \mathsf{inl}(s)}\,\vee_{\mathsf{I1}} \qquad \dfrac{\Theta;\Gamma;\Delta \vdash B \mid s}{\Theta;\Gamma;\Delta \vdash A \vee B \mid \mathsf{inr}(s)}\,\vee_{\mathsf{I2}}$$

$$\dfrac{\Theta;\Gamma;\Delta \vdash A \vee B \mid r \quad \Theta;\Gamma, x^A;\Delta \vdash C \mid s \quad \Theta;\Gamma, y^B;\Delta \vdash C \mid t}{\Theta;\Gamma;\Delta \vdash C \mid \mathsf{case}\, r\, x^A.s\, y^B.t}\,\vee_{\mathsf{E}}$$

Let $\Theta_1 \triangleq v^A$, $\Theta_2 \triangleq u^B$, $\Gamma \triangleq z^{\llbracket s \rrbracket A \vee \llbracket t \rrbracket B}$ $\Gamma_1 \triangleq \Gamma, x^{\llbracket s \rrbracket A}$ and $\Gamma_2 \triangleq \Gamma, y^{\llbracket t \rrbracket B}$ in the following two derivations $\pi_{1,2}$:

$$\dfrac{\cdot;\Gamma_1;\cdot \vdash \llbracket s \rrbracket A \mid x^{\llbracket s \rrbracket A} \qquad \dfrac{\dfrac{\dfrac{\Theta_1;\cdot;\cdot \vdash A \mid v^A}{\Theta_1;\cdot;\cdot \vdash A \vee B \mid \mathsf{inl}(v^A)}\,\vee_{\mathsf{I1}}}{\Theta_1;\cdot;\cdot \vdash A \vee B \mid \mathsf{inl}(v^A) + \mathsf{inr}(t)}\,\mathsf{PlusL}}{\Theta_1;\Gamma_1;\cdot \vdash \llbracket \mathsf{inl}(v^A) + \mathsf{inr}(t) \rrbracket (A \vee B) \mid !(\mathsf{inl}(v^A) + \mathsf{inr}(t))}\,\Box\mathsf{I}}{\cdot;\Gamma_1;\cdot \vdash \llbracket \mathsf{inl}(s) + \mathsf{inr}(t) \rrbracket (A \vee B) \mid !(\mathsf{inl}(v^A) + \mathsf{inr}(t))\langle v^A := s, x^{\llbracket s \rrbracket A} \rangle}\,\Box\mathsf{E}$$

$$\dfrac{\cdot;\Gamma_2;\cdot \vdash \llbracket t \rrbracket B \mid y^{\llbracket s \rrbracket B} \qquad \dfrac{\dfrac{\dfrac{\Theta_2;\cdot;\cdot \vdash B \mid u^B}{\Theta_2;\cdot;\cdot \vdash A \vee B \mid \mathsf{inr}(u^B)}\,\vee_{\mathsf{I2}}}{\Theta_2;\cdot;\cdot \vdash A \vee B \mid \mathsf{inl}(s) + \mathsf{inr}(u^B)}\,\mathsf{PlusR}}{\Theta_2;\Gamma_2;\cdot \vdash \llbracket \mathsf{inl}(s) + \mathsf{inr}(u^B) \rrbracket (A \vee B) \mid !(\mathsf{inl}(s) + \mathsf{inr}(u^B))}\,\Box\mathsf{I}}{\cdot;\Gamma_2;\cdot \vdash \llbracket \mathsf{inl}(s) + \mathsf{inr}(t) \rrbracket (A \vee B) \mid !(\mathsf{inl}(s) + \mathsf{inr}(u^B))\langle u^B := t, y^{\llbracket s \rrbracket B} \rangle}\,\Box\mathsf{E}$$

Finally, for π_3 below consider the definitions:

$$\begin{aligned} r_1 &\triangleq !(\mathsf{inl}(v^A) + \mathsf{inr}(t))\langle v^A := s, x^{\llbracket s \rrbracket A} \rangle \\ r_2 &\triangleq !(\mathsf{inl}(s) + \mathsf{inr}(u^B))\langle u^B := t, y^{\llbracket t \rrbracket B} \rangle \\ r_3 &\triangleq \mathsf{case}\, z^{\llbracket s \rrbracket A \vee \llbracket t \rrbracket B}\, x^A.r_1\, y^B.r_2 \end{aligned}$$

$$\dfrac{\cdot;\Gamma;\cdot \vdash \llbracket s \rrbracket A \vee \llbracket t \rrbracket B \mid z^{\llbracket s \rrbracket A \vee \llbracket t \rrbracket B} \quad \overset{\pi_1}{\cdot;\Gamma_1;\cdot \vdash \llbracket \mathsf{inl}(s) + \mathsf{inr}(t) \rrbracket (A \vee B) \mid r_1} \quad \overset{\pi_2}{\cdot;\Gamma_2;\cdot \vdash \llbracket \mathsf{inl}(s) + \mathsf{inr}(t) \rrbracket (A \vee B) \mid r_2}}{\cdot;\Gamma;\cdot \vdash \llbracket \mathsf{inl}(s) + \mathsf{inr}(t) \rrbracket (A \vee B) \mid r_3}\,\vee_{\mathsf{E}}$$

Note that the use of PlusL in π_1 and PlusR in π_2 is required in order to concatenate the two alternative proofs of $A \vee B$ into a unique proof, and allow the application of $\vee_{\mathsf{E}}$ in π_3.

Remark 2.5. One may wonder whether, for the implicative fragment, the plus may be dispensed with while still maintaining realization of all $\mathsf{S4}$ theorems. This is the case if, in the terminology of LP, so called non-injective constant specification sets[1] and non-normal realizations are allowed (see [13] and also [1, Sect. 11.2]).

We end the section with a basic metatheoretic result which may be proved by induction on the derivation of $\Theta;\Gamma;\Delta\vdash A\,|\,s$.

Lemma 2.6 (Weakening, Strengthening). *If* $\rhd_{\mathit{HLP}}\,\Theta;\Gamma;\Delta\vdash A\,|\,s$, *then*

1. $\rhd_{\mathit{HLP}}\,\Theta\cup\Theta';\Gamma\cup\Gamma';\Delta\cup\Delta'\vdash A\,|\,s$; *and*
2. $\rhd_{\mathit{HLP}}\,\Theta\cap \mathit{FVV}(s);\Gamma\cap \mathit{FVT}(s);\Delta\cap \mathit{FVF}(s)\vdash A\,|\,s$.

2.3. Proof Witness Equivalence

The $\Box\mathsf{I}$ inference we have presented resorts to a notion of proof witness equivalence in order to derive the corresponding formula. It would be tempting to use a simpler approach:

$$\dfrac{\Theta;\cdot;\cdot\vdash B\,|\,s}{\Theta;\Gamma;\Delta\vdash [\![s]\!]B\,|\,!s}\;\Box\mathsf{I}'$$

However, if we were to replace $\Box\mathsf{I}$ with $\Box\mathsf{I}'$, proof normalization (studied in detail in Sect. 4) would yield invalid proofs. For instance:

$$\dfrac{\dfrac{\dfrac{\overset{\pi_1}{\Theta;x^A;\cdot\vdash B\,|\,s}}{\Theta;\cdot;\cdot\vdash A\supset B\,|\,\lambda x^A.s}\;\supset\mathsf{I}\qquad \overset{\pi_2}{\Theta;\cdot;\cdot\vdash A\,|\,t}}{\Theta;\cdot;\cdot\vdash B\,|\,\Theta;\cdot;\cdot\vdash B\,|\,(\lambda x^A.s)\cdot t}\;\supset\mathsf{E}}{\Theta;\Gamma;\Delta\vdash [\![(\lambda x^A.s)\cdot t]\!]B\,|\,!((\lambda x^A.s)\cdot t)}\;\Box\mathsf{I}'$$

would be normalised to:

$$\dfrac{\overset{\pi_3}{\Theta;\cdot;\cdot\vdash B\,|\,s\{x^A\leftarrow t\}}}{\Theta;\Gamma;\Delta\vdash [\![(\lambda x^A.s)\cdot t]\!]B\,|\,!((\lambda x^A.s)\cdot t)}\;\Box\mathsf{I}'$$

by resorting to an appropriate substitution principle for truth variables. The derivation which results from the reduction in the above example is invalid, since the witnesses $(\lambda x^A.s)\cdot t$ and $s\{x^A\leftarrow t\}$ are not the same. This shows that a naïve approach to Subject Reduction is doomed to fail. The current formulation of $\Box\mathsf{I}$ allows us to regain this property. It relies on proof witness equivalence judgements, which take the form $\Theta;\Gamma;\Delta\vdash\ s\equiv t\colon A$, meaning that s and t are equivalent witnesses for A under the hypotheses from the contexts Θ, Γ, Δ. The meaning of this judgement is given by the congruence closure (*i.e.* the compatible, reflexive, symmetric, transitive closure) of the schemes in Figs. 2 and 3. The schemes defining proof witness equivalence arise from an analysis of all cases of proof normalisation.

[1] A constant specification CS is **injective** if for each constant c there is at most one formula $[\![c]\!]A\in \mathit{CS}$ (each constant denotes a proof of not more than one axiom) [6].

$$\frac{\Theta; \Gamma, x^A; \Delta \vdash B \,|\, s \quad \Theta; \Gamma; \Delta \vdash A \,|\, t}{\Theta; \Gamma; \Delta \vdash\ (\lambda x^A.s) \cdot t \equiv s\{x^A \leftarrow t\} \colon B}\ \textsf{Eq-}\beta$$

$$\frac{\Theta; \cdot; \cdot \vdash A \,|\, s \quad \Theta, v^A; \Gamma; \Delta \vdash C \,|\, t}{\Theta; \Gamma; \Delta \vdash\ t\langle v^A := s, !s\rangle \equiv t\{v^A \leftarrow s\} \colon C\{v^A \leftarrow s\}}\ \textsf{Eq-}\gamma$$

$$\frac{\Theta; \Gamma; \Delta, \alpha^A, \beta^A \vdash \bot \,|\, s}{\Theta; \Gamma; \Delta, \beta^A \vdash\ [\beta^A]\mu\alpha^A.s \equiv s\{\alpha^A \leftarrow \beta^A\} \colon \bot}\ \textsf{Eq-}\mu$$

$$\frac{\Theta; \Gamma; \Delta, \alpha^{A\supset B} \vdash \bot \,|\, s \quad \Theta; \Gamma; \Delta \vdash A \,|\, t}{\Theta; \Gamma; \Delta \vdash\ (\mu\alpha^{A\supset B}.s) \cdot t \equiv \mu\beta^B.s\big\{{\scriptstyle [\alpha^{A\supset B}](\bullet) \leftarrow [\beta^B](\bullet)t}\big\} \colon B}\ \textsf{Eq-}\zeta$$

$$\frac{\Theta; \Gamma; \Delta \vdash A \,|\, s \quad \alpha^A \notin \textsf{FVF}(s)}{\Theta; \Gamma; \Delta \vdash\ \mu\alpha^A.[\alpha^A]s \equiv s \colon A}\ \textsf{Eq-}\theta$$

Figure 2. Proof witness equivalence (1/2)

Remark 2.7. If $\rhd_{\textsf{HLP}}\, \Theta; \Gamma; \Delta \vdash A \,|\, s$, then there is a derivation of $\Theta; \Gamma; \Delta \vdash A \,|\, s$ which does not make use of the equivalence rules. That is, there is a derivation which uses $\Box\textsf{I}'$ instead of $\Box\textsf{I}$. This follows from Lemma 2.8(1), below (whose proof does not introduce applications of $\Box\textsf{I}$). However, this derivation may not be in normal form.

Some basic metatheoretic results follow, all of which can be proved by induction on the derivation of $\Theta; \Gamma; \Delta \vdash\ s \equiv t \colon A$.

Lemma 2.8. *If* $\rhd_{\textsf{HLP}}\, \Theta; \Gamma; \Delta \vdash\ s \equiv t \colon A$*, then*

1. $\rhd_{\textsf{HLP}}\, \Theta; \Gamma; \Delta \vdash A \,|\, s$ *and* $\rhd_{\textsf{HLP}}\, \Theta; \Gamma; \Delta \vdash A \,|\, t$*;*
2. $\rhd_{\textsf{HLP}}\, \Theta \cup \Theta'; \Gamma \cup \Gamma'; \Delta \cup \Delta' \vdash\ s \equiv t \colon A$*; and*
3. $\rhd_{\textsf{HLP}}\, \Theta \cap \textsf{FVV}(s) \cap \textsf{FVV}(t); \Gamma \cap \textsf{FVT}(s) \cap \textsf{FVT}(t); \Delta \cap \textsf{FVF}(s) \cap \textsf{FVF}(t) \vdash$ $s \equiv t \colon A$*.*

3. LP

This section addresses the proof of equivalence, in terms of provability, between LP and HLP. The LP → HLP direction is quite straightforward, the other direction requires some more work. The syntax of LP was presented in the introduction. We assume that $\mathcal{C}$ is exactly the set of constants that consists of one constant for each instance of each axiom. We often distinguish in our notation the axiom to which a constant refers by putting the name of the axiom as superindex and the instances of its metavariables as its subindices. For example, we write $c^{\mathbf{A1}}_{x^P,P}$ for the constant corresponding to the instance $[\![x^P]\!]P \supset P$ of axiom **A1** (and similarly for the other axioms). Also, We write $\rhd_{\textsf{LP}}\, \Gamma \vdash A$ to indicate that A is provable in LP under hypotheses Γ.

$$\frac{\Theta;\Gamma;\Delta\vdash A\supset B\,|\,r\quad \Theta;\Gamma;\Delta\vdash A\,|\,t}{\Theta;\Gamma;\Delta\vdash\ (r+s)\cdot t\equiv(r\cdot t)+s\colon B}\ \mathsf{Eq}\text{-}\psi_L$$

$$\frac{\Theta;\Gamma;\Delta\vdash A\supset B\,|\,s\quad \Theta;\Gamma;\Delta\vdash A\,|\,t}{\Theta;\Gamma;\Delta\vdash\ (r+s)\cdot t\equiv r+(s\cdot t)\colon B}\ \mathsf{Eq}\text{-}\psi_R$$

$$\frac{\Theta;\Gamma;\Delta\vdash \llbracket r\rrbracket A\,|\,s\quad \Theta,v^A;\Gamma;\Delta\vdash C\,|\,u}{\Theta;\Gamma;\Delta\vdash\ u\langle v^A{:=}r,(s+t)\rangle\equiv u\langle v^A{:=}r,s\rangle+t\colon C\{v^A\leftarrow r\}}\ \mathsf{Eq}\text{-}\phi_L$$

$$\frac{\Theta;\Gamma;\Delta\vdash \llbracket r\rrbracket A\,|\,t\quad \Theta,v^A;\Gamma;\Delta\vdash C\,|\,u}{\Theta;\Gamma;\Delta\vdash\ u\langle v^A{:=}r,(s+t)\rangle\equiv s+u\langle v^A{:=}r,t\rangle\colon C\{v^A\leftarrow r\}}\ \mathsf{Eq}\text{-}\phi_R$$

$$\frac{\Theta;\Gamma;\Delta,\alpha^A\vdash A\,|\,s}{\Theta;\Gamma;\Delta,\alpha^A\vdash[\alpha^A](s+t)\equiv([\alpha^A]s)+t\colon\bot}\ \mathsf{Eq}\text{-}\chi_L\qquad \frac{\Theta;\Gamma;\Delta,\alpha^A\vdash A\,|\,t}{\Theta;\Gamma;\Delta,\alpha^A\vdash[\alpha^A](s+t)\equiv s+[\alpha^A]t\colon\bot}\ \mathsf{Eq}\text{-}\chi_R$$

$$\frac{\Theta,v^C;\Gamma;\Delta\vdash A\supset B\,|\,s_1\quad \Theta;\Gamma;\Delta\vdash\llbracket r\rrbracket C\,|\,s_2\quad \Theta;\Gamma;\Delta\vdash A\,|\,t}{\Theta;\Gamma;\Delta\vdash\ s_1\langle v^C{:=}r,s_2\rangle\cdot t\equiv(s_1\cdot t)\langle v^C{:=}r,s_2\rangle\colon B\{v^C\leftarrow r\}}\ \mathsf{Eq}\text{-}\upsilon_\beta$$

$$\frac{\Theta,v^B,u^C;\Gamma;\Delta\vdash A\,|\,t_1\quad \Theta,u^C;\Gamma;\Delta\vdash\llbracket r\rrbracket B\,|\,t_2\quad \Theta;\Gamma;\Delta\vdash\llbracket s\rrbracket C\,|\,t_3}{\Theta;\Gamma;\Delta\vdash\ t_1\langle v^B{:=}r,t_2\langle u^C{:=}s,t_3\rangle\rangle\equiv t_1\langle v^B{:=}r,t_2\rangle\langle u^C{:=}s,t_3\rangle\colon A\{v^B\leftarrow r\}}\ \mathsf{Eq}\text{-}\upsilon_\gamma$$

$$\frac{\Theta,v^A;\Gamma;\Delta,\beta^B\vdash B\,|\,s\quad \Theta;\Gamma;\Delta,\beta^B\vdash\llbracket r\rrbracket A\,|\,t}{\Theta;\Gamma;\Delta,\beta^B\vdash\ [\beta^B](s\langle v^A{:=}r,t\rangle)\equiv([\beta^B]s)\langle v^A{:=}r,t\rangle\colon\bot}\ \mathsf{Eq}\text{-}\upsilon_\mu$$

$$\frac{\Theta,v^B;\Gamma;\Delta,\alpha^A\vdash\bot\,|\,s\quad \Theta;\Gamma;\Delta\vdash\llbracket r\rrbracket B\,|\,t\quad \alpha^A\notin\mathsf{FVF}(N^{\llbracket r\rrbracket B})}{\Theta;\Gamma;\Delta\vdash\ \mu\alpha^A.(s\langle v^B{:=}r,t\rangle)\equiv(\mu\alpha^A.s)\langle v^B{:=}r,t\rangle\colon A}\ \mathsf{Eq}\text{-}\upsilon_\theta$$

$$\frac{\Theta;\Gamma;\Delta,\alpha^A\vdash\bot\,|\,s}{\Theta;\Gamma;\Delta\vdash\mu\alpha^A.(s+t)\equiv(\mu\alpha^A.s)+t\colon A}\ \mathsf{Eq}\text{-}\iota_L\qquad \frac{\Theta;\Gamma;\Delta,\alpha^A\vdash\bot\,|\,t}{\Theta;\Gamma;\Delta\vdash\mu\alpha^A.(s+t)\equiv s+\mu\alpha^A.t\colon A}\ \mathsf{Eq}\text{-}\iota_R$$

Figure 3. Proof witness equivalence (2/2)

We occasionally write Γ, A for Γ, x^A with x a fresh name, and $A \in \Gamma$, means that there is some hypothesis x^A in Γ. We will use a, b, c, v, w, x, y, z, α as names for hypotheses in LP-contexts. Let $\Gamma = \{x_1^{A_1}, \ldots, x_n^{A_n}\}$ be a context, and $\vec{u} = u_1, \ldots, u_n$ a list of proof polynomials, we define $\llbracket\vec{u}\rrbracket\Gamma$ as $\{{x'_1}^{\llbracket u_1\rrbracket A_1}, \ldots, {x'_n}^{\llbracket u_n\rrbracket A_n}\}$ with $x'_1, \ldots, x'_n$ fresh names.[2]

[2] Fresh names are required in order to avoid collisions. Note that the variables $x_i^{A_i}$ and ${x'_i}^{\llbracket u_i\rrbracket A_i}$ have different types.

3.1. From LP to HLP

The translation $\underline{\bullet}$ is a function from LP formulae and proof polynomials to HLP formulae and proof witnesses, resp., that consists in simply replacing each constant in a formula with an appropriate proof witness. In the case of a context, $\underline{\Gamma}$ is just $\{x^{\underline{A}} \mid x^A \in \Gamma\}$. The clauses associating proof witnesses to constants are as follows, where the first three correspond to the axioms of classical propositional logic (for readability these have been decorated with their corresponding propositions, for the remaining ones the reader is referred to Sect. 1.1):

$$\begin{array}{rcl}
\underline{c^{\mathbf{A0}}_{A,B}} & \triangleq & (\lambda x^{\underline{A}}.\lambda y^{\underline{B}}.x)^{A\supset B\supset A} \\
\underline{c^{\mathbf{A0}}_{A,B,C}} & \triangleq & (\lambda x^{\underline{A\supset B\supset C}}.\lambda y^{\underline{A\supset B}}.\lambda z^{\underline{A}}.x\cdot z\cdot(y\cdot z))^{(A\supset B\supset C)\supset(A\supset B)\supset A\supset C} \\
\underline{c^{\mathbf{A0}}_{A}} & \triangleq & (\lambda y^{\neg\neg\underline{A}}.\mu\alpha^{\underline{A}}.y\cdot\lambda x^{\underline{A}}.[\alpha^{\underline{A}}]x)^{\neg\neg A\supset A} \\
\underline{c^{\mathbf{A1}}_{t,A}} & \triangleq & \lambda x^{\underline{[\![t]\!]A}}.v\langle v^{\underline{A}}:=\underline{t}, x\rangle \\
\underline{c^{\mathbf{A2}}_{s,t,A,B}} & \triangleq & \lambda x^{\underline{[\![s]\!]A\supset B}}.\lambda y^{\underline{[\![t]\!]A}}.!(w\cdot v)\langle w^{\underline{A\supset B}}:=\underline{s}, x\rangle\langle v^{\underline{A}}:=\underline{t}, y\rangle \\
\underline{c^{\mathbf{A3}}_{s,A}} & \triangleq & \lambda x^{\underline{[\![s]\!]A}}.!!v^{\underline{A}}\langle v^{\underline{A}}:=\underline{s}, x^{\underline{[\![s]\!]A}}\rangle \\
\underline{c^{\mathbf{A4}}_{s,t,A}} & \triangleq & \lambda x^{\underline{[\![s]\!]A}}.!(\underline{v}+\underline{t})\langle v^{\underline{A}}:=\underline{s}, x\rangle \\
\underline{c^{\mathbf{A5}}_{s,t,A}} & \triangleq & \lambda x^{\underline{[\![t]\!]A}}.!(\underline{s}+\underline{v})\langle v^{\underline{A}}:=\underline{t}, x\rangle
\end{array}$$

Proposition 3.1. *If $\rhd_{\mathsf{LP}}\Gamma\vdash A$, then $\rhd_{\mathsf{HLP}}\cdot;\underline{\Gamma};\cdot\vdash\underline{A}\mid s$, for some s.*

The proof proceeds by induction on the derivation of $\Gamma\vdash A$. We exhibit a sample case for an axiom and for an inference rule. In the case of the axiom **A4** we prove it in HLP as follows:.

$$\dfrac{\dfrac{\dfrac{}{\cdot; x^{[\![s]\!]A};\cdot\vdash[\![s]\!]A\mid x^{[\![s]\!]A}}\,\mathsf{Var}\qquad\dfrac{\dfrac{\dfrac{}{v^A;\cdot;\cdot\vdash A\mid v^A}\,\mathsf{VarM}}{v^A;\cdot;\cdot\vdash A\mid v^A+t}\,\mathsf{PlusL}}{v^A; x^{[\![s]\!]A};\cdot\vdash[\![v^A+t]\!]A\mid !(v^A+t)}\,\Box\mathsf{I}}{\cdot; x^{[\![s]\!]A};\cdot\vdash[\![s+t]\!]A\mid !(v^A+t)\langle v^A:=s, x^{[\![s]\!]A}\rangle}\,\Box\mathsf{E}}{\cdot;\cdot;\cdot\vdash[\![s]\!]A\supset[\![s+t]\!]A\mid\lambda x^{[\![s]\!]A}.!(v^A+t)\langle v^A:=s, x^{[\![s]\!]A}\rangle}\,\supset\mathsf{I}$$

Remark 3.2. This proof is invalid were we to adopt PlusL′ rather than PlusL.

In the case of **R2**, it is easy to verify that for each instance of each axiom scheme $\mathbf{A}_i(\cdots)$ (the dots indicate the formulae parameters instantiating the axiom scheme) with $i\in 0..5$, the judgement $\cdot;\cdot;\cdot\vdash\underline{\mathbf{A}_i(\cdots)}\mid\underline{c^{\mathbf{Ai}}_{\ldots}}$ can be derived. Therefore,

$$\dfrac{\cdot;\cdot;\cdot\vdash\underline{\mathbf{A}_i(\cdots)}\mid\underline{c^{\mathbf{Ai}}_{\ldots}}}{\cdot;\cdot;\cdot\vdash[\![\underline{c^{\mathbf{Ai}}_{\ldots}}]\!]\underline{\mathbf{A}_i(\cdots)}\mid !\underline{c^{\mathbf{Ai}}_{\ldots}}}\,\Box\mathsf{I}$$

3.2. From HLP to LP

This section addresses the reverse direction, namely that all theorems of HLP are theorems of LP. More precisely, we seek to prove the following result for a suitable translation from proof witnesses and formulae in HLP to proof polynomials and formulae in LP.

$$\begin{array}{rcl@{\qquad}rcl} P^\star &\triangleq& P & \cdot^\star &\triangleq& \cdot \\ \bot^\star &\triangleq& \bot & (\Theta, v^A)^\star &\triangleq& \Theta^\star, [\![v^{A^\star}]\!]A^\star \\ (A\supset B)^\star &\triangleq& A^\star\supset B^\star & (\Gamma, x^A)^\star &\triangleq& \Gamma^\star, [\![x^{A^\star}]\!]A^\star \\ ([\![s]\!]A)^\star &\triangleq& [\![s^\star]\!]A^\star & (\Delta, \alpha^A)^\star &\triangleq& \Delta^\star, [\![\alpha^{\neg A^\star}]\!]\neg A^\star \end{array}$$

Figure 4. Translating HLP formulae and contexts

Corollary 3.3. *If $\rhd_{HLP} \cdot;\cdot;\cdot \vdash A \,|\, s$, then both $\rhd_{LP} \cdot \vdash [\![s^\star]\!]A^\star$ and $\rhd_{LP} \cdot \vdash A^\star$.*

It turns out the translation is unproblematic for formulae and hypotheses (Fig. 4), however, special care must be taken when defining the translation on proof witnesses. The following cases are straightforward:

$$\begin{array}{c@{\qquad}c} & (s\cdot t)^\star \triangleq s^\star \cdot t^\star \\ (x^A)^\star \triangleq x^{A^\star} & ([\alpha^A]s)^\star \triangleq \alpha^{\neg A^\star} \cdot s^\star \\ (v^A)^\star \triangleq v^{A^\star} & (!s)^\star \triangleq !(s^\star) \\ (s+t)^\star \triangleq s^\star + t^\star & (t\langle v^A := r, s\rangle)^\star \triangleq t^\star\{v^{A^\star} \leftarrow r^\star\} \end{array}$$

The more delicate cases are: $(\lambda x^A.s)^\star$ and $(\mu\alpha^A.s)^\star$. We briefly explain the case of the abstraction since that of name abstraction is similar. Bear in mind that the translation of an HLP-judgement $\Theta;\Gamma;\Delta \vdash A \,|\, s$ is defined as: $(\Theta;\Gamma;\Delta \vdash A \,|\, s)^\star \triangleq \Theta^\star, \Gamma^\star, \Delta^\star \vdash [\![s^\star]\!]A^\star$. Suppose that the last scheme applied in the derivation of a judgement $\Theta;\Gamma;\Delta \vdash C \,|\, s$ is:

$$\frac{\Theta;\Gamma, x^A;\Delta \vdash B \,|\, s}{\Theta;\Gamma;\Delta \vdash A\supset B \,|\, \lambda x^A.s}\supset\mathsf{I}$$

The I.H. will yield derivability in LP of:

$$\Theta^\star, \Gamma^\star, [\![x^{A^\star}]\!]A^\star, \Delta^\star \vdash [\![s^\star]\!]B^\star \tag{3.1}$$

However, we are after derivability of $\Theta^\star, \Gamma^\star, \Delta^\star \vdash [\![t]\!](A^\star \supset B^\star)$, for an appropriate proof polynomial t. Building a derivation of this judgement requires three steps (which conform the content of the Abstraction Lemma 3.7):

1. We first need to "drop" the outermost modalities of $[\![x^{A^\star}]\!]A^\star$ and $[\![s^\star]\!]B^\star$ from (3.1). This is achieved via the Stripping Lemma (3.6).
2. This allows us then to resort to the standard Deduction Theorem to deduce $A^\star \supset B^\star$.
3. Finally, we resort to the reflective capabilities of LP in order to deduce the appropriate proof polynomial t. This is achieved via the Internalisation Lemma (3.5).

Note that t is thus a function of the original LP derivation of (3.1). Since there may be multiple LP derivations of an LP judgement we shall assume in our proof of Corollary 3.3 that all derivable occurrences of (3.1) use the same derivation.

3.2.1. Abstraction in LP. This subsection develops the results involved in the three steps of the abstraction lemma. We begin with a definition.

Definition 3.4 (Extracted proof polynomial). Suppose $\rhd_{\mathsf{LP}} [\![\vec{u}]\!]\Gamma \vdash D$, then r is an extracted proof polynomial of D in $[\![\vec{u}]\!]\Gamma$ if at least one of the following conditions holds:

- D is of the form $A \supset B \supset A$, $(A \supset B \supset C) \supset (A \supset B) \supset A \supset C$ or $\neg\neg A \supset A$ and $r = c^{\mathbf{A0}}_{A,B}$, $c^{\mathbf{A0}}_{A,B,C}$ or $c^{\mathbf{A0}}_{A}$ respectively.
- D is of the form $[\![t]\!]A \supset A$ and $r = c^{\mathbf{A1}}_{t,A}$.
- D is of the form $[\![s]\!](A \supset B) \supset ([\![t]\!]A \supset [\![s \cdot t]\!]B)$ and $r = c^{\mathbf{A2}}_{s,t,A,B}$.
- D is of the form $[\![t]\!]A \supset [\![!t]\!][\![t]\!]A$ and $r = c^{\mathbf{A3}}_{t,A}$.
- D is of the form $[\![s]\!]A \supset [\![s + t]\!]A$ and $r = c^{\mathbf{A4}}_{s,t,A}$.
- D is of the form $[\![t]\!]A \supset [\![s + t]\!]A$ and $r = c^{\mathbf{A5}}_{s,t,A}$.
- D is of the form $[\![s]\!]A$ and $r = !s$.
- There is some A s.t. $[\![\vec{u}]\!]\Gamma \vdash A \supset D$ and $[\![\vec{u}]\!]\Gamma \vdash A$ are both derivable, and $r = s \cdot t$ where s and t are extracted proof polynomials of $A \supset D$ and A in $[\![\vec{u}]\!]\Gamma$ respectively.

Note that for a given D there may be multiple proof polynomials that qualify as extracted. For example if $D = A \supset A$, then $r_1 = I_A$ and $r_2 = c^{\mathbf{A1}}_{I_A, A \supset A} \cdot !I_A$ are both extracted proof polynomials of D, where $I_A = c^{\mathbf{A0}}_{A,A\supset A,A} \cdot c^{\mathbf{A0}}_{A,A\supset A} \cdot c^{\mathbf{A0}}_{A,A}$

Lemma 3.5 (Internalization). *If $\rhd_{LP} [\![\vec{u}]\!]\Gamma \vdash D$, then:*

1. *There exists at least one extracted proof polynomial of D in $[\![\vec{u}]\!]\Gamma$.*
2. *If r is an extracted proof polynomial of D in $[\![\vec{u}]\!]\Gamma$, then $\rhd_{LP} [\![\vec{u}]\!]\Gamma \vdash [\![r]\!]D$.*

Proof. Part 2 follows directly from the axioms and inference rules of LP. Part 1 is by induction on the derivation of $[\![\vec{u}]\!]\Gamma \vdash D$, finding an extracted proof polynomial r for each case:

- If there is some hypothesis $x^{[\![u]\!]A} \in [\![\vec{u}]\!]\Gamma$ and the derivation is obtained by using this hypothesis, then $D = [\![u]\!]A$ and $r = !u$ (note that $[\![\vec{u}]\!]\Gamma$ can only contain hypotheses of the form $x^{[\![u]\!]A}$ for some u and A).
- If the derivation is an instance of an axiom **Ai** with $i \in \{0, \cdots, 5\}$, then $r = c^{\mathbf{Ai}}_{\ldots}$ (with the corresponding arguments for D).
- If the derivation is obtained by using **R2**, then D is of the form $[\![c^{\mathbf{Ai}}_{\ldots}]\!]A$ and $r = !c^{\mathbf{Ai}}_{\ldots}$.
- If the derivation is obtained by using **R1** from $[\![\vec{u}]\!]\Gamma \vdash A \supset D$ and $[\![\vec{u}]\!]\Gamma \vdash A$, then by I.H. there exist s and t extracted proof polynomial of $A \supset D$ and A respectively. Take $r = s \cdot t$.

□

Lemma 3.6 (Stripping). *Suppose $\rhd_{LP} \Gamma, x^{[\![y^A]\!]A} \vdash B$ with derivation π and $y^A \notin \Gamma$. Then there is a derivation of $\Gamma, y^A \vdash B'$, where B' results from B, by replacing all occurrences of $[\![t]\!]A$ by A for every proof polynomial t containing y^A (including constants for instances of axioms containing y^A).*

Proof. By induction on π.

- If $B = [\![y^A]\!]A$ and π is obtained by using the hypothesis $x^{[\![y^A]\!]A}$, then $B' = A$ and π' is the derivation of $\Gamma, y^A \vdash A$ obtained by using the hypothesis y^A.
- If π is obtained by using a hypothesis $y^B \in \Gamma$, then there is a derivation of $\Gamma \vdash B$ which uses neither $x^{[\![y^A]\!]A}$ nor y^A. We obtain π' from this derivation by Weakening, and $B' = B$.
- If π is obtained by using an axiom **A0-A5**, there are three possibilities:
  - B has no proof polynomial containing y^A: then $B' = B$, and the derivation of $\Gamma \vdash B$ can be obtained by Weakening of the axiom.
  - B has one or more proof polynomials containing y^A, but B' is still an instance of the same axiom. Since axioms can be derived in any context, then $\Gamma, y^A \vdash B'$ is derivable.
  - B has at least one proof polynomial containing y^A in a way that B' is no longer an instance of the same axiom as B: in this case, B' is an instance of one of the following schemes:
    1. $A \supset A$ from axioms **A1**, **A3**, **A4**, **A5**.
    2. $(A \supset B) \supset ([\![t]\!]A \supset B)$, 3. $[\![s]\!](A \supset B) \supset (A \supset B)$ or 4. $(A \supset B) \supset (A \supset B)$ from axiom **A2**.

    All these can be derived in LP in any context.
- If π is obtained by applying **R1**: then $\Gamma, x^{[\![y^A]\!]A} \vdash B$ is deduced from Γ, $x^{[\![y^A]\!]A} \vdash C \supset B$ and $\Gamma, x^{[\![y^A]\!]A} \vdash C$. By I.H. we have derivations of $\Gamma, y^A \vdash C' \supset B'$ and $\Gamma, y^A \vdash C'$. Therefore, by **R1**, we obtain a derivation of $\Gamma, y^A \vdash B'$.
- If π is obtained by applying **R2**, then B is of the form $[\![c]\!]D$ with c a proof constant and D an instance of an axiom. If $y^A \in D$, then $B' = D'$ and we resort to the third item of the proof above. Otherwise, $B' = B$. Finally, we conclude with necessitation.

□

Below we shall write $t^A_\lambda(\Gamma)$ to emphasize that the proof polynomial is associated to λ-abstraction, that the formula that it proves is A and that it depends on hypothesis in Γ.

Lemma 3.7 (λ-Abstraction). *If $\rhd_{\mathsf{LP}} [\![\vec{u}]\!]\Gamma, y^{[\![x^A]\!]A} \vdash [\![s(\vec{u}, x^A)]\!]B$ and $x^A \notin \Gamma, B$, then there exists $t^{A\supset B}_\lambda([\![\vec{u}]\!]\Gamma)$ such that $\rhd_{\mathsf{LP}} [\![\vec{u}]\!]\Gamma \vdash [\![t^{A\supset B}_\lambda([\![\vec{u}]\!]\Gamma)]\!](A \supset B)$, and $t^{A\supset B}_\lambda([\![\vec{u}]\!]\Gamma)$ is an extracted proof polynomial of $A \supset B$ in $[\![\vec{u}]\!]\Gamma$.*

Proof. W.l.o.g. we may assume that $x^A \in s(\vec{u}, x^A)$. Indeed, if this were not the case, then we could add it as follows:

(a) $[\![\vec{u}]\!]\Gamma, y^{[\![x^A]\!]A} \vdash [\![c^{\mathbf{A0}}_{B,A}]\!](B \supset A \supset B)$
(b) $[\![\vec{u}]\!]\Gamma, y^{[\![x^A]\!]A} \vdash [\![s(\vec{u}, x^A)]\!]B$
(c) $[\![\vec{u}]\!]\Gamma, y^{[\![x^A]\!]A} \vdash [\![c^{\mathbf{A0}}_{B,A} \cdot s(\vec{u}, x^A)]\!](A \supset B)$
(d) $[\![\vec{u}]\!]\Gamma, y^{[\![x^A]\!]A} \vdash [\![x^A]\!]A$
(e) $[\![\vec{u}]\!]\Gamma, y^{[\![x^A]\!]A} \vdash [\![c^{\mathbf{A0}}_{B,A} \cdot s(\vec{u}, x^A) \cdot x^A]\!]B$

We reason as follows:

$$\begin{array}{ll}
[\![\vec{u}]\!]\Gamma, y^{[\![x^A]\!]A} \vdash [\![s(\vec{u}, x^A)]\!]B & \text{(Hypothesis)} \\
[\![\vec{u}]\!]\Gamma, x^A \vdash B & \text{(Stripping and } x \in s(\vec{u}, x)\text{)} \\
[\![\vec{u}]\!]\Gamma \vdash A \supset B & \text{(Deduction for } \mathsf{LP}\text{)} \\
[\![\vec{u}]\!]\Gamma \vdash [\![t_\lambda^{A\supset B}([\![\vec{u}]\!]\Gamma)]\!](A \supset B) & \text{(Internalization for } \mathsf{LP}\text{)}
\end{array}$$

□

Corollary 3.8 (μ-Abstraction). *If* $\rhd_{\mathsf{LP}} [\![\vec{u}]\!]\Gamma, y^{[\![\alpha^{\neg A}]\!]\neg A} \vdash [\![s(\vec{u}, \alpha^{\neg A})]\!]\bot$ *and* $\alpha^{\neg A} \notin \Gamma$, *let* $t_\mu^A([\![\vec{u}]\!]\Gamma) = c_A^{\mathbf{A0}} \cdot t_\lambda^{\neg\neg A}([\![\vec{u}]\!]\Gamma)$, *then* $\rhd_{\mathsf{LP}} [\![\vec{u}]\!]\Gamma \vdash [\![t_\mu^A([\![\vec{u}]\!]\Gamma)]\!]A$ *(where* $c_A^{\mathbf{A0}}$ *is a constant corresponding to the classical logic axiom* $\neg\neg A \supset A$*).*

Proof. We reason as follows:

$$\begin{array}{ll}
[\![\vec{u}]\!]\Gamma \vdash [\![t_\lambda^{\neg\neg A}([\![\vec{u}]\!]\Gamma)]\!](\neg\neg A) & (\lambda\text{-Abstraction}) \\
[\![\vec{u}]\!]\Gamma \vdash [\![c_A^{\mathbf{A0}}]\!](\neg\neg A \supset A) & (\mathbf{A0} \text{ and } \mathbf{R2}) \\
[\![\vec{u}]\!]\Gamma \vdash [\![c_A^{\mathbf{A0}} \cdot t_\lambda^{\neg\neg A}([\![\vec{u}]\!]\Gamma)]\!]A & (\mathbf{A2}, \text{ and } \mathbf{R1} \text{ twice})
\end{array}$$

□

Lemma 3.9 (Substitution). $\Gamma \vdash [\![s]\!]A$ *and* $\Gamma, y^{[\![x^A]\!]A} \vdash B$ *and* $x^A \notin \Gamma$ *implies* $\Gamma \vdash B\{x^A \leftarrow s\}$.

3.2.2. Completing the Definition of the Translation. Returning to our translation described at the beginning of Sect. 3.2, we now address the defining clauses for $(\lambda x^A.s)^\star$ and $(\mu\alpha^A.s)^\star$. Let us say a proof witness s is **inhabited** if for some Θ, Γ, Δ and A, $\rhd_{\mathsf{HLP}} \Theta; \Gamma; \Delta \vdash A \,|\, s$. Also, let $c^{\mathbf{A1}}$ be the proof constant denoting any instance of **A1**.

$$\begin{array}{lll}
(\lambda x^A.s)^\star & \triangleq & \text{any } t_\lambda^{A^\star \supset B^\star}(\Theta^\star, \Gamma^\star, \Delta^\star) \text{ for any } \Theta, \Gamma, \Delta, B \text{ s.t.} \\
& & \Theta; \Gamma; \Delta \vdash A \supset B \,|\, \lambda x^A.s \text{ is derivable, if } \lambda x^A.s \text{ is inhabited.} \\
(\lambda x^A.s)^\star & \triangleq & c^{\mathbf{A1}} \cdot c^{\mathbf{A1}}, \text{ otherwise.} \\
(\mu\alpha^A.s)^\star & \triangleq & \text{any } t_\mu^A(\Theta^\star, \Gamma^\star, \Delta^\star) \text{ for any } \Theta, \Gamma, \Delta \text{ s.t.} \\
& & \Theta; \Gamma; \Delta \vdash A \,|\, \mu\alpha^A.s \text{ is derivable, if } \mu\alpha^A.s \text{ is inhabited.} \\
(\mu\alpha^A.s)^\star & \triangleq & c^{\mathbf{A1}} \cdot c^{\mathbf{A1}}, \text{ otherwise.}
\end{array}$$

In our use of this translation (Proposition 3.10) the conditions of the first clause and third clauses shall be met when dealing with modalities that are introduced using □I; the other cases are used when uninhabited proof witnesses occur inside boxes that are not introduced. In the former cases, note that there may be more than one possible proof polynomial (for instance, $\lambda x^A.(y^B + z^B)$ and $[\![\lambda x^A.(y^B + z^B)]\!]A \supset B$). Any of these may be resorted to since they are all extracted proof polynomials of the same formula under the same context, provided that the proof witnesses to be translated can verify some formula (*i.e.* they are the s in some derivable judgment $\Theta; \Gamma; \Delta \vdash A \,|\, s$). Otherwise, if the proof witness is not inhabited (for example $\lambda x^A.x^A \cdot x^A$), then its content is unimportant and any translation will yield the same results. For each inhabited proof witness, we shall assume that we use one and the same proof of the corresponding judgement.

Proposition 3.10. *If* $\rhd_{\mathsf{HLP}} \Theta; \Gamma; \Delta \vdash D \,|\, s$ *without resorting to proof witness equivalence, then* $\rhd_{\mathsf{LP}} \Theta^\star \cup \Gamma^\star \cup \Delta^\star \vdash [\![s^\star]\!]D^\star$.

Proof. Since $\Theta; \Gamma; \Delta \vdash D \,|\, s$ is derivable in HLP, let π be a such a derivation. We will prove by induction on π that $\rhd_{\mathsf{LP}} \Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket s^\star \rrbracket D^\star$.

1. Case Var (VarM is similar and hence omitted): $\Theta; \Gamma; \Delta \vdash D \,|\, s$ is of the form $\Theta; \Gamma', x^A; \Delta \vdash A \,|\, x^A$. Trivially we have $\rhd_{\mathsf{LP}} \llbracket x^{A^\star} \rrbracket A^\star \vdash \llbracket x^{A^\star} \rrbracket A^\star$ and hence $\rhd_{\mathsf{LP}} \Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket x^{A^\star} \rrbracket A^\star$ by Weakening.

2. Case $\supset\mathsf{I}$: the derivation ends in $\dfrac{\Theta; \Gamma, x^A; \Delta \vdash B \,|\, s}{\Theta; \Gamma; \Delta \vdash A \supset B \,|\, \lambda x^A.s} \supset\mathsf{I}$:

   we will use the contexts $\Theta^\star$, $\Gamma^\star$ and $\Delta^\star$ for the translation of $\lambda x^A.s$. We want to see that $\rhd_{\mathsf{LP}} \Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket t_\lambda^{A^\star \supset B^\star}(\Theta^\star, \Gamma^\star, \Delta^\star) \rrbracket (A^\star \supset B^\star)$. (We know $\llbracket t_\lambda^{A^\star \supset B^\star}(\Theta^\star, \Gamma^\star, \Delta^\star) \rrbracket (A^\star \supset B^\star)$ is a correct translation of $\llbracket s \rrbracket D$, since $\Theta; \Gamma; \Delta \vdash A \supset B \,|\, \lambda x^A.s$ is derivable by hypothesis).

   By the I.H. $\rhd_{\mathsf{LP}} \Theta^\star, \Gamma^\star, \llbracket x^{A^\star} \rrbracket A^\star, \Delta^\star \vdash \llbracket s^\star \rrbracket B^\star$. Therefore, from the λ-Abstraction Lemma (3.7), we obtain $t_\lambda^{A^\star \supset B^\star}(\Theta^\star, \Gamma^\star, \Delta^\star)$ extracted proof polynomial of $A^\star \supset B^\star$ in $\Theta^\star, \Gamma^\star, \Delta^\star$. This proof polynomial moreover verifies $\rhd_{\mathsf{LP}} \Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket t_\lambda^{A^\star \supset B^\star}(\Theta^\star, \Gamma^\star, \Delta^\star) \rrbracket (A^\star \supset B^\star)$. Note that, by Internalization, *any* extracted proof polynomial of $A^\star \supset B^\star$ in $\Theta^\star, \Gamma^\star, \Delta^\star$ can be used in place of $t_\lambda^{A^\star \supset B^\star}(\Theta^\star, \Gamma^\star, \Delta^\star)$. This means that, whenever $\supset\mathsf{I}$ is used within a derivation, we may choose whatever extracted proof polynomial works best in order to translate the derivation as a whole.

3. Case $\supset\mathsf{E}$: the derivation ends in $\dfrac{\Theta; \Gamma; \Delta \vdash A \supset B \,|\, s \quad \Theta; \Gamma; \Delta \vdash A \,|\, t}{\Theta; \Gamma; \Delta \vdash B \,|\, s \cdot t} \supset\mathsf{E}$

   By the I.H. both of the following judgements are derivable in LP:
   (a) $\Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket s^\star \rrbracket (A \supset B)^\star$ and
   (b) $\Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket t^\star \rrbracket A^\star$

   From these, using **A2** and **R1** twice, we derive $\Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket s^\star \cdot t^\star \rrbracket B^\star$ in LP.

   Note that we can always choose the same $A^\star$ as the translation of A on both sides regardless of how each premise was derived.

4. Case $\Box\mathsf{I}$: the derivation ends in $\dfrac{\Theta; \cdot; \cdot \vdash B \,|\, s}{\Theta; \Gamma; \Delta \vdash \llbracket s \rrbracket B \,|\, !s} \Box\mathsf{I}$

   We reason as follows:
   (a) $\Theta^\star \vdash \llbracket s^\star \rrbracket B^\star$ (I.H.)
   (b) $\Theta^\star \vdash \llbracket s^\star \rrbracket B^\star \supset \llbracket !s^\star \rrbracket \llbracket s^\star \rrbracket B^\star$ (**A3**)
   (c) $\Theta^\star \vdash \llbracket !s^\star \rrbracket \llbracket s^\star \rrbracket B^\star$ (**R1** from (b) and (a))
   (d) $\Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket !s^\star \rrbracket \llbracket s^\star \rrbracket B^\star$ (Weakening)

5. Case $\Box\mathsf{E}$: the derivation ends in $\dfrac{\Theta; \Gamma; \Delta \vdash \llbracket r \rrbracket A \,|\, s \quad \Theta, v^A; \Gamma; \Delta \vdash C \,|\, t}{\Theta; \Gamma; \Delta \vdash C\{v^A \leftarrow r\} \,|\, t\langle v^A := r, s\rangle} \Box\mathsf{E}$

   By the I.H. both of the following judgements are derivable in LP:
   (a) $\Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket s^\star \rrbracket \llbracket r^\star \rrbracket A^\star$ and
   (b) $\Theta^\star, \llbracket v^{A^\star} \rrbracket A^\star, \Gamma^\star, \Delta^\star \vdash \llbracket t^\star \rrbracket C^\star$

   We now reason as follows:
   (1) $\Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket s^\star \rrbracket \llbracket r^\star \rrbracket A^\star \supset \llbracket r^\star \rrbracket A^\star$ (**A1**)
   (2) $\Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket r^\star \rrbracket A^\star$ ((a) and **R1**)
   (3) $\Theta^\star, \Gamma^\star, \Delta^\star \vdash \llbracket t^\star\{v^{A^\star} \leftarrow r^\star\} \rrbracket C^\star\{v^{A^\star} \leftarrow r^\star\}$ (Lemma 3.9)

6. Case Name: the derivation ends in $\dfrac{\Theta;\Gamma;\Delta,\alpha^A \vdash A \,|\, s}{\Theta;\Gamma;\Delta,\alpha^A \vdash \bot \,|\, [\alpha^A]s}$ Name

   By I.H., $\Theta^\star,\Gamma^\star,\Delta^\star, x^{\llbracket \alpha^{\neg A^\star}\rrbracket \neg A^\star} \vdash \llbracket s^\star \rrbracket A^\star$ is derivable in LP.
   We reason as follows:

   (1) $\Theta^\star,\Gamma^\star,\Delta^\star, x^{\llbracket \alpha^{\neg A^\star}\rrbracket \neg A^\star} \vdash \llbracket \alpha^{\neg A^\star}\rrbracket \neg A^\star$ (hypothesis $x^{\llbracket \alpha^{\neg A^\star}\rrbracket \neg A^\star}$)
   (2) $\Theta^\star,\Gamma^\star,\Delta^\star, x^{\llbracket \alpha^{\neg A^\star}\rrbracket \neg A^\star} \vdash \llbracket s^\star \rrbracket A^\star$ (I.H.)
   (3) $\Theta^\star,\Gamma^\star,\Delta^\star, x^{\llbracket \alpha^{\neg A^\star}\rrbracket \neg A^\star} \vdash \llbracket \alpha^{\neg A^\star} \cdot s^\star \rrbracket \bot$ (**A2** and **R1** twice)

7. Case NAbs: the derivation ends in $\dfrac{\Theta;\Gamma;\Delta,\alpha^A \vdash \bot \,|\, s}{\Theta;\Gamma;\Delta \vdash A \,|\, \mu\alpha^A.s}$ NAbs

   By I.H. $\rhd_{\mathsf{LP}} \Theta^\star,\Gamma^\star,\Delta^\star, \llbracket \alpha^{\neg A^\star}\rrbracket A^\star \vdash \llbracket s^\star \rrbracket \bot$. From the μ-Abstraction Corollary (3.8), $\rhd_{\mathsf{LP}} \Theta^\star,\Gamma^\star,\Delta^\star \vdash \llbracket t_\mu^{A^\star}(\Theta^\star,\Gamma^\star,\Delta^\star)\rrbracket A^\star$, where the proof polynomial $t_\mu^{A^\star}(\Theta^\star,\Gamma^\star,\Delta^\star) = c^{\mathbf{A0}}_{A^\star} \cdot t_\lambda^{\neg\neg A}(\Theta^\star,\Gamma^\star,\Delta^\star)$. Again, by Internalization, if this rule is applied within a larger derivation, we can choose $t_\lambda^{\neg\neg A}(\Theta^\star,\Gamma^\star,\Delta^\star)$ freely among all possible extracted proof polynomials of $\neg\neg A$ in $\Theta^\star,\Gamma^\star,\Delta^\star$.

8. Case PlusL (the case PlusR is similar and hence omitted): the derivation ends in $\dfrac{\Theta;\Gamma;\Delta \vdash A \,|\, s}{\Theta;\Gamma;\Delta \vdash A \,|\, s+t}$ PlusL.

   By the I.H. $\rhd_{\mathsf{LP}} \Theta^\star,\Gamma^\star,\Delta^\star \vdash \llbracket s^\star \rrbracket A^\star$. Thus, by **A4** and **R1**, also $\rhd_{\mathsf{LP}} \Theta^\star,\Gamma^\star,\Delta^\star \vdash \llbracket s^\star + t^\star \rrbracket A^\star$.

□

Finally, note that the proof of the first item of Corollary 3.3 follows from Proposition 3.10 and that any judgement derivable in HLP may also be derived in the system in which □I is replaced by □I′ (Remarks 2.7). The latter item of Corollary 3.3 is obtained by additionally resorting to axiom **A1**.

4. Term Assignment

This section presents a term assignment for HLP. We seek to encode derivations in HLP as terms and analyse normalisation of derivations by means of these terms. Note that proof witnesses do not play the role of terms since they do not encode derivations in HLP (cf. Fig. 1). For instance, the proof witness $v^A + w^A$ ensures that A is true but it does not tell us which hypothesis was used in order to derive it. In fact, there are two possible derivations, one using v^A and PlusL, and the other using w^A and PlusR. Similarly, $!v^A$ can be used to verify that $\llbracket v^A \rrbracket A$ is true assuming v^A as a validity hypothesis, but this may have been derived in an infinite number of ways, using □I with any witness which is equivalent to v^A (for example, v^A itself, $(\lambda x^A.x^A) \cdot v^A$, $\mu\alpha^A.[\alpha^A]v^A$, etc.). So we introduce a notion of term very similar to that of proof witness, but which is better suited for studying normalisation of derivations and then focus on the combinatorial properties of normalisation, namely strong normalisation and confluence.

4.1. Terms and Substitution

The set of terms for HLP is defined as follows:

$$\begin{aligned} M, N ::= {} & x^A \mid v^A \mid (\lambda x^A.M^B)^{A \supset B} \mid (M^{A \supset B} N^A)^B \mid (!M^A)^{[\![s]\!]A} \\ \mid \quad & (N^B \langle v^A{:=}r, M \rangle)^{B\{v^A \leftarrow r\}} \mid ([\alpha^A]M^A)^{\perp} \mid (\mu\alpha^A.M^{\perp})^A \\ \mid \quad & (M^A +_{\mathrm{L}} s)^A \mid (s +_{\mathrm{R}} N^B)^B \end{aligned}$$

Free variables of validity, truth and falsehood over terms are defined analogously to those for proof witnesses. Again, decorations may be omitted where it is safe and we will use the letters M, N, L—with or without superindices—to refer to terms. Also, we assume, in all contexts, that bound variables are renamed in order to avoid unwanted capture. Returning to the above-mentioned examples, the term $(v^A +_{\mathrm{L}} w^A)^A$ encodes a proof of A using PlusL and v^A, and not the alternative (which would be encoded by $(v^A +_{\mathrm{R}} w^A)^A$). Similarly, the term $(!((\lambda x^A.x^A)^{A \supset A} v^A)^A)^{[\![v^A]\!]A}$ encodes a proof of $[\![v^A]\!]A$ which uses $(\lambda x^A.x^A) \cdot v^A$ as a witness for the premises, and not v^A, $\mu\alpha^A.[\alpha^A]v^A$ nor any other equivalent witness. Also, the terms $(!v^A)^{[\![v^A]\!]A}$ and $(!v^A)^{[\![(\lambda x^A.x^A) \cdot v^A]\!]A}$ encode different derivations, which are used to prove different formulae. Hence type annotations over a "!" term constructor are important.

Note, however, that some information is still left out, since our terms do not encode the proof witness equivalence schemes used to derive the second premise of □I (nor the contexts used in the derivations). However, these terms provide us with enough information to reason about the proof normalisation process and other properties of the metatheory.

Remark 4.1. For term assignments in which the full derivation is encoded, the reader is referred to [7]. There, an additional syntactic category encoding derivations of equivalence of proof witnesses is introduced and related to computation traces.

Before presenting the typing rules, we briefly introduce the various notions of substitution. There are three kinds of substitution following the three kinds of variable which are substituted: *truth variable substitution*, *validity variable substitution* and *structural substitution*. Apart from that, for each of these three notions of substitution, we in turn have three variants depending on the nature of the expression in which the variable is substituted. For example, in the case of truth variable substitution we have:

truth variable substitution (over proof witnesses)	$r\{y^A \leftarrow s^A\}$
truth variable substitution (over terms)	$M\{y^A \leftarrow N^A\}$
truth variable substitution (over formulae)	$B\{y^A \leftarrow s^A\}$

For the purposes of easing the presentation we shall present truth variable substitution in some detail and then only present the more interesting defining clauses of the remaining notions. Truth variable substitution over proof witnesses ($r\{y^A \leftarrow s^A\}$) is defined recursively as follows:

$$\begin{array}{ll}
y^A & \{y^A \leftarrow s^A\} \triangleq s \\
x^B & \{y^A \leftarrow s^A\} \triangleq x^B \text{ if } x^B \neq y^A \\
v^B & \{y^A \leftarrow s^A\} \triangleq v^B \\
(\lambda y^A.t) & \{y^A \leftarrow s^A\} \triangleq \lambda y^A.t \\
(\lambda x^B.t) & \{y^A \leftarrow s^A\} \triangleq \lambda x^B.(t\{y^A \leftarrow s\}) \text{ if } x^B \neq y^A \\
r \cdot t & \{y^A \leftarrow s^A\} \triangleq r\{y^A \leftarrow s\} \cdot (t\{y^A \leftarrow s\}) \\
!t & \{y^A \leftarrow s^A\} \triangleq !t \\
t\langle v^B{:=}u, r\rangle & \{y^A \leftarrow s^A\} \triangleq t\{y^A \leftarrow s\}\langle v^B{:=}u, r\{y^A \leftarrow s\}\rangle \\
r + t & \{y^A \leftarrow s^A\} \triangleq (r\{y^A \leftarrow s\}) + (t\{y^A \leftarrow s\}) \\
([\alpha^B]t) & \{y^A \leftarrow s^A\} \triangleq [\alpha^B](t\{y^A \leftarrow s\}) \\
(\mu\alpha^B.t) & \{y^A \leftarrow s^A\} \triangleq \mu\alpha^B.(t\{y^A \leftarrow s\})
\end{array}$$

Truth variable substitution over terms is written $M\{y^A \leftarrow N^A\}$. Note that y^A is substituted by a term, namely N^A. However, consider the term $M = P^A +_{\mathrm{L}} y^A$. The variable y^A to the right of the plus, must be substituted by a proof witness associated to N^A rather than the term itself. This can be obtained from N^A by computing its *associated witness*:

$$\begin{array}{ll}
\mathsf{w}(x^A) & = x^A \\
\mathsf{w}(v^A) & = v^A \\
\mathsf{w}((\lambda x^A.M^B)^{A\supset B}) & = \lambda x^A.\,\mathsf{w}(M^B) \\
\mathsf{w}((M^{A\supset B} N^A)^B) & = \mathsf{w}(M^{A\supset B}) \cdot \mathsf{w}(N^A) \\
\mathsf{w}((!M^A)^{[\![s]\!]A}) & = !s \\
\mathsf{w}((N^B\langle v^A{:=}r, M^{[\![r]\!]A}\rangle)^{B\{v^A \leftarrow r\}}) & = \mathsf{w}(N^B)\langle v^A{:=}r, \mathsf{w}(M^{[\![r]\!]A})\rangle \\
\mathsf{w}(([\alpha^A]M^A)^{\perp}) & = [\alpha^A]\,\mathsf{w}(M^A) \\
\mathsf{w}((\mu\alpha^A.M^{\perp})^A) & = \mu\alpha^A.\,\mathsf{w}(M^{\perp}) \\
\mathsf{w}((M^A +_{\mathrm{L}} t)^A) & = \mathsf{w}(M^A) + t \\
\mathsf{w}((s +_{\mathrm{R}} N^B)^B) & = s + \mathsf{w}(N^B)
\end{array}$$

We now provide the definition of truth variable substitution over terms:

$$\begin{array}{ll}
y^A & \{y^A{\leftarrow}N^A\} \triangleq N^A \\
x^B & \{y^A{\leftarrow}N^A\} \triangleq x^B \text{ if } x^B \neq y^A \\
v^B & \{y^A{\leftarrow}N^A\} \triangleq v^B \\
(\lambda y^A.M^B)^{A\supset B} & \{y^A{\leftarrow}N^A\} \triangleq (\lambda y^A.M^B)^{A\supset B} \\
(\lambda x^B.M^B)^{A\supset B} & \{y^A{\leftarrow}N^A\} \triangleq (\lambda x^B.(M^B\{\alpha^A{\leftarrow}N^A\}))^{A\supset B} \text{ if } x^B \neq y^A \\
(M_1^{C\supset B} M_2^C)^B & \{y^A{\leftarrow}N^A\} \triangleq (M_1^{C\supset B}\{\alpha^A{\leftarrow}N^A\}(M_2^C\{\alpha^A{\leftarrow}N^A\}))^B \\
(!M^B)^{[\![s]\!]B} & \{y^A{\leftarrow}N^A\} \triangleq (!M^B)^{[\![s]\!]B} \\
(M_1\langle v^B{:=}u, M_2\rangle)^{B\{v^A \leftarrow u\}} & \{y^A{\leftarrow}N^A\} \triangleq (M_1\{\alpha^A{\leftarrow}N^A\}\langle v^B{:=}u, M_2\{\alpha^A{\leftarrow}N^A\}\rangle)^{B\{v^A \leftarrow u\}} \\
(M^B +_{\mathrm{L}} t)^B & \{y^A{\leftarrow}N^A\} \triangleq (M^B\{\alpha^A{\leftarrow}N^A\} +_{\mathrm{L}} t\{\alpha^A \leftarrow \mathsf{w}(N^A)\})^B \\
(s +_{\mathrm{R}} M^B)^B & \{y^A{\leftarrow}N^A\} \triangleq (s\{\alpha^A \leftarrow \mathsf{w}(N^A)\} +_{\mathrm{R}} M^B\{\alpha^A{\leftarrow}N^A\})^B \\
([\alpha^B]M^B)^{\perp} & \{y^A{\leftarrow}N^A\} \triangleq ([\alpha^B](M^B\{\alpha^A{\leftarrow}N^A\}))^{\perp} \\
(\mu\alpha^B.M^{\perp})^B & \{y^A{\leftarrow}N^A\} \triangleq (\mu\alpha^B.(M^{\perp}\{\alpha^A{\leftarrow}N^A\}))^B
\end{array}$$

Note that substitution operates only on the immediate level: it does not affect superindices ($x^{[\![y^A]\!]A}\{y^A \leftarrow s\} = x^{[\![y^A]\!]A}$ and not $x^{[\![s]\!]A}$). Finally, truth variable substitution over formulas ($B\{y^A \leftarrow s^A\}$) is defined as:

$$\begin{array}{ll}
P & \{y^A \leftarrow s\} \triangleq P \\
\bot & \{y^A \leftarrow s\} \triangleq \bot \\
B \supset C & \{y^A \leftarrow s\} \triangleq B\{y^A \leftarrow s\} \supset C\{y^A \leftarrow s\} \\
[\![t]\!]B & \{y^A \leftarrow s\} \triangleq [\![t\{y^A \leftarrow s\}]\!]B\{y^A \leftarrow s\}
\end{array}$$

Validity variable substitution over formulae ($B\{v^A \leftarrow s^A\}$) is as expected; the case over proof witnesses ($t\{v^A \leftarrow s^A\}$) deserves mention only with regards to the following defining clauses:

$$\begin{array}{ll}
!t & \{v^A \leftarrow s\} \triangleq !(t\{v^A \leftarrow s\}) \\
t\langle w^B{:=}u, r\rangle & \{v^A \leftarrow s\} \triangleq t\{v^A \leftarrow s\}\langle w^B{:=}u\{v^A \leftarrow s\}, r\{v^A \leftarrow s\}\rangle \text{ if } w^B \neq v^A \\
t\langle v^A{:=}u, r\rangle & \{v^A \leftarrow s\} \triangleq t\langle v^A{:=}u, r\rangle \ (v^A \notin \mathsf{FVV}(r)) \\
r + t & \{v^A \leftarrow s\} \triangleq (r\{v^A \leftarrow s\}) + (t\{v^A \leftarrow s\})
\end{array}$$

The assumption that $v^A \notin \mathsf{FVV}(r)$ in the definition of $t\langle v^A{:=}u, r\rangle\{v^A \leftarrow s\}$ is based on the already mentioned variable convention. Validity variable substitution over terms ($M^C\{v^A \leftarrow N^A, t\}$) is defined as follows:

$$\begin{array}{ll}
x^B & \{v^A \leftarrow N^A, t\} \triangleq x^B \\
v^A & \{v^A \leftarrow N^A, t\} \triangleq N^A \\
w^B & \{v^A \leftarrow N^A, t\} \triangleq w^B \text{ if } w^B \neq v^A \\
(\lambda x^B.M^C)^{B \supset C} & \{v^A \leftarrow N^A, t\} \triangleq (\lambda x^B.(M^C\{v^A \leftarrow N^A, t\}))^{B \supset (C\{v^A \leftarrow t\})} \\
(M_1^{B \supset C} M_2^B)^C & \{v^A \leftarrow N^A, t\} \triangleq (M_1^{B \supset C}\{v^A \leftarrow N^A, t\}(M_2^B\{v^A \leftarrow N^A, t\}))^{C\{v^A \leftarrow t\}} \\
(!M^B)^{[\![s^B]\!]B} & \{v^A \leftarrow N^A, t\} \triangleq !(M^B\{v^A \leftarrow N^A, t\})^{([\![s^B]\!]B)\{v^A \leftarrow t\}} \\
M_2^C\langle v^A{:=}r, M_1\rangle & \{v^A \leftarrow N^A, t\} \triangleq M_2^C\langle v^A{:=}r, M_1\rangle \text{ (because } v^A \notin \mathsf{FVV}(M_1^{[\![r]\!]A})) \\
\multicolumn{2}{l}{(M_2^C\langle w^B{:=}r, M_1\rangle)^D\{v^A \leftarrow N^A, t\} \triangleq \begin{pmatrix} M_2^C\{v^A \leftarrow N^A, t\} \\ \langle w^B{:=}r\{v^A \leftarrow t\}, M_1\{v^A \leftarrow N^A, t\}\rangle \end{pmatrix}^{D\{v^A \leftarrow t\}}} \\
 & \qquad\qquad \text{if } w^B \neq v^A \text{ (where } D = C\{w^B \leftarrow r\}) \\
(M^B +_{\mathrm{L}} s)^B & \{v^A \leftarrow N^A, t\} \triangleq (M^B\{v^A \leftarrow N^A, t\} +_{\mathrm{L}} s\{v^A \leftarrow t\})^{B\{v^A \leftarrow t\}} \\
(s +_{\mathrm{R}} M_2^C)^C & \{v^A \leftarrow N^A, t\} \triangleq (s\{v^A \leftarrow t\} +_{\mathrm{R}} M_2^C\{v^A \leftarrow N^A, t\})^{C\{v^A \leftarrow t\}} \\
([\alpha^B]M^B)^\bot & \{v^A \leftarrow N^A, t\} \triangleq ([\alpha^B](M^B\{v^A \leftarrow N^A, t\}))^\bot \\
(\mu\alpha^B.M^\bot)^B & \{v^A \leftarrow N^A, t\} \triangleq (\mu\alpha^B.M^\bot\{v^A \leftarrow N^A, t\})^B
\end{array}$$

Structural substitution is a notion introduced in the work of Parigot [16]. It is written $M\{\!\!\{[\alpha^{A \supset B}](\bullet) \leftarrow [\beta^B](\bullet)N^A\}\!\!\}$ and consists of replacing in M all occurrences of subexpressions of the form $[\alpha^{A \supset B}]P$ for some P, with $[\beta^B]PN^A$. Structural substitution ($M\{\!\!\{[\alpha^{A \supset B}](\bullet) \leftarrow [\beta^B](\bullet)N^A\}\!\!\}$) is defined as follows:

$$\begin{array}{ll}
x^D & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq x^D \\
v^D & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq v^D \\
\lambda x^D.M^C & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq \lambda x^D.(M^C\{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\}) \\
M_1^{D \supset C} M_2^D & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq M_1^{D \supset C}\{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\}(M_2^D\{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\}) \\
!M^D & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq !M^D \\
M\langle v^D{:=}r, M'\rangle & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq M\{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\}\langle v^D{:=}r, M'\{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\}\rangle \\
M +_{\mathrm{L}} t & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq (M\{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\}) +_{\mathrm{L}} (t\{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)\,\mathsf{w}(N)\}\!\!\}) \\
s +_{\mathrm{R}} N & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq (s\{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)\,\mathsf{w}(N)\}\!\!\}) +_{\mathrm{R}} (N\{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\}) \\
[\alpha^{A \supset B}]M & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq [\beta^B]MN \\
[\gamma^D]M & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq [\gamma^D](M\{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\}) \text{ if } \gamma^D \neq \alpha^{A \supset B} \\
\mu\alpha^{A \supset B}.M & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq \mu\alpha^{A \supset B}.M \\
\mu\gamma^D.M & \{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\} \triangleq \mu\gamma^D.(M\{\!\!\{[\alpha](\bullet) \leftarrow [\beta](\bullet)N\}\!\!\}) \text{ if } \gamma^D \neq \alpha^{A \supset B}
\end{array}$$

$$\frac{}{\Theta;\Gamma,x^A;\Delta\vdash x^A\,|\,x^A}\;\textsf{T-Var}\qquad\frac{}{\Theta,v^A;\Gamma;\Delta\vdash v^A\,|\,v^A}\;\textsf{T-VarM}$$

$$\frac{\Theta;\Gamma,x^A;\Delta\vdash M^B\,|\,s}{\Theta;\Gamma;\Delta\vdash(\lambda x^A.M)^{A\supset B}\,|\,\lambda x^A.s}\;\textsf{T-}\supset\textsf{I}\qquad\frac{\Theta;\cdot;\cdot\vdash M^B\,|\,s\quad\Theta;\cdot;\cdot\vdash\ s\equiv t:B}{\Theta;\Gamma;\Delta\vdash(!M^B)^{\llbracket t\rrbracket B}\,|\,!t}\;\textsf{T-}\Box\textsf{I}$$

$$\frac{\Theta;\Gamma;\Delta\vdash M^{A\supset B}\,|\,s\quad\Theta;\Gamma;\Delta\vdash N^A\,|\,t}{\Theta;\Gamma;\Delta\vdash(MN)^B\,|\,s\cdot t}\;\textsf{T-}\supset\textsf{E}$$

$$\frac{\Theta;\Gamma;\Delta\vdash M^{\llbracket r\rrbracket A}\,|\,s\quad\Theta,v^A;\Gamma;\Delta\vdash N^C\,|\,t}{\Theta;\Gamma;\Delta\vdash(N^C\langle v^A{:=}r,M\rangle)^{C\{v^A\leftarrow r\}}\,|\,t\langle v^A{:=}r,s\rangle}\;\textsf{T-}\Box\textsf{E}$$

$$\frac{\Theta;\Gamma;\Delta\vdash M^A\,|\,s}{\Theta;\Gamma;\Delta\vdash(M+_{\mathrm{L}}t)^A\,|\,s+t}\;\textsf{T-PlusL}\qquad\frac{\Theta;\Gamma;\Delta\vdash N^B\,|\,t}{\Theta;\Gamma;\Delta\vdash(s+_{\mathrm{R}}N)^B\,|\,s+t}\;\textsf{T-PlusR}$$

$$\frac{\Theta;\Gamma;\Delta,\alpha^A\vdash M^A\,|\,s}{\Theta;\Gamma;\Delta,\alpha^A\vdash([\alpha^A]M)^\perp\,|\,[\alpha^A]s}\;\textsf{T-Name}\qquad\frac{\Theta;\Gamma;\Delta,\alpha^A\vdash M^\perp\,|\,s}{\Theta;\Gamma;\Delta\vdash(\mu\alpha^A.M)^A\,|\,\mu\alpha^A.s}\;\textsf{T-NAbs}$$

FIGURE 5. Typing rules for λ^{LP}

Structural substitution over proof witnesses is defined analogously (ignoring the additional proof witness, replacing M and N by s and t, $+_{\mathrm{L}}$ and $+_{\mathrm{R}}$ by $+$, and term application by $\cdot$).

4.2. The Typing Rules

The typing rules (Fig. 5) are derived by assigning terms to the inference rules of HLP. Additionally, these typing rules are syntactically driven, as the last symbol used to construct the term in the succedent of each rule is different to the others. Finally, note that the term in the succedent of each rule contains (as subterms) all the terms used in the premises of that same rule. As a result, every well-typed term encodes a derivation in HLP (modulo the equivalence rules, which are not encoded), and every HLP-derivation can be encoded by a term.

We now present a series of metatheoretical results of which we shall make use in our proof of Subject Reduction (Proposition 4.11).

Lemma 4.2 (Inversion). *If* $\rhd_{\mathsf{HLP}}\Theta;\Gamma;\Delta\vdash N^F\,|\,u$, *then:*

- *if* $N^F=x^A$, *then* $x^A\in\Gamma$, $u=x^A$ *and* $F=A$;
- *if* $N^F=v^A$, *then* $v^A\in\Theta$, $u=v^A$ *and* $F=A$;
- *if* $N^F=(\lambda x^A.M^B)^{A\supset B}$, *then* $\Theta;\Gamma,x^A;\Delta\vdash M^B\,|\,s$ *is derivable for some* s, *and* $u=\lambda x^A.s$ *and* $F=A\supset B$;
- *if* $N^F=(M_1^{A\supset B}M_2^A)^B$, *then both* $\Theta;\Gamma;\Delta\vdash M_1^{A\supset B}\,|\,s$ *and* $\Theta;\Gamma;\Delta\vdash M_2^A\,|\,t$ *are derivable for some* s *and* t, *and* $u=s\cdot t$ *and* $F=B$;
- *if* $N^F=(!M^A)^{\llbracket t\rrbracket A}$, *then* $\exists s$ *s.t.* $\Theta;\cdot;\cdot\vdash M^A\,|\,s$ *is derivable, and* $u=\,!t$, $\Theta;\cdot;\cdot\vdash\ s\equiv t:A$ *and* $F=\llbracket t\rrbracket A$;
- *if* $N^F=(M_2^B\langle v^A{:=}r,M_1\rangle)^{B\{v^A\leftarrow r^A\}}$, *then both* $\Theta;\Gamma;\Delta\vdash M_1^{\llbracket r\rrbracket A}\,|\,s$ *and* $\Theta,v^A;\Gamma;\Delta\vdash M_2^B\,|\,t$ *are derivable for some* s *and* t, *and* $u=t\langle v^A{:=}r,s\rangle$ *and* $F=B\{v^A\leftarrow r^A\}$;

- *if* $N^F = ([\alpha^A]M^A)^\perp$, *then* $\exists\ \Delta', s$ *s.t.* $\Delta = \Delta', \alpha^A$, $\Theta; \Gamma; \Delta', \alpha^A \vdash M^A \,|\, s$ *is derivable, and* $u = [\alpha^A]s$ *and* $F = \perp$;
- *if* $N^F = (\mu\alpha^A.M^\perp)^A$, *then* $\Theta; \Gamma; \Delta, \alpha^A \vdash M^\perp \,|\, s$ *is derivable for some* s, *and* $u = \mu\alpha^A.s$ *and* $F = A$;
- *if* $N^F = (M^A +_{\mathrm{L}} t)^A$, *then* $\Theta; \Gamma; \Delta \vdash M^A \,|\, s$ *is derivable for some* s, *and* $u = s + t$ *and* $F = A$;
- *if* $N^F = (s +_{\mathrm{R}} M^B)^B$, *then* $\Theta; \Gamma; \Delta \vdash M^B \,|\, t$ *is derivable for some* t, *and* $u = s + t$ *and* $F = B$.

Proof. By structural induction on N. One and only one rule applies to each of the cases, and the only rule which can modify the witness is $\mathsf{T}\text{-}\Box\mathsf{I}$, which replaces it by an equivalent proof witness for the same type under the same contexts. □

Lemma 4.3 (Truth Variable Substitution). *If* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma, y^A; \Delta \vdash M^B \,|\, s$ *and* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta \vdash N^A \,|\, t$ *are derivable, then* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta \vdash M\{y^A \leftarrow N\}^B \,|\, s\{y^A \leftarrow t\}$.

Lemma 4.4 (Validity Variable Substitution).

1. *If* $\rhd_{\mathit{HLP}}\, \Theta, v^A; \Gamma; \Delta \vdash M^B \,|\, s$ *and* $\rhd_{\mathit{HLP}}\, \Theta; \cdot; \cdot \vdash N^A \,|\, t$, *then* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta \vdash M\{v^A \leftarrow N^A, t\}^{B\{v^A \leftarrow t\}} \,|\, s\{v^A \leftarrow t\}$.
2. *If* $\rhd_{\mathit{HLP}}\, \Theta, v^A; \Gamma; \Delta \vdash\ s \equiv r : B$ *and* $\rhd_{\mathit{HLP}}\, \Theta; \cdot; \cdot \vdash N^A \,|\, t$, *then* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta \vdash\ s\{v^A \leftarrow t\} \equiv r\{v^A \leftarrow t\} : B\{v^A \leftarrow t\}$.

Lemma 4.5 (Validity Variable Substitution with Proof Witness Equivalence). *If* $\rhd_{\mathit{HLP}}\, \Theta, v^A; \Gamma; \Delta \vdash M^B \,|\, s$, $\rhd_{\mathit{HLP}}\, \Theta; \cdot; \cdot \vdash N^A \,|\, r$ *and* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta \vdash\ r \equiv t : A$, *then there exists* s' *such that both* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta \vdash M^B\{v^A \leftarrow N^A, t\}^{B\{v^A \leftarrow t\}} \,|\, s'$ *and* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta \vdash\ s' \equiv s\{v^A \leftarrow t\} : B\{v^A \leftarrow t\}$.

Lemma 4.6 (Falsehood Variable Renaming). *If* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta, \alpha^A, \beta^A \vdash M^B \,|\, s$, *then* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta, \beta^A \vdash M\{\alpha^A \leftarrow \beta^A\}^B \,|\, s\{\alpha^A \leftarrow \beta^A\}$.

Lemma 4.7 (Structural Substitution). *If* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta, \alpha^{A \supset B} \vdash M^F \,|\, s$ *and* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta \vdash N^A \,|\, t$, *then also* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta, \beta^B \vdash M\big\{[\alpha^{A \supset B}](\bullet) \leftarrow [\beta^B](\bullet) N^A\big\}^F \,|\, s\big\{[\alpha^{A \supset B}](\bullet) \leftarrow [\beta^B](\bullet) t\big\}$.

Corollary 4.8. *If* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta, \alpha^{A \supset B} \vdash M^\perp \,|\, s$ *and* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta \vdash N^A \,|\, t$, *then* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta \vdash (\mu\beta^B.M^\perp\big\{[\alpha^{A \supset B}](\bullet) \leftarrow [\beta^B](\bullet) N^A\big\})^B \,|\, \mu\beta^B.s\big\{[\alpha^{A \supset B}](\bullet) \leftarrow [\beta^B](\bullet) t\big\}$.

Lemma 4.9. *If* $\rhd_{\mathit{HLP}}\, \Theta; \Gamma; \Delta \vdash M^A \,|\, s$, *then* $\mathit{FVT}(s) \subseteq \mathit{FVT}(M^A)$ *and* $\mathit{FVF}(s) \subseteq \mathit{FVF}(M^A)$.

4.3. The Reduction Rules

Reduction in λ^{LP} is defined as the compatible closure of the following reduction rules. The first set of rules arises from the principal cases of normalisation of derivations and are referred to as the *principal rules*:

$$\begin{array}{lrl}
\beta : & (\lambda x^A.M^B)N^A & \rightarrow M^B\{x^A \leftarrow N^A\} \\
\gamma : & M^B\langle v^A{:=}r,\ !N^A\rangle & \rightarrow M^B\{v^A \leftarrow N^A, r\}, \text{ if } \mathsf{FVT}(N^A) = \mathsf{FVF}(N^A) = \emptyset \\
\mu : & [\beta^A]\mu\alpha^A.M^\perp & \rightarrow M^\perp\{\alpha^A \leftarrow \beta^A\} \\
\zeta : & (\mu\alpha^{A \supset B}.M^\perp)N^A & \rightarrow \mu\beta^B.M^\perp\big\{[\alpha^{A \supset B}](\bullet) \leftarrow [\beta^B](\bullet) N^A\big\} \\
\theta : & \mu\alpha^A.[\alpha^A]M^A & \rightarrow M^A, \text{ if } \alpha^A \notin \mathsf{FVF}(M^A)
\end{array}$$

The second set of rules, the *permutative rules*, arise from the permutative cases:

$$\begin{array}{lll}
\psi_L : & (M^{A\supset B} +_{\mathrm{L}} t)^{A\supset B} N^A & \to (M^{A\supset B} N^A)^B +_{\mathrm{L}} t \\
\psi_R : & (s +_{\mathrm{R}} M^{A\supset B})^{A\supset B} N^A & \to s +_{\mathrm{R}} (M^{A\supset B} N^A)^B \\
\phi_L : & N^B \langle v^A{:=}r, (M^{[\![r]\!]A} +_{\mathrm{L}} t)\rangle & \to (N^B\langle v^A{:=}r, M\rangle)^{B\{v^A \leftarrow r^A\}} +_{\mathrm{L}} t \\
\phi_R : & N^B \langle v^A{:=}r, (s +_{\mathrm{R}} M^{[\![r]\!]A})\rangle & \to s +_{\mathrm{R}} (N^B\langle v^A{:=}r, M\rangle)^{B\{v^A \leftarrow r^A\}} \\
\chi_L : & [\beta^A](M^A +_{\mathrm{L}} t)^A & \to ([\beta^A]M^A)^\perp +_{\mathrm{L}} t \\
\chi_R : & [\beta^B](s +_{\mathrm{R}} N^B)^B & \to s +_{\mathrm{R}} ([\beta^B]N^B)^\perp \\
\iota_L : & \mu\alpha^A.(M^\perp +_{\mathrm{L}} t)^\perp & \to (\mu\alpha^A.M^\perp) +_{\mathrm{L}} t \text{ if } \alpha^A \notin \mathsf{FVF}(t) \\
\iota_R : & \mu\alpha^A.(s +_{\mathrm{R}} N^\perp)^\perp & \to s +_{\mathrm{R}} (\mu\alpha^A.N^\perp) \text{ if } \alpha^A \notin \mathsf{FVF}(s)
\end{array}$$

The restrictions to rules γ, θ, ι_L and ι_R prevent the creation of free variables upon reduction. Bound variables may be renamed before reduction to avoid capture.

Lemma 4.10. *If $\rhd_{\mathit{HLP}}\, \Theta;\Gamma;\Delta \vdash M^D \,|\, s$ and $M^D \to N^D$ by reducing a redex at the root of M^D, then $\rhd_{\mathit{HLP}}\, \Theta;\Gamma;\Delta \vdash N^D \,|\, s'$ for some witness s' such that $\Theta;\Gamma;\Delta \vdash\ s \equiv s' : D$.*

Proof. We must consider which reduction rule was used.

- $\beta : M = (\lambda x^A.M_1^B)M_2^A,\ N = M_1^B\{x^A \leftarrow M_2^A\}$ and, by Inversion Lemma (used twice), $D = B$, $s = (\lambda x^A.t) \cdot t'$ and both $\Theta;\Gamma;\Delta \vdash M_2^A \,|\, t'$ and $\Theta;\Gamma, x^A;\Delta \vdash M_1^B \,|\, t$ are derivable. By Lemma 4.3, we can derive $\Theta;\Gamma;\Delta \vdash M_1^B\{x^A \leftarrow M_2^A\}^B \,|\, t\{x^A \leftarrow t'\}$. And, by Eq-β, $\Theta;\Gamma;\Delta \vdash\ (\lambda x^A.t)\cdot t' \equiv t\{x^A \leftarrow t'\} : B$.
- γ : in this case $M = (M_1^B\langle v^A{:=}r, !M_2^A\rangle)^{B\{v^A\leftarrow r\}},\ N = (M_1^B\{v^A \leftarrow M_2^A, r\})$ ${}^{B\{v^A\leftarrow r\}}$ and, by Inversion Lemma (twice),$D = B\{v^A \leftarrow r\}$, $s = t\langle v^A{:=}r, !r\rangle$ and there is a witness r' such that $\Theta;\cdot;\cdot \vdash\ r' \equiv r : A$ and both $\Theta;\cdot;\cdot \vdash M_2^A \,|\, r'$ and $\Theta, v^A;\Gamma;\Delta \vdash M_1^B \,|\, t$ are derivable. By Weakening and Lemma 4.5, we can derive $\Theta;\Gamma;\Delta \vdash\ M_1^B\{v^A \leftarrow M_2^A, r\}^{B\{v^A\leftarrow r\}} \,|\, s'$ and $\Theta;\Gamma;\Delta \vdash\ s' \equiv t\{v^A \leftarrow r\} : B\{v^A \leftarrow r\}$ for some witness s' - and, by Eq-Symm, we derive $\Theta;\Gamma;\Delta \vdash\ t\{v^A \leftarrow r\} \equiv s' : B\{v^A \leftarrow r\}$. By Eq-γ, we can derive $\Theta;\Gamma;\Delta \vdash\ s \equiv t\{v^A \leftarrow r\} : B\{v^A \leftarrow r\}$. And finally, by Eq-Trans, $\Theta;\Gamma;\Delta \vdash s \equiv s' : B\{v^A \leftarrow r\}$.
- $\mu : M = [\beta^A]\mu\alpha^A.M_1^\perp,\ N = M_1^\perp\{\alpha^A \leftarrow \beta^A\}$ and, by Inversion Lemma (twice), $s = [\beta^A]\mu\alpha^A.t$, $D = \perp$, $\Delta = \Delta', \beta^A$ and both $\Theta;\Gamma;\Delta',\beta^A$ $\vdash (\mu\alpha^A.M_1^\perp)^A \,|\, \mu\alpha^A.t$ and $\Theta;\Gamma;\Delta',\alpha^A,\beta^A \vdash M_1^\perp \,|\, t$ are derivable. Then, by Lemma 4.6, $\Theta;\Gamma;\Delta',\beta^A \vdash M_1^\perp\{\alpha^A \leftarrow \beta^A\}^\perp \,|\, t\{\alpha^A \leftarrow \beta^A\}$ is also derivable. And, by Eq-μ, $\Theta;\Gamma;\Delta',\beta^A \vdash\ [\beta^A]\mu\alpha^A.t \equiv t\{\alpha^A \leftarrow \beta^A\} : \perp$.
- $\zeta : M = (\mu\alpha^{A\supset B}.M_1^\perp)^{A\supset B} M_2^A,\ N = \mu\beta^B.M_1^\perp\{\![\alpha^{A\supset B}](\bullet)\leftarrow[\beta^B](\bullet)M_2^A\}\!\}$ and, by Inversion Lemma (twice), $D = B$, $s = (\mu\alpha^{A\supset B}.s_1)\cdot s_2$ and the judgements $\Theta;\Gamma;\Delta \vdash M_2^A \,|\, s_2$, $\Theta;\Gamma;\Delta \vdash (\mu\alpha^{A\supset B}.M_1)^{A\supset B} \,|\, \mu\alpha^{A\supset B}.s_1$ and $\Theta;\Gamma;\Delta,\alpha^{A\supset B} \vdash M_1^\perp \,|\, s_1$ are derivable. By Corollary 4.8, we can derive $\Theta;\Gamma;\Delta\ \ \vdash\ (\mu\beta^B.M_1^\perp\{\![\alpha^{A\supset B}](\bullet)\leftarrow[\beta^B](\bullet)M_2^A\}\!\})^B \,|\, mut\beta B s_1\{\![\alpha^{A\supset B}](\bullet)\leftarrow[\beta^B](\bullet)s_2\}\!\}$. And by Eq-ζ, $\Theta;\Gamma;\Delta \vdash\ (\mu\alpha^{A\supset B}.s_1)\cdot s_2 \equiv s_1\{\![\alpha^{A\supset B}](\bullet)\leftarrow[\beta^B](\bullet)s_2\}\!\} : B$.
- $\theta : M = \mu\alpha^A.[\alpha^A]M_1^A,\ N = M_1^A$ and $\alpha^A \notin \mathsf{FVF}(M^A)$. By Inversion Lemma (twice), $D = A$, $s = \mu\alpha^A.[\alpha^A]t$ and both $\Theta;\Gamma;\Delta,\alpha^A \vdash ([\alpha^A]M_1^A)^\perp \,|\, [\alpha^A]t$ and $\Theta;\Gamma;\Delta,\alpha^A \vdash\ M_1^A \,|\, t$ are derivable. Since $\alpha^A \notin \mathsf{FVF}(M_1^A)$ - and, by

Lemma 4.9, $\alpha^A \notin \mathsf{FVF}(t)$ -, then $\Theta;\Gamma;\Delta \vdash M_1^A \,|\, t$ is derivable and, by Eq-Θ, $\Theta;\Gamma;\Delta \vdash\ \mu\alpha^A.[\alpha^A]t \equiv t\colon A$.

- ψ_L : $M = (M_1^{A\supset B} +_{\mathrm{L}} s_2)^{A\supset B} M_3^A$ and $N = (M_1^{A\supset B} M_3^A)^B +_{\mathrm{L}} s_2$. By Inversion Lemma (twice), $D = B$, $s = (s_1 + s_2)\cdot s_3$, and the judgements $\Theta;\Gamma;\Delta \vdash M_1^{A\supset B} \,|\, s_1$, $\Theta;\Gamma;\Delta \vdash M_3^A \,|\, s_3$ and $\Theta;\Gamma;\Delta \vdash (M_1 +_{\mathrm{L}} s_2)^{A\supset B} \,|\, s_1 + s_2$ are derivable. By T- $\supset$ E, we can derive $\Theta;\Gamma;\Delta \vdash (M_1^{A\supset B} M_3^A)^B \,|\, s_1 \cdot s_3$. By T-PlusL, we obtain $\Theta;\Gamma;\Delta \vdash (M_1^{A\supset B} M_3^A) +_{\mathrm{L}} s_2^B \,|\, (s_1 \cdot s_3) + s_2$. And, by Eq-$\psi_L$, $\Theta;\Gamma;\Delta \vdash\ (s_1 + s_2)\cdot s_3 \equiv (s_1 \cdot s_3) + s_2\colon B$.
- ψ_R : $M = (s_1 +_{\mathrm{R}} M_2^{A\supset B})^{A\supset B} M_3^A$ and $N = s_1 +_{\mathrm{R}} (M_2^{A\supset B} M_3^A)^B$. This case is analogous to the previous one.
- ϕ_L : (ϕ_R is similar and hence omitted) $M = L^B\langle v^A{:=}r, (M_1^{[\![r]\!]A} +_{\mathrm{L}} s_2)\rangle$ and $N = (L^B\langle v^A{:=}r, M_1\rangle)^{B\{v^A \leftarrow r^A\}} +_{\mathrm{L}} s_2$. By Inversion Lemma (twice), $D = B\{v^A \leftarrow r\}$, $s = t\langle v^A{:=}r, (s_1 + s_2)\rangle$, and the judgements $\Theta, v^A;\Gamma;\Delta \vdash L^B \,|\, t$, $\Theta;\Gamma, v^A;\Delta \vdash (M_1^{[\![r]\!]A} +_{\mathrm{L}} s_2)^{[\![r]\!]A} \,|\, s_1 + s_2$ and $\Theta;\Gamma;\Delta \vdash M_1^{[\![r]\!]A} \,|\, s_1$ are derivable. By T-$\Box$E, $\Theta;\Gamma;\Delta \vdash (L^B\langle v^A{:=}r, M_1\rangle)^{B\{v^A \leftarrow r\}} \,|\, t\langle v^A{:=}r, s_1\rangle$. By T-PlusL, the judgment $\Theta;\Gamma;\Delta \vdash\ N^{B\{v^A \leftarrow r\}} \,|\, (t\langle v^A{:=}r, s_1\rangle) + s_2$ is derivable. And, by Eq-ϕ_L, so is $\Theta;\Gamma;\Delta \vdash\ t\langle v^A{:=}r, (s_1 + s_2)\rangle \equiv (t\langle v^A{:=}r, s_1\rangle) + s_2\colon B\{v^A \leftarrow r\}$.
- χ_L : (χ_R is similar and hence omitted) $M = [\beta^A](M_1^A +_{\mathrm{L}} s_2)^A$ and $N = ([\beta^A]M_1^A)^\perp +_{\mathrm{L}} s_2$. By Inversion Lemma (twice), $D = \perp$, $s = [\beta^A]s_1 + s_2$, $\Delta = \Delta', \beta^A$ and the judgements $\Theta;\Gamma;\Delta',\beta^A \vdash\ (M_1^A +_{\mathrm{L}} s_2)^A \,|\, s_1 + s_2$ and $\Theta;\Gamma;\Delta',\beta^A \vdash M_1^A \,|\, s_1$ are derivable. By T-Name, we can derive $\Theta;\Gamma;\Delta',\beta^A \vdash ([\beta^A]M_1^A)^\perp \,|\, [\beta^A]s_1$. By T-PlusL, we obtain $\Theta;\Gamma;\Delta',\beta^A \vdash ([\beta^A]M_1^A)^\perp +_{\mathrm{L}} s_2^\perp \,|\, ([\beta^A]s_1) + s_2$. And finally, by Eq-$\chi_L$, $\Theta;\Gamma;\Delta',\beta^A \vdash\ [\beta^A]s_1 + s_2 \equiv ([\beta^A]s_1) + s_2\colon \perp$.
- ι_L : $M = \mu\alpha^A.(M_1^\perp +_{\mathrm{L}} s_2)^\perp$ and $N = (\mu\alpha^A.M_1^\perp)^A +_{\mathrm{L}} s_2$. By Inversion Lemma (twice), $D = A$, $s = \mu\alpha^A.s_1 + s_2$, and the judgements $\Theta;\Gamma;\Delta',\alpha^A \vdash (M_1^\perp +_{\mathrm{L}} s_2)^\perp \,|\, s_1 + s_2$ and $\Theta;\Gamma;\Delta',\alpha^A \vdash M_1^\perp \,|\, s_1$ are derivable. By T-NAbs, we can derive $\Theta;\Gamma;\Delta \vdash\ (\mu\alpha^A.M_1^\perp)^A \,|\, \mu\alpha^A.s_1$. By T-PlusL, we obtain $\Theta;\Gamma;\Delta \vdash (\mu\alpha^A.M_1^\perp)^A +_{\mathrm{L}} s_2^A \,|\, (\mu\alpha^A.s_1) + s_2$. And finally, by Eq-$\chi_L$, $\Theta;\Gamma;\Delta \vdash\ \mu\alpha^A.s_1 + s_2 \equiv (\mu\alpha^A.s_1) + s_2\colon A$.
- ι_R : This case is analogous to the previous one.

□

The following result is proved by induction on the derivation of $\Theta;\Gamma;\Delta \vdash M^B|s$ and resorting to 4.10 and the congruence schemes for proof witness equivalence.

Proposition 4.11 (Subject Reduction). *If* $\rhd_{\mathit{HLP}}\Theta;\Gamma;\Delta \vdash M^B|s$ *and* $M^B \to N^B$, *then* $\rhd_{\mathit{HLP}}\,\Theta;\Gamma;\Delta \vdash N^B \,|\, s'$ *for some witness* s' *such that* $\Theta;\Gamma;\Delta \vdash\ s \equiv s'\colon B$.

Corollary 4.12. *If* $\rhd_{\mathit{HLP}}\,\Theta;\Gamma;\Delta \vdash (!M^B)^A|t$ *and* $M^B \to N^B$, *then* $\rhd_{\mathit{HLP}}\,\Theta;\Gamma;\Delta \vdash (!N^B)^A \,|\, t$.

Proof. By the Inversion Lemma, $A = [\![r]\!]B$, $t = !r$ for some proof witness r, and there is an s such that both $\Theta;\cdot;\cdot \vdash M^B|s$ and $\Theta;\cdot;\cdot \vdash s \equiv r : B$ are derivable. By Proposition 4.11, there is an s' such that both $\Theta;\cdot;\cdot \vdash N^B|s'$ and

$$\frac{}{x^A : \Gamma, x^A \vdash A, \Delta}\ \mathsf{Ax} \qquad \frac{}{\texttt{unit} : \Gamma \vdash \mathbf{1}, \Delta}\ \mathsf{Unit}$$

$$\frac{M : \Gamma \vdash B, \Delta}{\lambda x^A.M : \Gamma \setminus \{x^A\} \vdash A \supset B, \Delta}\ {\supset}\mathsf{I} \qquad \frac{M : \Gamma \vdash A \supset B, \Delta \quad N : \Gamma \vdash A, \Delta}{MN : \Gamma \vdash B, \Delta}\ {\supset}\mathsf{E}$$

$$\frac{M : \Gamma \vdash A, \Delta}{[\alpha^A]M : \Gamma \vdash \Delta, \alpha^A}\ \mu_1 \qquad \frac{M : \Gamma \vdash \Delta, \alpha^A}{\mu\alpha^A.M : \Gamma \vdash A, \Delta}\ \mu_2$$

$$\begin{array}{llcl}
R_1 : & (\lambda x^A.M)N & \rightarrow & M\{x^A \leftarrow N\} \\
R_2 : & (\mu\alpha^{A\supset B}.M)N & \rightarrow & \mu\beta^B.M\{[\alpha^{A\supset B}](\bullet) \leftarrow [\beta^B](\bullet)N\} \\
S_1 : & [\beta^A]\mu\alpha^A.M & \rightarrow & M\{\alpha^A \leftarrow \beta^A\} \\
S_2 : & \mu\alpha^A.[\alpha^A]M & \rightarrow & M \text{ if } \alpha^A \notin \mathsf{FVF}(M)
\end{array}$$

Figure 6. Inference schemes and reduction rules of $\lambda\mu^{\mathbf{1}}$

$\Theta; \cdot; \cdot \vdash s' \equiv s : B$ are derivable. By $\mathsf{Eq\text{-}Trans}$, $\Theta; \cdot; \cdot \vdash s' \equiv r : B$ is also derivable. And, by $\mathsf{T\text{-}\Box I}$, so is $\Theta; \Gamma; \Delta \vdash (!N^B)^{[\![r]\!]B} \mid !r$. □

5. Strong Normalisation

We prove strong normalisation (SN) of term reduction by mapping λ^{LP}-terms into terms of Parigot's $\lambda\mu$-calculus with unit type ($\lambda\mu^{\mathbf{1}}$). A proof of SN of the $\lambda\mu$-calculus can be found in [17]. Since we are working with propositional logic, we will only use the pure (propositional) $\lambda\mu$-calculus, rather than its second-order extension.

$\lambda\mu^{\mathbf{1}}$ inherits the inference schemes (top of Fig. 6) and reduction rules from $\lambda\mu$ along with all its properties, since `unit` is not involved in the reduction. $\lambda\mu^{\mathbf{1}}$-judgements take the form $M : \Gamma \vdash \Delta$, with M a $\lambda\mu^{\mathbf{1}}$-term, Γ a truth context and Δ a falsehood context. For clarity, we adapt Parigot's notation replacing $\rightarrow$ by $\supset$ and A^x (resp. A^α) as x^A (resp. α^A). Also, we include $\perp$ as a formula or type since it simplifies our mapping and assume that $\perp, \Delta = \Delta$. Finally, we also assume that application is left-associative, dropping the parentheses where it is safe. The reduction rules of $\lambda\mu^{\mathbf{1}}$ are given in Fig. 6 (bottom) and correspond, respectively, to rules β, ζ, μ and θ in λ^{LP}.

As mentioned above, in order to prove SN of λ^{LP}, we introduce a mapping $\llparenthesis \cdot \rrparenthesis$, which associates types (formulas) and terms (proofs) in λ^{LP} with types and terms in $\lambda\mu^{\mathbf{1}}$. The modal type $[\![s]\!]A$ is mapped to a functional type whose domain is the unit type $\mathbf{1}$ and whose co-domain is the mapping of A.

$$\begin{array}{rlrl}
\llparenthesis P \rrparenthesis & \triangleq P & \llparenthesis \cdot \rrparenthesis & \triangleq \cdot \\
\llparenthesis \perp \rrparenthesis & \triangleq \perp & \llparenthesis \Theta, v^A \rrparenthesis & \triangleq \llparenthesis \Theta \rrparenthesis, x_v^{\mathbf{1} \supset \llparenthesis A \rrparenthesis} \\
\llparenthesis A \supset B \rrparenthesis & \triangleq \llparenthesis A \rrparenthesis \supset \llparenthesis B \rrparenthesis & \llparenthesis \Gamma, x^A \rrparenthesis & \triangleq \llparenthesis \Gamma \rrparenthesis, x^{\llparenthesis A \rrparenthesis} \\
\llparenthesis [\![s]\!]A \rrparenthesis & \triangleq \mathbf{1} \supset \llparenthesis A \rrparenthesis & \llparenthesis \Delta, \alpha^A \rrparenthesis & \triangleq \llparenthesis \Delta \rrparenthesis, \alpha^{\llparenthesis A \rrparenthesis}
\end{array}$$

Since $\lambda\mu^{\mathbf{1}}$ has truth and falsehood variables but not validity variables, the mapping of validity variables will rely on a new set of truth variables in $\lambda\mu^{\mathbf{1}}$.

$$
\begin{aligned}
\llparenthesis x^{A} \rrparenthesis &\triangleq x^{\llparenthesis A \rrparenthesis}\\
\llparenthesis v^{A} \rrparenthesis &\triangleq (x_{v}^{\mathbf{1}\supset\llparenthesis A \rrparenthesis})\mathtt{unit}\\
\llparenthesis (M^{A\supset B} N^{B})^{B} \rrparenthesis &\triangleq \llparenthesis M^{A\supset B} \rrparenthesis \llparenthesis N^{B} \rrparenthesis\\
\llparenthesis ([\alpha^{A}]M^{A})^{\perp} \rrparenthesis &\triangleq [\alpha^{\llparenthesis A \rrparenthesis}]\llparenthesis M^{A} \rrparenthesis\\
\llparenthesis (\mu\alpha^{A}.M^{\perp})^{A} \rrparenthesis &\triangleq \mu\alpha^{\llparenthesis A \rrparenthesis}.\llparenthesis M^{\perp} \rrparenthesis\\
\llparenthesis (!M^{A})^{[\![s]\!]A} \rrparenthesis &\triangleq \lambda x^{\mathbf{1}}.\llparenthesis M^{A} \rrparenthesis \text{ with } x^{\mathbf{1}} \text{ a fresh variable.}\\
\llparenthesis (N^{B}\langle v^{A}{:=}r, M^{[\![r]\!]A}\rangle)^{B\{v^{A}\leftarrow r\}} \rrparenthesis &\triangleq (\lambda x_{v}^{\mathbf{1}\supset\llparenthesis A \rrparenthesis}.\llparenthesis N^{B} \rrparenthesis)\llparenthesis M^{[\![r]\!]A} \rrparenthesis\\
\llparenthesis (M^{A} +_{\mathrm{L}} t)^{A} \rrparenthesis &\triangleq \llparenthesis M^{A} \rrparenthesis\\
\llparenthesis (s +_{\mathrm{R}} M^{A})^{A} \rrparenthesis &\triangleq \llparenthesis M^{A} \rrparenthesis
\end{aligned}
$$

Note that the truth $\lambda\mu^{\mathbf{1}}$-variables which appear in the translations of different validity λ^{LP}-variables are different from each other, and from the translations of all truth λ^{LP}-variables.

The following result is proved by by induction on the derivation of $\Theta;\Gamma;\Delta \vdash M^{A} \,|\, s$ and noting that $\llparenthesis C\{v^{A} \leftarrow r\} \rrparenthesis = \llparenthesis C \rrparenthesis$ for every formula C, validity variable v^{A} and proof witness r.

Lemma 5.1. *If $\rhd_{\lambda^{LP}} \Theta;\Gamma;\Delta \vdash M^{A} \,|\, s$, then $\llparenthesis M \rrparenthesis : \llparenthesis \Theta \rrparenthesis \cup \llparenthesis \Gamma \rrparenthesis \vdash \llparenthesis A \rrparenthesis, \llparenthesis \Delta \rrparenthesis$ is derivable in $\lambda\mu^{1}$.*

The mapping preserves substitution of truth variables, renaming of falsehood variables and even structural substitution, as may be proved by structural induction on M:

Lemma 5.2. *For all λ^{LP}-terms M, N, for every truth variable x^{A}: $\llparenthesis M \rrparenthesis\{x^{\llparenthesis A \rrparenthesis} \leftarrow \llparenthesis N \rrparenthesis\} = \llparenthesis M\{x^{A} \leftarrow N\} \rrparenthesis$.*

Lemma 5.3. *For every λ^{LP}-term M, for all falsehood variables α^{A}, β^{A}: $\llparenthesis M \rrparenthesis$ $\{\alpha^{\llparenthesis A \rrparenthesis} \leftarrow \beta^{\llparenthesis A \rrparenthesis}\} = \llparenthesis M\{\alpha^{A} \leftarrow \beta^{A}\} \rrparenthesis$.*

Lemma 5.4. *For all λ^{LP}-terms M, N^{A}, for all falsehood variables $\alpha^{A\supset B}, \beta^{B}$: $\llparenthesis M \rrparenthesis \big\{[\alpha^{\llparenthesis A\supset B \rrparenthesis}](\bullet) \leftarrow [\beta^{\llparenthesis B \rrparenthesis}](\bullet)\llparenthesis N^{A} \rrparenthesis\big\} = \llparenthesis M\big\{[\alpha^{A\supset B}](\bullet) \leftarrow [\beta^{B}](\bullet)N^{A}\big\} \rrparenthesis$.*

The same cannot be said for substitution of validity variables however. For instance, if $M = v^{A}$, then $\llparenthesis M \rrparenthesis\{x_{v}^{\mathbf{1}\supset\llparenthesis A \rrparenthesis} \leftarrow \llparenthesis N \rrparenthesis\} = ((x_{v}^{\mathbf{1}\supset\llparenthesis A \rrparenthesis})\mathtt{unit})\{x_{v}^{\mathbf{1}\supset\llparenthesis A \rrparenthesis} \leftarrow \llparenthesis N \rrparenthesis\} = \llparenthesis N \rrparenthesis\mathtt{unit}$, which is clearly not the same as $\llparenthesis M \rrparenthesis\{v^{A} \leftarrow N, \mathsf{w}(N)\} = \llparenthesis N \rrparenthesis$. In the case of substitution of validity variables we have the following weaker result, which can also be verified by induction on M.

Lemma 5.5. *For all λ^{LP}-terms M, N, for every validity variable v^{A} and every truth variable $y^{\mathbf{1}} \notin \mathsf{FVT}(\llparenthesis N \rrparenthesis)$: $\llparenthesis M \rrparenthesis\{x_{v}^{\mathbf{1}\supset\llparenthesis A \rrparenthesis} \leftarrow \lambda y^{\mathbf{1}}.\llparenthesis N \rrparenthesis\} \twoheadrightarrow_{R_1} \llparenthesis M\{v^{A} \leftarrow \}N, \mathsf{w}(N) \rrparenthesis$, where $\twoheadrightarrow_{R_1}$ is the reflexive transitive closure of β-reduction (rule R_1 in $\lambda\mu^{1}$).*

In order to prove that the mapping preserves SN, we need to distinguish between the two kinds of λ^{LP}-reduction: principal reduction (using the rules β, γ, μ, ζ and θ) and permutative reduction (rules ψ_L, ψ_R, ϕ_L, ϕ_R, χ_L, χ_R, ι_L and ι_L). A principal reduction step maps to one or more reduction steps in $\lambda\mu^1$, while permutative reduction steps are dropped by the mapping (i.e. they translate to 0 reduction steps in $\lambda\mu^1$).

Lemma 5.6. *If $M \to N$ in λ^{LP} without the use of permutative rules, then $\langle\!| M |\!\rangle \to^+ \langle\!| N |\!\rangle$ in $\lambda\mu^1$. That is, $\langle\!| M |\!\rangle$ reduces to $\langle\!| N |\!\rangle$ in 1 or more steps.*

Lemma 5.7. *If $M \to N$ in λ^{LP} using only permutative rules, then $\langle\!| M |\!\rangle = \langle\!| N |\!\rangle$.*

SN of permutative reduction may be shown by means of a polynomial interpretation using the standard ordering over the natural numbers. For every reduction step $M \to N$ one shows that $N_{\mathcal{A}} < M_{\mathcal{A}}$. For example, the following interpretation may be used:

$$\begin{aligned}
x^B_{\mathcal{A}} &\triangleq 2 \\
v^B_{\mathcal{A}} &\triangleq 2 \\
(M^{C\supset B} N^A)^B_{\mathcal{A}} &\triangleq M^{C\supset B}_{\mathcal{A}} \times N^A_{\mathcal{A}} \\
(\lambda x^A.M^B)^A \supset B_{\mathcal{A}} &\triangleq 2 \times M^B_{\mathcal{A}} \\
([\alpha^B]M^B)^{\perp}_{\mathcal{A}} &\triangleq 2 \times M^B_{\mathcal{A}} \\
(\mu\alpha^B.M^{\perp})^B_{\mathcal{A}} &\triangleq 2 \times M^{\perp}_{\mathcal{A}} \\
(!M^B)^{[\![s]\!]B}_{\mathcal{A}} &\triangleq 1 + M^B_{\mathcal{A}} \\
(N^B\langle v^C{:=}r, M\rangle)^{B\{v^C\leftarrow r\}}_{\mathcal{A}} &\triangleq N^B_{\mathcal{A}} \times M^{[\![r]\!]B}_{\mathcal{A}} + 1 \\
(M^B +_{\mathrm{L}} t)^B_{\mathcal{A}} &\triangleq 2 \times M^B_{\mathcal{A}} + 2 \\
(s +_{\mathrm{R}} M^B)^B_{\mathcal{A}} &\triangleq 2 \times M^B_{\mathcal{A}} + 2
\end{aligned}$$

Lemma 5.8. *Permutative reduction is SN.*

We may now prove the main result of this section.

Proposition 5.9. *Every typable λ^{LP}-term is SN.*

Proof. We prove this result by contradiction. Assume that there is an infinite reduction sequence starting from a typable λ^{LP}-term M_0. Since, by Lemma 5.8, permutative reduction is SN, our sequence must contain an infinite number of principal reduction steps. Between any two principal steps, there may be 0 or more permutative steps (always a finite number). Therefore, the reduction sequence has the form:

$$M_0 \xrightarrow{\mathrm{P}}\!\!\!\!\!\rightarrow M_0' \xrightarrow{\mathrm{B}} M_1 \xrightarrow{\mathrm{P}}\!\!\!\!\!\rightarrow M_1' \xrightarrow{\mathrm{B}} M_2 \xrightarrow{\mathrm{P}}\!\!\!\!\!\rightarrow M_2' \xrightarrow{\mathrm{B}} \cdots$$

where $\xrightarrow{\mathrm{B}}$ denotes a principal reduction step and $\xrightarrow{\mathrm{P}}$ a permutative one. Additionally, by Lemma 5.7, $\langle\!| M_i |\!\rangle = \langle\!| M_i' |\!\rangle$ for every i. Also, by Lemma 5.6, we know that for every i, $\langle\!|M_i|\!\rangle \to^{+} \langle\!|M_{i+1}|\!\rangle$ in $\lambda\mu^{1}$. We can therefore construct an infinite $\lambda\mu^{1}$-reduction sequence:

$$\langle\!|M_0|\!\rangle \to^{+} \langle\!|M_1|\!\rangle \to^{+} \langle\!|M_2|\!\rangle \to^{+} \cdots$$

However, M_0 is typable in λ^{LP} and, by Proposition 4.11, so is every M_i. Since the mapping preserves typability (Lemma 5.1), then we have an infinite reduction sequence of typable $\lambda\mu^{1}$-terms. This is an absurd, since reduction of typable $\lambda\mu^{1}$-terms is SN. Therefore, there cannot be an infinite reduction sequence starting from a typable λ^{LP}-term. □

6. Confluence

This section addresses confluence of λ^{LP}, namely that if $M_0 \twoheadrightarrow M_1$ and $M_0 \twoheadrightarrow M_2$, then there exists M_3 s.t. $M_1 \twoheadrightarrow M_3$ and $M_2 \twoheadrightarrow M_3$. Confluence is an immediate consequence (via Newman's Lemma) of the fact that λ^{LP} is strongly normalising and that all critical pairs are joinable. Regarding the latter point, note that λ^{LP} has the following critical pairs:

- $\mu - \theta :\ [\beta^A]\mu\alpha^A.[\alpha^A]M^A$ with $\alpha^A \notin \mathsf{FVF}(M^A)$
- $\mu - \iota_L :\ [\beta^A]\mu\alpha^A.M^{\perp} +_{\mathrm{L}} t$ with $\alpha^A \notin \mathsf{FVF}(t)$
- $\mu - \iota_R :\ [\beta^A]\mu\alpha^A.s +_{\mathrm{R}} M^{\perp}$ with $\alpha^A \notin \mathsf{FVF}(s)$
- $\zeta - \theta :\ (\mu\alpha^{A\supset B}.[\alpha^{A\supset B}]M^{A\supset B})N^A$ with $\alpha^{A\supset B} \notin \mathsf{FVF}(M^{A\supset B})$
- $\zeta - \iota_L :\ (\mu\alpha^{A\supset B}.M^{\perp} +_{\mathrm{L}} t)N^A$ with $\alpha^A \notin \mathsf{FVF}(t)$
- $\zeta - \iota_R :\ (\mu\alpha^{A\supset B}.s +_{\mathrm{R}} M^{\perp})N^A$ with $\alpha^A \notin \mathsf{FVF}(s)$
- $\theta - \mu :\ \mu\beta^A.[\beta^A]\mu\alpha^A.M^A$ with $\beta^A \notin \mathsf{FVF}(M^A)$
- $\theta - \chi_L :\ \mu\alpha^A.[\alpha^A]M^A +_{\mathrm{L}} t$ with $\alpha^A \notin \mathsf{FVF}(t)$
- $\theta - \chi_R :\ \mu\alpha^A.[\alpha^A]s +_{\mathrm{R}} M^A$ with $\alpha^A \notin \mathsf{FVF}(s)$

As depicted in Fig. 7 all these critical pairs are joinable (note that those involving ι_R, ϕ_R or χ_R are analogous to those involving ι_L, ϕ_L or χ_L, resp., and hence are omitted).

Proposition 6.1 (Confluence). *Reduction in λ^{LP} is confluent.*

7. Additional Permutative Rules

We briefly comment on the λ_p^{LP}-calculus, resulting from adding the following permutative reduction rules to λ^{LP}, where υ_θ is subject to the condition that $\alpha^A \notin \mathsf{FVF}(N^{[\![r]\!]B})$:

$$\begin{array}{ll}
\upsilon_\beta : M_1^{A\supset B}\langle v^C{:=}r, M_2^{[\![r]\!]C}\rangle N^A & \to (M_1^{A\supset B}N^A)\langle v^C{:=}r, M_2^{[\![r]\!]C}\rangle \\
\upsilon_\gamma : M^A\langle v^B{:=}r, N_1^{[\![r]\!]B}\langle u^C{:=}s, N_2^{[\![s]\!]C}\rangle\rangle & \to M^A\langle v^B{:=}r, N_1^{[\![r]\!]B}\rangle\langle u^C{:=}s, N_2^{[\![s]\!]C}\rangle \\
\upsilon_\mu : [\beta^B](M^B\langle v^A{:=}r, N^{[\![r]\!]A}\rangle) & \to ([\beta^B]M^B)\langle v^A{:=}r, N^{[\![r]\!]A}\rangle \\
\upsilon_\theta : \mu\alpha^A.(M^{\perp}\langle v^B{:=}r, N^{[\![r]\!]B}\rangle) & \to (\mu\alpha^A.M^{\perp})\langle v^B{:=}r, N^{[\![r]\!]B}\rangle
\end{array}$$

Proof witness equivalence must also be augmented with the inference schemes of Fig. 8. Subject Reduction is then seen to hold. Also, the following new critical pairs appear:

μ-θ Critical pair:

$$\begin{tikzcd}
{[\beta^A]\mu\alpha^A.[\alpha^A]M^A} \arrow[d, bend right] \arrow[d, bend left] \\
{[\beta^A]M^A}
\end{tikzcd}$$

ζ-θ Critical pair:

$$\begin{tikzcd}
& (\mu\alpha^{A\supset B}.[\alpha^{A\supset B}]M^{A\supset B})N^A \arrow[dl] \arrow[dr] & \\
\mu\beta^B.[\beta^B]M^{A\supset B}N^A \arrow[rr] & & M^{A\supset B}N^A
\end{tikzcd}$$

θ-μ Critical pair:

$$\begin{tikzcd}
& \mu\beta^A.[\beta^A]\mu\alpha^A.M^A \arrow[dl] \arrow[dr] & \\
\mu\alpha^A.M^A \arrow[rr, dotted, no head, "=_\alpha"] & & \mu\beta^A.M^A\{\alpha^A \leftarrow \beta^A\}
\end{tikzcd}$$

μ-ι_L Critical pair:

$$\begin{tikzcd}
& {[\beta^A]\mu\alpha^A.M^\perp +_{\mathrm{L}} t} \arrow[dl] \arrow[dr] & \\
{[\beta^A]M^\perp\{\alpha^A \leftarrow \beta^A\} +_{\mathrm{L}} t} \arrow[d] & & {[\beta^A](\mu\alpha^A.M^\perp) +_{\mathrm{L}} t} \arrow[d] \\
{([\beta^A]M^\perp\{\alpha^A \leftarrow \beta^A\}) +_{\mathrm{L}} t} & & {([\beta^A]\mu\alpha^A.M^\perp) +_{\mathrm{L}} t} \arrow[ll]
\end{tikzcd}$$

ζ-ι_L Critical pair:

$$\begin{tikzcd}
& (\mu\alpha^{A\supset B}.M^\perp +_{\mathrm{L}} t)N^A \arrow[dl] \arrow[dr] & \\
\mu\beta^B.M' +_{\mathrm{L}} t \arrow[dr] & & (\mu\alpha^{A\supset B}.M^\perp)N^A +_{\mathrm{L}} t \arrow[dl] \\
& (\mu\beta^B.M') +_{\mathrm{L}} t &
\end{tikzcd}$$

where $M' = M^\perp\{[\alpha^{A\supset B}](\bullet) \leftarrow [\beta^B](\bullet)N^A\}$

θ-χ_L Critical pair:

$$\begin{tikzcd}
& \mu\alpha^A.[\alpha^A]M^A +_{\mathrm{L}} t \arrow[dl] \arrow[dr] & \\
M^A +_{\mathrm{L}} t & & \mu\alpha^A.([\alpha^A]M^A) +_{\mathrm{L}} t \arrow[dl] \\
& (\mu\alpha^A.[\alpha^A]M^A) +_{\mathrm{L}} t \arrow[ul] &
\end{tikzcd}$$

FIGURE 7. Critical pairs of λ^{LP}

- $\mu - \upsilon_\theta :\ [\beta^A]\mu\alpha^A.(M^\perp\langle v^B{:=}r, N^{[\![r]\!]B}\rangle)$ with $\alpha^A \notin \mathsf{FVF}(N^{[\![r]\!]B})$
- $\zeta - \upsilon_\theta :\ (\mu\alpha^{A\supset B}.M_1^\perp\langle v^C{:=}r, N^{[\![r]\!]C}\rangle)M_2^A$ with $\alpha^A \notin \mathsf{FVF}(N^{[\![r]\!]C})$
- $\upsilon_\beta - \gamma :\ (M_1^{A\supset B}\langle v^C{:=}r, !N^C\rangle)M_2^A$ with $v^C \notin \mathsf{FVV}(M_2^A)$, $\mathsf{FVT}(N^C) = \mathsf{FVT}(N^C) = \emptyset$
- $\upsilon_\beta - \phi_L :\ (M_1^{A\supset B}\langle v^C{:=}r, N^{[\![r]\!]C} +_{\mathrm{L}} t\rangle)M_2^A$
- $\upsilon_\beta - \phi_R :\ (M_1^{A\supset B}\langle v^C{:=}r, s +_{\mathrm{R}} N^{[\![r]\!]C}\rangle)M_2^A$
- $\upsilon_\beta - \upsilon_\gamma :\ (M_1^{A\supset B}\langle v^C{:=}r, M_2^{[\![r]\!]C}\langle u^F{:=}s, M_3^{[\![s]\!]F}\rangle\rangle)N^A$
- $\upsilon_\gamma - \gamma :\ M_1^A\langle v^B{:=}r, M_2^{[\![r]\!]B}\langle u^C{:=}s, !N^C\rangle\rangle$ with $\mathsf{FVT}(N^C) = \mathsf{FVT}(N^C) = \emptyset$
- $\upsilon_\gamma - \phi_L :\ M_1^A\langle v^B{:=}r, M_2^{[\![r]\!]B}\langle u^C{:=}s, M_3^{[\![s]\!]C} +_{\mathrm{L}} t\rangle\rangle$
- $\upsilon_\gamma - \phi_R :\ M_1^A\langle v^B{:=}r, M_2^{[\![r]\!]B}\langle u^C{:=}s, t +_{\mathrm{R}} M_3^{[\![s]\!]C}\rangle\rangle$
- $\upsilon_\gamma - \upsilon_\gamma :\ M_1^A\langle v^B{:=}r, M_2^{[\![r]\!]B}\langle u^C{:=}s, M_3^{[\![s]\!]C}\langle w^F{:=}t, M_4^{[\![w]\!]F}\rangle\rangle\rangle$
- $\upsilon_\mu - \gamma :\ [\alpha^A](M^A\langle v^B{:=}r, !N^B\rangle)$with $\mathsf{FVT}(N^B) = \mathsf{FVT}(N^B) = \emptyset$
- $\upsilon_\mu - \phi_L :\ [\alpha^A](M^A\langle v^B{:=}r, N^{[\![r]\!]B} +_{\mathrm{L}} t\rangle)$
- $\upsilon_\mu - \phi_R :\ [\alpha^A](M^A\langle v^B{:=}r, s +_{\mathrm{R}} N^{[\![r]\!]B}\rangle)$
- $\upsilon_\mu - \upsilon_\gamma :\ [\alpha^A](M_1^A\langle v^B{:=}r, M_2^{[\![r]\!]B}\langle u^C{:=}s, M_3^{[\![s]\!]C}\rangle\rangle)$
- $\upsilon_\theta - \gamma :\ \mu\alpha^A.(M^A\langle v^B{:=}r, !N^B\rangle)$ with $\mathsf{FVT}(N^B) = \mathsf{FVT}(N^B) = \emptyset$
- $\upsilon_\theta - \phi_L :\ \mu\alpha^A.(M^A\langle v^B{:=}r, N^{[\![r]\!]B} +_{\mathrm{L}} t\rangle)$ with $\alpha^A \notin \mathsf{FVF}(N^{[\![r]\!]B} +_{\mathrm{L}} t)$
- $\upsilon_\theta - \phi_R :\ \mu\alpha^A.(M^A\langle v^B{:=}r, s +_{\mathrm{R}} N^{[\![r]\!]B}\rangle)$ with $\alpha^A \notin \mathsf{FVF}(s +_{\mathrm{R}} N^{[\![r]\!]B})$

$$\frac{\Theta, \upsilon^{C}; \Gamma; \Delta \vdash A \supset B \mid s_1 \quad \Theta; \Gamma; \Delta \vdash [\![r]\!]C \mid s_2 \quad \Theta; \Gamma; \Delta \vdash A \mid t}{\Theta; \Gamma; \Delta \vdash\ s_1\langle \upsilon^{C} := r, s_2\rangle \cdot t \equiv (s_1 \cdot t)\langle \upsilon^{C} := r, s_2\rangle : B\{\upsilon^{C} \leftarrow r\}} \ \mathsf{Eq}\text{-}\upsilon_{\beta}$$

$$\frac{\Theta, \upsilon^{B}, u^{C}; \Gamma; \Delta \vdash A \mid t_1 \quad \Theta, u^{C}; \Gamma; \Delta \vdash [\![r]\!]B \mid t_2 \quad \Theta; \Gamma; \Delta \vdash [\![s]\!]C \mid t_3}{\Theta; \Gamma; \Delta \vdash\ t_1\langle \upsilon^{B} := r, t_2\langle u^{C} := s, t_3\rangle\rangle \equiv t_1\langle \upsilon^{B} := r, t_2\rangle\langle u^{C} := s, t_3\rangle : A\{\upsilon^{B} \leftarrow r\}} \ \mathsf{Eq}\text{-}\upsilon_{\gamma}$$

$$\frac{\Theta, \upsilon^{A}; \Gamma; \Delta, \beta^{B} \vdash B \mid s \quad \Theta; \Gamma; \Delta, \beta^{B} \vdash [\![r]\!]A \mid t}{\Theta; \Gamma; \Delta, \beta^{B} \vdash\ [\beta^{B}](s\langle \upsilon^{A} := r, t\rangle) \equiv ([\beta^{B}]s)\langle \upsilon^{A} := r, t\rangle : \bot} \ \mathsf{Eq}\text{-}\upsilon_{\mu}$$

$$\frac{\Theta, \upsilon^{B}; \Gamma; \Delta, \alpha^{A} \vdash \bot \mid s \quad \Theta; \Gamma; \Delta \vdash [\![r]\!]B \mid t \quad \alpha^{A} \notin \mathsf{FVF}(N^{[\![r]\!]B})}{\Theta; \Gamma; \Delta \vdash\ \mu\alpha^{A}.(s\langle \upsilon^{B} := r, t\rangle) \equiv (\mu\alpha^{A}.s)\langle \upsilon^{B} := r, t\rangle : A} \ \mathsf{Eq}\text{-}\upsilon_{\theta}$$

Figure 8. Additional proof witness equivalence schemes

- $\upsilon_{\theta} - \upsilon_{\gamma}$: $\mu\alpha^{A}.(M_1^{A}\langle \upsilon^{B} := r, M_2^{[\![r]\!]B}\langle u^{C} := s, M_3^{[\![s]\!]C}\rangle\rangle)$ with $\alpha^{A} \notin \mathsf{FVF}(M_2^{[\![r]\!]B}) \cup \mathsf{FVF}(M_3^{[\![s]\!]C})$

These are all joinable (Appendix section). Regarding SN, $\lambda_p^{\mathsf{LP}} \backslash \{\upsilon_{\mu}, \upsilon_{\theta}\}$ may be proved SN by translating it into the $\lambda\mu^{\rightarrow\wedge\vee\bot}$-calculus of [11] adapting the translation of [15]. The translation is the same as the one shown in Sect. 5, except for the following clauses:

$$\begin{aligned} (\!| \upsilon^{A} |\!) &\triangleq \upsilon^{(\!| A |\!)} \\ (\!| (!M^{A})^{[\![s]\!]A} |\!) &\triangleq \iota_1((\!| M^{A} |\!)) \\ (\!| (N^{B}\langle \upsilon^{A} := r, M^{[\![r]\!]A}\rangle)^{B\{\upsilon^{A} \leftarrow r\}} |\!) &\triangleq \delta((\!| N^{B} |\!), \upsilon^{(\!| A |\!)}.(\!| M^{A} |\!), \upsilon^{(\!| A |\!)}.(\!| M^{A} |\!)) \end{aligned}$$

where ι_1 is the term denoting a left injection into a disjoint union and δ is the case elimination construct of the disjoint union. Note that the translated versions of rules υ_{β} and υ_{γ} are already present in $\lambda\mu^{\rightarrow\wedge\vee\bot}$, since this calculus already includes the two permutation rules:

$$\begin{gathered} \delta(M, x.N, y.O)\ P \rightarrow \delta(M, x.N\,P, y.O\,P) \\ \delta(\delta(M, x.N, y.O), u.P, v.Q) \rightarrow \delta(M, x.\delta(N, u.P, v.Q), y.\delta(O, u.P, v.Q)) \end{gathered}$$

For $\lambda_p^{\mathsf{LP}} \backslash \{\upsilon_{\mu}, \upsilon_{\theta}\}$ we thus obtain confluence from Newman's Lemma. As regards SN for λ_p^{LP}, we conjecture that it should be easily obtainable by adapting the approach mentioned above for $\lambda_p^{\mathsf{LP}} \backslash \{\upsilon_{\mu}, \upsilon_{\theta}\}$.

8. Related Work

Applications of modal logic to programming languages are extensive. A review may be found here [12]. The specific applications of LP, via the Curry–Howard isomorphism, to programming languages were mentioned in the introduction. Further details are supplied in this section.

In [2] a lambda calculus where the reduction history is part of the term is introduced. The following scheme is used to recover Subject Reduction (which fails for the naive scheme as discussed in Sect. 2), e encoding the derivation of the judgement $\Theta;\Gamma \vdash s \equiv t : A|e$:

$$\frac{\Theta;\Gamma \vdash M^A \mid s \quad \Theta;\Gamma \vdash s \equiv t : A|e}{\Theta;\Gamma \vdash e \rhd M^A \mid s}\,\mathsf{Eq}$$

Strong normalisation is deduced for the resulting term assignment λ^I from weak-normalisation using techniques from higher-order rewriting. Also, a Church–Rosser theorem yields confluence of λ^I. Note that since terms carry information on how a result is computed (very much in line with Lévy labels in rewriting), the CR result may be considered a strengthening of the standard CR result of the typed lambda calculus.

In [7] the history or computation trail is allowed to be inspected by introducing trail variables; this permits the calculus to model history-based access control [3] and history-based information flow [9]. In that work the following term assignment for $\Box\mathsf{I}$ is proposed, where Δ is a set of trail variables:

$$\frac{\Theta;\Delta;\cdot \vdash M^A \mid s \quad \Theta;\Delta;\cdot \vdash s \equiv t : A|e}{\Theta;\Delta';\Gamma \vdash (!^{\Delta}_{e} M)^{\llbracket t \rrbracket A} \mid !t}\,\Box\mathsf{I}$$

A term of the form $!^{\Delta}_{e} M$ operates as an audited computation unit, where all computation is audited and locally scoped within M.

Also, in [8] by interpreting $\Box A$ as mobile code of type A, LP suggests a calculus of certified mobile units which enriches mobile code with certificates (representing type derivations). Such units take the form $\mathsf{box}_s\, M$, s being the certificate and M the executable. Composition of certified mobile units allows one to build mobile code out of other pieces of mobile code together with certificates that are also composed out of other certificates. For example, the term

$$\lambda a.\lambda b.unpack\; a\; to\; \langle \overset{\bullet}{u}, \overset{\circ}{u} \rangle\; in\; (unpack\; b\; to\; \langle \overset{\bullet}{v}, \overset{\circ}{v} \rangle\; in\; (box_{\overset{\circ}{u}\cdot\overset{\circ}{v}}\; \overset{\bullet}{u}\, \overset{\bullet}{v}))$$

reads as follows: "Given a mobile unit a and a mobile unit b, extract code $\overset{\bullet}{v}$ and certificate $\overset{\circ}{v}$ from b and extract code $\overset{\bullet}{u}$ and certificate $\overset{\circ}{u}$ from a. Then create new code $\overset{\bullet}{u}\,\overset{\bullet}{v}$ by applying $\overset{\bullet}{u}$ to $\overset{\bullet}{v}$ and a new certificate for this code $\overset{\circ}{u} \cdot \overset{\circ}{v}$. Finally, wrap both of these up into a new mobile unit.". The type system ensures that certificates always correspond to the mobile code with which it is enclosed.

9. Conclusions

A presentation of LP based on hypothetical reasoning, dubbed HLP, is proposed. The work builds, on the one hand, on Parigot's Classical Natural Deduction and, on the other, on prior work by one of the authors on hypothetical presentations of an intuitionistic fragment of LP [2,7,8,20]. This yields a Natural Deduction formalism for proving LP theorems. A term assignment is proposed which is accompanied by a fine analysis of normalisation of derivations in HLP: derivations are represented as terms and normalisation steps on derivations are encoded as reduction steps over terms. This yields a lambda calculus, the λ^{LP}-calculus. Strong normalisation of reduction in λ^{LP} is shown to hold together with confluence (which is a rather immediate consequence of strong normalisation given that all critical pairs converge).

The are a number of avenues for further research. Given that one of the main motivations behind this work is to uncover programming idioms behind HLP via the Curry-Howard isomorphism, quite some work needs to be developed in that direction. A combination of continuation-based computation together with history-based computation should emerge. The latter feature may require variants of the term assignment proposed here in which the full set of derivations is encoded (cf. [7]). Other issues involve the study of fundamental properties of programming languages with regards to the calculus, as pioneered by the work of Plotkin [19]. In particular this includes the study of abstract machines, reduction strategies such as call-by-name and appropriate notions of standard derivations.

Appendix: Confluence

This section depicts (Figs. 9, 10, 11) how the critical pairs that arise from the additional permutation rules (Sect. 7) may be joined.

μ-υ_θ Critical pair:

$$\begin{tikzcd}
 & {[\beta^A]\mu\alpha^A.(M^\perp\langle v^B{:=}r, N^{\llbracket r\rrbracket B}\rangle)} \arrow[dl] \arrow[dr] & \\
M^\perp\{\alpha^A \leftarrow \beta^A\}\langle v^B{:=}r, N^{\llbracket r\rrbracket B}\rangle & & {[\beta^A]((\mu\alpha^A.M^\perp)\langle v^B{:=}r, N^{\llbracket r\rrbracket B}\rangle)} \arrow[dl] \\
 & {([\beta^A]\mu\alpha^A.M^\perp)\langle v^B{:=}r, N^{\llbracket r\rrbracket B}\rangle} \arrow[ul] &
\end{tikzcd}$$

ζ-υ_θ Critical pair:

$$\begin{tikzcd}
 & (\mu\alpha^{A\supset B}.M_1^\perp\langle v^C{:=}r, N^{\llbracket r\rrbracket C}\rangle)M_2^A \arrow[dl] \arrow[dr] & \\
\mu\beta^B.(M_1^\perp\{[\alpha^{A\supset B}](\bullet)\leftarrow[\beta^B](\bullet)M_2^A\}\langle v^C{:=}r, N^{\llbracket r\rrbracket C}\rangle) \arrow[d] & & (\mu\alpha^{A\supset B}.M_1^\perp)\langle v^C{:=}r, N^{\llbracket r\rrbracket C}\rangle M_2^A \arrow[d] \\
(\mu\beta^B.M_1^\perp\{[\alpha^{A\supset B}](\bullet)\leftarrow[\beta^B](\bullet)M_2^A\})\langle v^C{:=}r, N^{\llbracket r\rrbracket C}\rangle & & ((\mu\alpha^{A\supset B}.M_1^\perp)M_2^A)\langle v^C{:=}r, N^{\llbracket r\rrbracket C}\rangle \arrow[ll]
\end{tikzcd}$$

υ_β-γ Critical pair:

$$\begin{tikzcd}
 & (M_1^{A\supset B}\langle v^C{:=}r, !N^C\rangle)M_2^A \arrow[dl] \arrow[dr] & \\
(M_1^{A\supset B}M_2^A)\langle v^C{:=}r, !N^C\rangle \arrow[rr] & & M_1^{A\supset B}\{v^C\leftarrow N^C, r\}M_2^A
\end{tikzcd}$$

υ_β-ϕ_L Critical pair:

$$\begin{tikzcd}
 & (M_1^{A\supset B}\langle v^C{:=}r, N^{\llbracket r\rrbracket C}+_{\mathrm{L}} t\rangle)M_2^A \arrow[dl] \arrow[dr] & \\
(M_1^{A\supset B}M_2^A)\langle v^C{:=}r, N^{\llbracket r\rrbracket C}+_{\mathrm{L}} t\rangle \arrow[d] & & (M_1^{A\supset B}\langle v^C{:=}r, N^{\llbracket r\rrbracket C}\rangle+_{\mathrm{L}} t)M_2^A \arrow[d] \\
(M_1^{A\supset B}M_2^A)\langle v^C{:=}r, N^{\llbracket r\rrbracket C}\rangle+_{\mathrm{L}} t & & (M_1^{A\supset B}\langle v^C{:=}r, N^{\llbracket r\rrbracket C}\rangle M_2^A)+_{\mathrm{L}} t \arrow[ll]
\end{tikzcd}$$

FIGURE 9. Additional critical pairs associated to permutative reductions (1/3)

υ_β-υ_γ Critical pair:

$$\begin{tikzcd}
& (M_1^{A\supset B}\langle v^C{:=}r, M_2^{\llbracket r\rrbracket C}\langle u^F{:=}s, M_3^{\llbracket s\rrbracket F}\rangle\rangle)N^A \arrow[dl] \arrow[dr] & \\
(M_1^{A\supset B}N^A)\langle v^C{:=}r, M_2^{\llbracket r\rrbracket C}\langle u^F{:=}s, M_3^{\llbracket s\rrbracket F}\rangle\rangle \arrow[d] & & M_1^{A\supset B}\langle v^C{:=}r, M_2^{\llbracket r\rrbracket C}\rangle\langle u^F{:=}s, M_3^{\llbracket s\rrbracket F}\rangle N^A \arrow[d] \\
(M_1^{A\supset B}N^A)\langle v^C{:=}r, M_2^{\llbracket r\rrbracket C}\rangle\langle u^F{:=}s, M_3^{\llbracket s\rrbracket F}\rangle & & (M_1^{A\supset B}\langle v^C{:=}r, M_2^{\llbracket r\rrbracket C}\rangle)N^A\langle u^F{:=}s, M_3^{\llbracket s\rrbracket F}\rangle \arrow[ll]
\end{tikzcd}$$

υ_γ-γ Critical pair:

$$\begin{tikzcd}
& M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\langle u^C{:=}s, !N^C\rangle\rangle \arrow[dl] \arrow[dr] & \\
M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\rangle\langle u^C{:=}s, !N^C\rangle \arrow[rr] & & M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\{U^C \leftarrow N^C, s\}\rangle
\end{tikzcd}$$

υ_γ-ϕ_L Critical pair:

$$\begin{tikzcd}
& M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C} +_{\mathrm{L}} t\rangle\rangle \arrow[dl] \arrow[dr] & \\
M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\rangle\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C} +_{\mathrm{L}} t\rangle \arrow[d] & & M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C}\rangle +_{\mathrm{L}} t\rangle \arrow[d] \\
M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\rangle\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C}\rangle +_{\mathrm{L}} t & & M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C}\rangle\rangle +_{\mathrm{L}} t \arrow[ll]
\end{tikzcd}$$

υ_γ-υ_γ Critical pair:

$$\begin{tikzcd}
& M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C}\langle w^F{:=}t, M_4^{\llbracket w\rrbracket F}\rangle\rangle\rangle \arrow[dl] \arrow[dr] & \\
M_1\langle v^B{:=}r, M_2\rangle\langle u^C{:=}s, M_3\langle w^F{:=}t, M_4\rangle\rangle \arrow[d] & & M_1\langle v^B{:=}r, M_2\langle u^C{:=}s, M_3\rangle\langle w^F{:=}t, M_4\rangle\rangle \arrow[d] \\
M_1\langle v^B{:=}r, M_2\rangle\langle u^C{:=}s, M_3\rangle\langle w^F{:=}t, M_4\rangle & & M_1\langle v^B{:=}r, M_2\langle u^C{:=}s, M_3\rangle\rangle\langle w^F{:=}t, M_4\rangle \arrow[ll]
\end{tikzcd}$$

υ_μ-γ Critical pair:

$$\begin{tikzcd}
& {[\alpha^A](M^A\langle v^B{:=}r, !N^B\rangle)} \arrow[dl] \arrow[dr] & \\
([\alpha^A]M^A)\langle v^B{:=}r, !N^B\rangle \arrow[rr] & & {[\alpha^A]M^A\{v^B \leftarrow r, N^B\}}
\end{tikzcd}$$

υ_μ-ϕ_L Critical pair:

$$\begin{tikzcd}
& {[\alpha^A](M^A\langle v^B{:=}r, N^{\llbracket r\rrbracket B} +_{\mathrm{L}} t\rangle)} \arrow[dl] \arrow[dr] & \\
([\alpha^A]M^A)\langle v^B{:=}r, N^{\llbracket r\rrbracket B} +_{\mathrm{L}} t\rangle \arrow[d] & & {[\alpha^A](M^A\langle v^B{:=}r, N^{\llbracket r\rrbracket B}\rangle +_{\mathrm{L}} t)} \arrow[d] \\
([\alpha^A]M^A)\langle v^B{:=}r, N^{\llbracket r\rrbracket B}\rangle +_{\mathrm{L}} t & & ([\alpha^A](M^A\langle v^B{:=}r, N^{\llbracket r\rrbracket B}\rangle)) +_{\mathrm{L}} t \arrow[ll]
\end{tikzcd}$$

FIGURE 10. Additional critical pairs associated to permutative reductions (2/3)

υ_μ-υ_γ Critical pair:

$$\begin{tikzcd}
& {[\alpha^A](M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C}\rangle\rangle)} \arrow[dl] \arrow[dr] & \\
{([\alpha^A]M^A)\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C}\rangle\rangle} \arrow[d] & & {[\alpha^A](M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\rangle\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C}\rangle)} \arrow[d] \\
{([\alpha^A]M^A)\langle v^B{:=}r, M_2\rangle\langle u^C{:=}s, M_3\rangle} & & {([\alpha^A](M^A\langle v^B{:=}r, M_2\rangle))\langle u^C{:=}s, M_3\rangle} \arrow[ll, two heads]
\end{tikzcd}$$

υ_θ-γ Critical pair:

$$\begin{tikzcd}
& {\mu\alpha^A.(M^A\langle v^B{:=}r, !N^B\rangle)} \arrow[dl] \arrow[dr] & \\
{(\mu\alpha^A.M^A)\langle v^B{:=}r, !N^B\rangle} \arrow[rr] & & {\mu\alpha^A.M^A\{v^B \leftarrow r, N^B\}}
\end{tikzcd}$$

υ_θ-ϕ_L Critical pair:

$$\begin{tikzcd}
& {\mu\alpha^A.(M^A\langle v^B{:=}r, N^{\llbracket r\rrbracket B} +_{\mathrm{L}} t\rangle)} \arrow[dl] \arrow[dr] & \\
{(\mu\alpha^A.M^A)\langle v^B{:=}r, N^{\llbracket r\rrbracket B} +_{\mathrm{L}} t\rangle} \arrow[d] & & {\mu\alpha^A.(M^A\langle v^B{:=}r, N^{\llbracket r\rrbracket B}\rangle +_{\mathrm{L}} t)} \arrow[d] \\
{(\mu\alpha^A.M^A)\langle v^B{:=}r, N^{\llbracket r\rrbracket B}\rangle +_{\mathrm{L}} t} & & {(\mu\alpha^A.(M^A\langle v^B{:=}r, N^{\llbracket r\rrbracket B}\rangle)) +_{\mathrm{L}} t} \arrow[ll, two heads]
\end{tikzcd}$$

υ_θ-υ_γ Critical pair:

$$\begin{tikzcd}
& {\mu\alpha^A.(M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C}\rangle\rangle)} \arrow[dl] \arrow[dr] & \\
{(\mu\alpha^A.M^A)\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C}\rangle\rangle} \arrow[d] & & {\mu\alpha^A.(M_1^A\langle v^B{:=}r, M_2^{\llbracket r\rrbracket B}\rangle\langle u^C{:=}s, M_3^{\llbracket s\rrbracket C}\rangle)} \arrow[d] \\
{(\mu\alpha^A.M^A)\langle v^B{:=}r, M_2\rangle\langle u^C{:=}s, M_3\rangle} & & {(\mu\alpha^A.(M^A\langle v^B{:=}r, M_2\rangle))\langle u^C{:=}s, M_3\rangle} \arrow[ll, two heads]
\end{tikzcd}$$

Figure 11. Additional critical pairs associated to permutative reductions (3/3)

References

[1] Artemov, S.N., Beklemishev, L.D.: Provability logic. In: Handbook of Philosophical Logic, 2nd ed, 13, pp. 189–360. Springer, New York (2005)

[2] Sergei, N.: Artëmov and Eduardo Bonelli. The intensional lambda calculus. In: Artëmov, S.N., Nerode, A. (eds.) LFCS, vol. 4514 of Lecture Notes in Computer Science, pp. 12–25. Springer, New York (2007)

[3] Abadi, M., Fournet, C.: Access control based on execution history. In: In Proceedings of the 10th Annual Network and Distributed System Security Symposium, pp. 107–121, (2003)

[4] Sergei, N.: Artëmov and Rosalie Iemhoff. The basic intuitionistic logic of proofs. J. Symb. Log. **72**(2), 439–451 (2007)

[5] Artëmov, S.: Operational modal logic. Technical Report Technical Report MSI 95-29, Cornell University (1995)

[6] Sergei, N.: Artëmov. Explicit provability and constructive semantics. Bull. Symbolic Logic **7**(1),1–36 (2001)

[7] Bavera, F., Bonelli, E.: Justification logic and history based computation. In: Cavalcanti, A., Déharbe, D., Gaudel, M., Woodcock, J. (eds.) ICTAC, vol. 6255 of Lecture Notes in Computer Science, pp. 337–351. Springer, New York (2010)

[8] Bonelli, E., Feller, F.: Justification logic as a foundation for certifying mobile computation. Ann. Pure Appl. Logic **163**(7), 935–950 (2012)

[9] Banerjee, A., Naumann, D.A.: History-based access control and secure information flow. In: Construction and Analysis of Safe, Secure, and Interoperable Smart Devices, International Workshop (CASSIS 2004), Revised Selected Papers, vol. 3362 of Lecture Notes in Computer Science, pp. 27–48. Springer-Verlag, Berlin (2005)

[10] Dashkov, E.: Arithmetical completeness of the intuitionistic logic of proofs. J. Log. Comput. **21**(4), 665–682 (2011)

[11] de Groote, P.: Strong normalization of classical natural deduction with disjunction. In: Typed Lambda Calculi and Applications, pp. 182–196. Springer, New York (2001)

[12] Davies, R., Pfenning, F.: A modal analysis of staged computation. In: Hans-Juergen B., Guy L.S. Jr. (eds.) POPL, pp. 258–270. ACM Press, New York (1996)

[13] Kuznets, R.: A note on the use of sum in the logic of proofs (2009)

[14] Lévy, J.-J.: Réductions correctes et optimales dans le lambda-calcul. PhD thesis, Paris 7 (1978)

[15] Nanevski, A., Pfenning, F., Pientka, B.: Contextual modal type theory. ACM Trans. Comput. Log. **9**(3), 23:1–23:49 (2008)

[16] Parigot, M.: Lambda-mu-calculus: an algorithmic interpretation of classical natural deduction. In: Voronkov, A. (ed.) LPAR, vol. 624 of Lecture Notes in Computer Science, pp. 190–201. Springer, New York (1992)

[17] Parigot, M.: Proofs of strong normalisation for second order classical natural deduction. J. Symbolic Logic **62**(4), 1461–1479 (1997)

[18] Pfenning, F., Davies, R.: A judgmental reconstruction of modal logic. Math. Struct. Comput. Sci. **11**(4), 511–540 (2001)

[19] Plotkin, G.D.: Call-by-name, call-by-value and the lambda-calculus. Theor. Comput. Sci. **1**(2), 125–159 (1975)

[20] Steren, G., Bonelli, E.: Intuitionistic hypothetical logic of proofs. Electr. Notes Theor. Comput. Sci. **300**, 89–103 (2014)

Eduardo Bonelli
CONICET, UNQ and ITBA
Roque Sáenz Peña 352, Bernal, Buenos Aires
Argentina
e-mail: ebonelli@unq.edu.ar

Gabriela Steren
UBA
Buenos Aires
Argentina
e-mail: gsteren@yahoo.com

Received: September 16, 2013.
Accepted: February 5, 2014.