Journal of Logic and Computation Advance Access published January 30, 2016

The first-order hypothetical logic of proofs

GABRIELA STEREN, *Depto. de Computación, FCEyN, UBA, Argentina.*
E-mail: gsteren@yahoo.com

EDUARDO BONELLI, *Depto. de Ciencia y Tecnología, UNQ, Argentina and CONICET.*
E-mail: eabonelli@gmail.com

Abstract

The Propositional Logic of Proofs (LP) is a modal logic in which the modality $\Box A$ is revisited as $[\![t]\!]A$, t being an expression that bears witness to the validity of A. It enjoys arithmetical soundness and completeness, can realize all S4 theorems and is capable of reflecting its own proofs ($\vdash A$ implies $\vdash [\![t]\!]A$, for some t). A presentation of first-order LP has recently been proposed, FOLP, which enjoys arithmetical soundness and has an exact provability semantics. A key notion in this presentation is how free variables are dealt with in a formula of the form $[\![t]\!]A(i)$. We revisit this notion in the setting of a Natural Deduction presentation and propose a Curry–Howard correspondence for FOLP. A term assignment is provided and a proof of strong normalization is given.

Keywords: First-Order Logic of Proofs, lambda calculus, natural deduction, curry howard isomorphism.

1 Introduction

Justification Logic [2] is a family of modal logics in which the modality $\Box A$ is revisited as $[\![t]\!]A$, t being an expression that bears witness to the validity of A. The Propositional Logic of Proofs (LP) is the first member of this family. A recent addition is the First-Order Logic of Proofs (FOLP) [9], which extends LP to first-order logic, enjoys a natural provability semantics (just like its propositional counterpart) and is able to realize all first-order modal logic theorems. We build on proof theoretical investigations of modal logic based on *judgemental reconstruction* of intuitionistic S4 [17–19, 28] later applied to LP [5, 10, 11, 14], to construct a Natural Deduction presentation for FOLP. The overall aim is to explore possible computational metaphors of (first-order) LP in terms of the Curry–Howard isomorphism. A term assignment (a lambda calculus) is proposed for which some fundamental properties are studied. We next provide a brief overview of LP and FOLP, and spell out the main ideas behind our proposal.

1.1 The logic of proofs

Early work of Orlov [36] and Gödel [23] propose an explanation of intuitionistic truth in terms of classical provability by prefixing every subformula in Int (Intuitionistic Propositional Logic) with '$\Box$', where '$\Box$' is subject to the laws of S4. Gödel established that the translation of formulas which are provable in Int are provable in S4 (this embedding is also faithful [34]). In order to complete the explanation, it is necessary to relate the '$\Box$' modality with provability in PA:

$$\mathsf{Int} \hookrightarrow \mathsf{S4} \hookrightarrow\ ?\ \hookrightarrow \mathsf{PA}. \tag{1}$$

doi:10.1093/logcom/exv090

Reading '$\Box A$' as '$\exists x.\mathit{Proof}(x,\ulcorner A \urcorner)$', where $\ulcorner A \urcorner$ denotes an appropriate numeric encoding of A, is problematic since the $\mathsf{S4}$ theorem $\Box(\neg\Box\bot)$, which expresses $\mathit{Con}(\mathsf{PA})$, is provable in PA. This situation was observed by Gödel [23], who posed two problems:

(1) Uncover the modal logic of the formal provability predicate $\exists x.\mathit{Proof}(x,\ulcorner A \urcorner)$.
(2) Devise the intended provability semantics for $\mathsf{S4}$.

Both of these problems have been solved. The first is answered by Solovay's completeness theorem [44] of Löb's logic; the second by LP [1, 3][1]:

$$\mathsf{Int} \hookrightarrow \mathsf{S4} \overbrace{\hookrightarrow}^{a} \mathsf{LP} \overbrace{\hookrightarrow}^{b} \mathsf{PA}. \tag{2}$$

LP arises essentially from skolemizing the existential quantifier which is implicit in the provability interpretation of $\Box$. It replaces statements of the form $\Box A$ (read as: *'there is some proof of A'*) by $[[t]]A$ (read as: *'t is a proof of A'*). Here t is called a **proof term**, and belongs to the set of expressions specified by the following grammar:

$$s,t ::= x \,|\, c \,|\, s\cdot t \,|\, !s \,|\, s+t.$$

Proof terms are constructed from proof variables, proof constants, application, bang and sum. The axiom and inference schemes of LP are as follows:

A0. Axioms of classical propositional logic in the language of LP
A1. $[[s]]A \supset A$
A2. $[[s]](A \supset B) \supset ([[t]]A \supset [[s\cdot t]]B)$
A3. $[[s]]A \supset [[!s]][[s]]A$
A4. $[[s]]A \supset [[s+t]]A$
A5. $[[t]]A \supset [[s+t]]A$
MP. $\vdash A \supset B \wedge \vdash A \Rightarrow \vdash B$
Nec. A axiom $\mathbf{A0}-\mathbf{A5} \Rightarrow \vdash [[c]]A$

Note that if one discards the proof terms decorating these axioms, one obtains the axioms of $\mathsf{S4}$ (**A4** and **A5** collapse to a trivial theorem). Returning to (2), the arrow marked with an (a) is Artemov's **realization theorem** [1, Thm.9.4] which states that $\mathsf{S4} \vdash A$ implies $\mathsf{LP} \vdash A^r$, for some normal realization $\bullet^r$. A **realization** is a function that decorates each occurrence of $\Box$ with a proof term; it is said to be *normal* if each negative such occurrence is decorated with a different proof variable. This entails that each $\mathsf{S4}$ theorem has an underlying statement about proofs. For instance: $\Box A \supset \Box B$ can be realized as $[[x]]A \supset [[t(x)]]B$, for an appropriate proof term $t(x)$. The arrow marked (b) in (2) is Artemov's **arithmetical soundness and completeness theorem**. The correspondence (2) was later extended to a fragment of LP capturing provability in HA [7, 16]. A further salient property of LP is that it is endowed with a **reflection** (or internalization) mechanism, meaning that $\vdash A$ implies there exists a ground t s.t. $\vdash [[t]]A$ [1, Corollary 5.5]. The proof of this result consists in analyzing the given derivation of A in LP, and encoding it using proof terms.

1.2 *The first-order logic of proofs*

Given a first-order language $\mathcal{L}$, the language of FOLP is obtained by extending $\mathcal{L}$ with proof variables and functional symbols for operations on proofs (*cf.* Definition 2.1). Also, the set of formulas is

[1] LP later gave birth to the family of Justification Logics [2, 4].

extended with a skolemized version of the modal operator $\Box$ whose notation we shall introduce shortly. A crucial aspect is how parameters are understood in this skolemized version. Consider the formula $\Box A(i)$, where A has a parameter i. This parameter can play one of two roles in a *proof* of $A(i)$. It can be interpreted as a *global parameter*. Global parameters are placeholders and, as such, may be substituted by any first-order expression (denoting an individual) at all. For example, in the following derivation $\pi(j)$, where P is a binary predicate letter and F is a first-order expression:

$$\dfrac{\dfrac{\forall i,j.P(i,j)\supset P(j,i)}{P(F,j)\supset P(j,F)} \qquad P(F,j)}{P(j,F)}$$

the parameter j acts as a global parameter since it may be substituted for any first-order expression E in order to obtain a derivation $\pi(E)$ of $P(E,F)$. However, parameters can also play a different role, namely that of *eigenvariables*: syntactic objects subject to generalization. For example, consider the derivation:

$$\dfrac{\pi(j)}{\forall j.\forall i.P(i,j)},$$

where $\pi(j)$ is:

$$\dfrac{\dfrac{\dfrac{\forall i.\forall j.P(i,j)}{\forall j.P(i,j)}}{P(i,j)}}{\forall i.P(i,j)}.$$

The parameter j here is not meant to be substituted for; rather it acts as a fresh scoped constant. These two distinct roles have been identified in Computer Science in the context of proof assistants where reasoning over open objects is explored (*cf.* [22] and the citations therein; see also the discussion on proving universally quantified expressions using the extensional versus intensional approach of Miller and Tiu [32]).

The above considerations lead to the following skolemized modal operator, proposed in [9], which allows both interpretations to be accounted for:

$$[[s]]_{\Xi}A.$$

Here Ξ is a set of variables and determines the role that a variable plays in a proof of A. Variables in Ξ play the role of global parameters in A and hence in s (which encodes a proof of A). Variables that occur in A but that are *not* in Ξ are understood as eigenvariables. These are therefore taken to be implicitly bound in A: $\mathsf{FIV}([[s]]_{\Xi}A)$, the set of free individual variables in $[[s]]_{\Xi}A$, is defined to be Ξ. Arithmetical soundness, realization and reflection are generalized to FOLP [9].

1.3 The first-order hypothetical logic of proofs

Our Natural Deduction presentation for FOLP, dubbed FOHLP, arises from the task of giving meaning to expressions of the following form called *judgements*:

$$\Theta;\Gamma;\Delta\vdash A\,|\,s$$

$$\Gamma, A \vdash A; \Delta$$

$$\frac{\Gamma, A \vdash B; \Delta}{\Gamma \vdash A \supset B; \Delta} \supset I \qquad \frac{\Gamma \vdash A \supset B; \Delta \quad \Gamma \vdash A; \Delta}{\Gamma \vdash B; \Delta} \supset E$$

$$\frac{\Gamma \vdash \bot; \Delta, A}{\Gamma \vdash A; \Delta} \,\mathsf{NAbs} \qquad \frac{\Gamma \vdash A; \Delta, A}{\Gamma \vdash \bot; \Delta, A} \,\mathsf{Name}$$

FIGURE 1. Classical natural deduction schemes.

Θ is a set of validity hypotheses, Γ is a set of truth hypotheses, and Δ is a set of negated truth (false) hypotheses. The intended reading is, 's is evidence of the truth of A under truth hypotheses Γ, validity hypotheses Θ and false hypotheses Δ'. Hypotheses of truth and validity arise from the work on judgemental reconstruction of S4 [17–19, 28]; the hypothesis of falsity is perhaps less frequently used. It arises from the work of Parigot [37, 38] on Classical Natural Deduction (CND), a variation of Natural Deduction for classical logic. CND admits the $\lambda\mu$-calculus as term assignment, a variation of the lambda calculus which supplies classical logic with an interesting computational interpretation built around the notion of *continuation* (and, more recently, also related to *streams* [43]).

Before proceeding any further, and for the sake of self-containedness, we briefly revisit Parigot's CND[2].

CND. Parigot introduces sequents of the form $\Gamma \vdash \Delta$, where Γ and Δ are sets of formulas. The axioms and inference schemes are given in Figure 1. Note that all inferable sequents have a formula in Δ that is singled out and called *active* (written to the left of the ';'). CND proves exactly the classical tautologies. On an understanding that hypotheses in Δ are negated, NAbs is interpreted as classical absurdity and Name as an instance of implication elimination. CND admits the following term assignment where hypotheses in Γ are labeled $x, y, \ldots$ and those in Δ are labelled $\alpha, \beta, \ldots$:

$$\Gamma, x : A \vdash x : A; \Delta$$

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

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

Apart from β, three further rules describe reduction in $\lambda\mu$, where $N\llparenthesis [\alpha^{A\supset B}](\bullet) \leftarrow [\beta^B](\bullet)U \rrparenthesis$ below is a notion of substitution called *structural substitution* and consists in replacing all occurrences of $[\alpha^{A\supset B}]M$ in N with $[\beta^B](MU)$.

$$\begin{array}{llll}
\varsigma: & (\mu\alpha^{A\supset B}.M)N & \to & \mu\beta^B.M\llparenthesis [\alpha^{A\supset B}](\bullet) \leftarrow [\beta^B](\bullet)N \rrparenthesis \\
\beta_\mu: & [\beta^A]\mu\alpha^A.M & \to & M\{\alpha^A \leftarrow \beta^A\} \\
\eta_\mu: & \mu\alpha^A.[\alpha^A]M & \to & M, \qquad\qquad\qquad\qquad \text{if } \alpha^A \notin \mathsf{FV}(U).
\end{array}$$

[2] There are nowadays a number of variations of Parigot's CND and its associated $\lambda\mu$-calculus (*cf.* [42]); we essentially follow the simplified presentation of [45].

These schemes spell out an interesting operational reading of the new term constructs. The term $\mu\alpha^A.M$ may be understood as naming its current evaluation context α and then continuing as M. Similarly, $[\alpha^A]M$ calls the continuation α, passing it the value of M. An encoding of the standard throw and catch mechanism by means of naming and abstraction is possible [45, Ex.6.2.9.]. Computation with continuations has been present in many influential programming languages such as Scheme and ML.

FOHLP. Returning to our discussion on FOHLP, the introduction scheme for the modality in Propositional Hypothetical LP [5, 14] is:

$$\frac{\Theta;\cdot;\cdot\vdash A\,|\,s \qquad \Theta;\cdot;\cdot\vdash s\equiv t{:}A}{\Theta;\Gamma;\Delta\vdash [[t]]A\,|\,!t}\ \Box\mathsf{I}_{\mathsf{LP}}.$$

Here '$\cdot$' denotes the empty context. Moreover, the judgement $\Theta;\cdot;\cdot\vdash s\equiv t{:}A$ establishes that s and t are *equivalent* in as much as proof witnesses of the validity of A (*cf.* Figure 3, Figure 4). Dropping this judgement yields the following, simpler, scheme which however does not allow the set of derivations to be closed under normalization [5]:

$$\frac{\Theta;\cdot;\cdot\vdash A\,|\,s}{\Theta;\Gamma;\Delta\vdash [[s]]A\,|\,!s}\ \Box\mathsf{I}'_{\mathsf{LP}}.$$

So consider $\Box\mathsf{I}_{\mathsf{LP}}$. The double role that variables play, as discussed above, must now be reflected in this scheme (and also in the corresponding elimination scheme). Replacing $[[t]]A$ by $[[t]]_{\Xi}A$ in $\Box\mathsf{I}_{\mathsf{LP}}$ would not do since the resulting scheme allows to prove formulas which are not valid theorems of FOLP. An example is $[[t]]_{\{i\}}P(i)\supset[[t]]_{\emptyset}P(i)$, for any t. The standard rule for generalization (i.e. introduction for $\forall$) suggests that the free individual variables in A that are additionally in Θ are not eligible for generalization and hence must play the role of *global parameters*. Otherwise, they are eigenvariables. This suggests the following inference scheme:

$$\frac{\Theta;\cdot;\cdot\vdash A\,|\,s \qquad \Theta;\cdot;\cdot\vdash s\equiv t{:}A \qquad \mathsf{FIV}(\Theta)\cap\mathsf{FIV}(A)\subseteq\Xi}{\Theta;\Gamma;\Delta\vdash [[t]]_{\Xi}A\,|\,!t}\ \Box\mathsf{I}.$$

Note the condition $\mathsf{FIV}(\Theta)\cap\mathsf{FIV}(A)\subseteq\Xi$. It spells that the free individual letters in A that are in Θ *must* be treated as global parameters. Let us consider now the elimination rule. In Propositional LP it is:

$$\frac{\Theta;\Gamma;\Delta\vdash [[r]]A\,|\,s \qquad \Theta,v^A;\Gamma;\Delta\vdash C\,|\,t}{\Theta;\Gamma;\Delta\vdash C\{v^A\leftarrow r\}\,|\,t\langle v^A{:=}r,s\rangle}\ \Box\mathsf{E}_{\mathsf{LP}}.$$

The proof witness $t\langle v^A{:=}r,s\rangle$, may be ignored for now; it simply records the application of $\Box\mathsf{E}_{\mathsf{LP}}$. The upper left-hand judgement becomes $\Theta;\Gamma;\Delta\vdash[[r]]_{\Xi}A\,|\,s$ in our first-order setting. We are now faced with the following problem: when a proof of unconditional truth (validity) of A is to be substituted for v^A, the validity variable v^A supplies no information on the role that the free individual variables in A play. Indeed, the rule as it stands allows proving theorems that are not valid in FOLP (the same example as above applies). This missing information may be regained by writing $v^A_{\Xi'}$ rather than v^A.

A validity variable $v^A_{\Xi'}$ stands for a proof of unconditional truth whose global parameters must be among Ξ'*s*. These considerations lead to the following proposal for elimination of the modality:

$$\frac{\Theta;\Gamma;\Delta\vdash[[r]]_{\Xi}A\,|\,s \qquad \Theta,v^A_{\Xi'};\Gamma;\Delta\vdash C\,|\,t \qquad \Xi\cap\mathsf{FIV}(A)\subseteq\Xi'}{\Theta;\Gamma;\Delta\vdash C\{v^A_{\Xi'}\leftarrow r\}\,|\,t\langle v^A_{\Xi'}:=r,s\rangle}\ \Box\mathsf{E}.$$

The formula $[[t]]_{\{i\}}P(i)\supset[[t]]_{\emptyset}P(i)$ is no longer provable with these rules (as will be made clear in Sec. 3 where the correspondence between FOLP and FOHLP is studied).

The remainder of this work consists in verifying whether the above intuitions—and the schemes they suggest—yield a Natural Deduction presentation for FOLP which admits a strongly normalizing notion of proof normalization producing valid derivations. A term assignment will also be proposed as a step forward towards a computational reading of FOLP in terms of the Curry–Howard isomorphism.

Structure of the article. Section 2 introduces FOLP and some of its salient properties. Section 3 is devoted to the Natural Deduction presentation for FOLP. Section 4 studies the relation between FOLP and FOHLP. Section 5 proposes a term assignment and addresses strong normalization. Section 6 presents related work. Finally, we conclude. An Appendix includes detailed proofs of all results.

2 First-order logic of proofs

The language of FOLP [9] has a countable number of individual variables $i_0,i_1,\ldots$, predicate letters of any arity $P_0,P_1,\ldots$ and functional letters[3] of any arity $f_0,f_1,\ldots$, but no equality. FOLP *expressions*, denoted $E_0,E_1,\ldots$ thus are either of the form i or $f(E_1,\ldots,E_n)$, for $E_1,\ldots,E_n$ FOLP expressions. In addition to that, the language includes symbols for constructing *proof terms*. These include a countable number of proof variables,[4] proof constants and functional symbols for operations on proofs.

Definition 2.1
Proof terms and formulas of FOLP are defined as follows:

$$\begin{aligned} s,t &::= x^A\,|\,c\,|\,s\cdot t\,|\,!s\,|\,s+t\,|\,\mathsf{gen}_i(s)\\ A,B &::= P(E_1,\ldots,E_n)\,|\,\bot\,|\,A\supset B\,|\,[[s]]_{\Xi}A\,|\,\forall i.A, \end{aligned}$$

where Ξ is a set of individual variables. We often abbreviate $[[s]]_{\emptyset}A$ with $[[s]]A$.

We use '$\neg A$' as an abbreviation for '$A\supset\bot$'. Note that the functional symbols for constructing proof terms are binary '$\cdot$', unary '!', binary '+', (these three are inherited from LP) and an infinite number of unary operators '$\mathsf{gen}_i()$', one for each individual variable i. The free individual variables in E are the set of all variables that occur in it and is denoted $\mathsf{FIV}(E)$. A proof term has a free individual variable i only if it occurs in the formula that decorates a proof variable and does not occur in an expression of the form $\mathsf{gen}_i(s)$. As stated earlier, the individual variables which are free in $[[t]]_{\Xi}A$ are exactly those contained in Ξ. All other individual variables are assumed to be bound. The set of free proof variables in A are all the proof variables that occur in A and are denoted FV(A).

[3] In [9], no functional letters are assumed.

[4] In contrast to [9], we assume proof variables to be decorated with formulas.

Definition 2.2
Free individual variables in proof terms and formulas are defined by recursion as follows[5]:

$$
\begin{array}{rcl@{\qquad}rcl}
\mathsf{FIV}(P(E_1,\dots,E_n)) & \triangleq & \bigcup_{i\in 1..n}\mathsf{FIV}(E_i) & \mathsf{FIV}(x^A) & \triangleq & \mathsf{FIV}(A) \\
\mathsf{FIV}(\bot) & \triangleq & \emptyset & \mathsf{FIV}(c) & \triangleq & \emptyset \\
\mathsf{FIV}(A\supset B) & \triangleq & \mathsf{FIV}(A)\cup\mathsf{FIV}(B) & \mathsf{FIV}(s\cdot t) & \triangleq & \mathsf{FIV}(s)\cup\mathsf{FIV}(t) \\
\mathsf{FIV}([[t]]_{\Xi}A) & \triangleq & \Xi & \mathsf{FIV}(!s) & \triangleq & \mathsf{FIV}(s) \\
\mathsf{FIV}(\forall i.A) & \triangleq & \mathsf{FIV}(A)\backslash\{i\} & \mathsf{FIV}(s+t) & \triangleq & \mathsf{FIV}(s)\cup\mathsf{FIV}(t) \\
 & & & \mathsf{FIV}(\mathsf{gen}_i(s)) & \triangleq & \mathsf{FIV}(s)\backslash\{i\}
\end{array}
$$

For instance, in the formula $[[c]]_{\{j\}}(P(i)\supset Q(j)\supset P(i))$, the variable j is free, while i is bound. We work modulo α-equivalence over individual variables as generated by the following α-equivalence axioms:

$$
\begin{array}{lcll}
\forall i.A & =_{\alpha} & \forall j.A\{i\leftarrow j\}, & \text{if } j\notin\mathsf{FIV}(A) \\
[[t]]_{\Xi}A & =_{\alpha} & [[t\{i\leftarrow j\}]]_{\Xi}A\{i\leftarrow j\}, & \text{if } i\notin\Xi \text{ and } j \text{ fresh}
\end{array}
$$

Furthermore, we assume the following **variable convention**: we rename where appropriate so that the names of the bound individual variables are distinct and also different from the names of the free individual variables, in any proof witness, formula, statement or proof. For example, we do not allow formulas of the form $[[s]]_{\Xi}A$ where Ξ contains one or more individual variables which are bound in either s or A.

There are two notions of substitution, namely substitution of free individual variables and substitution of proof term variables. The latter is the standard notion of substitution where, in particular, $y^B\{x^A\leftarrow s\}=y^B$. The former is defined below.

Definition 2.3 (Individual variable substitution in FOLP)
Substitution of individual variable i in a first-order expression E' by E, written $E'\{i\leftarrow E\}$, is defined as:

$$
\begin{array}{rcll}
i\{i\leftarrow E\} & \triangleq & E & \\
j\{i\leftarrow E\} & \triangleq & j, & \text{if } j\neq i \\
f(E_1,\dots,E_n)\{i\leftarrow E\} & \triangleq & f(E_1\{i\leftarrow E\},\dots,E_n\{i\leftarrow E\}) &
\end{array}
$$

Substitution of individual variable i in a formula is defined as:

$$
\begin{array}{rcll}
P(E_1,\dots,E_n)\{i\leftarrow E\} & \triangleq & P(E_1\{i\leftarrow E\},\dots,E_n\{i\leftarrow E\}) & \\
\bot\{i\leftarrow E\} & \triangleq & \bot & \\
(A\supset B)\{i\leftarrow E\} & \triangleq & A\{i\leftarrow E\}\supset B\{i\leftarrow E\} & \\
([[s]]_{\Xi}A)\{i\leftarrow E\} & \triangleq & [[s\{i\leftarrow E\}]]_{(\Xi\backslash\{i\})\cup\mathsf{FIV}(E)}A\{i\leftarrow E\}, & \text{if } i\in\Xi \\
([[s]]_{\Xi}A)\{i\leftarrow E\} & \triangleq & [[s]]_{\Xi}A, & \text{if } i\notin\Xi \\
(\forall j.A)\{i\leftarrow E\} & \triangleq & \forall j.A\{i\leftarrow E\}, & \text{if } i\neq j \\
(\forall i.A)\{i\leftarrow E\} & \triangleq & \forall i.A &
\end{array}
$$

[5] '$\triangleq$' denotes definitional equality.

Finally, substitution of individual variable i in a proof witness is defined as:

$$\begin{array}{rcl}
x^A\{i\leftarrow E\} & \triangleq & x^{A\{i\leftarrow E\}} \\
c\{i\leftarrow E\} & \triangleq & c \\
(s\cdot t)\{i\leftarrow E\} & \triangleq & s\{i\leftarrow E\}\cdot t\{i\leftarrow E\} \\
(!s)\{i\leftarrow E\} & \triangleq & !s\{i\leftarrow E\} \\
(s+t)\{i\leftarrow E\} & \triangleq & s\{i\leftarrow E\}+t\{i\leftarrow E\} \\
\mathsf{gen}_i(s)\{i\leftarrow E\} & \triangleq & \mathsf{gen}_i(s) \\
\mathsf{gen}_j(s)\{i\leftarrow E\} & \triangleq & \mathsf{gen}_j(s\{i\leftarrow E\}), \quad \text{if } j\neq i
\end{array}$$

Note that the formula which decorates a proof variable may change after a substitution. For example $x^A\{i\leftarrow E\}=x^{A\{i\leftarrow E\}}$.

Remark 2.4
For every formula A, proof variable x and proof term s, $\mathsf{FIV}(A\{x^A\leftarrow s\})=\mathsf{FIV}(A)$.

Definition 2.5
The axiom schemes and inference rules of FOLP are the following:

A1. Axioms of first-order logic in the language of FOLP
A2. $([[t]]_{\Xi,i}A)\supset[[t]]_{\Xi}A$, if $i\notin\mathsf{FIV}(A)$
A3. $([[t]]_{\Xi}A)\supset[[t]]_{\Xi,i}A$
B1. $([[t]]_{\Xi}A)\supset A$
B2. $([[s]]_{\Xi}(A\supset B))\supset([[t]]_{\Xi}A)\supset[[(s\cdot t)]]_{\Xi}B$
B3a. $([[s]]_{\Xi}A)\supset[[(s+t)]]_{\Xi}A$
B3b. $([[t]]_{\Xi}A)\supset[[(s+t)]]_{\Xi}A$
B4. $([[t]]_{\Xi}A)\supset\ [[!t]]_{\Xi}[[t]]_{\Xi}A$
B5. $([[t]]_{\Xi}A)\supset[[\mathsf{gen}_i(t)]]_{\Xi}\forall i.A$, if $i\notin\Xi$
MP. $\vdash A\supset B\wedge\vdash A\Rightarrow\vdash B$
Gen. $\vdash A\Rightarrow\vdash\forall i.A$
Nec. A an axiom $\Rightarrow\vdash[[c]]A$

where we assume the following axiom schemes for first-order logic:

A1a. $A\supset B\supset A$
A1b. $(A\supset B\supset C)\supset(A\supset B)\supset A\supset C$
A1c. $\neg\neg A\supset A$
A1d. $(\forall i.A)\supset A\{i\leftarrow E\}$
A1e. $(\forall i.(A\supset B))\supset(\forall i.A)\supset\forall i.B$
A1f. $A\supset\forall i.A$, if $i\notin\mathsf{FIV}(A)$

A *FOLP-derivation* $(\pi,\pi'$, etc) is a sequence of formulas each of which is an instance of an axiom or the conclusion of an instance of a rule whose premisses occur before in the sequence. A set of labelled hypotheses (Γ,Γ', etc.) is written $\{x_1^{A_1},\dots,x_n^{A_n}\}$ where the x_i, with $i\in 1..n$, are labels taken from some given infinite set of labels. A FOLP-derivation from a set of labelled hypotheses $\{x_1^{A_1},\dots,x_n^{A_n}\}$ is one in which the formulas A_i, for $i\in 1..n$, may also be used in the sequence.

A *constant specification* is a set $\mathcal{C}$ of formulas of FOLP of the form $[[c]]_{\emptyset}A$. It is assumed that A is an axiom. Given a constant specification $\mathcal{C}$, a derivation is said to *meet* it if whenever the rule **Nec** is used to introduce $[[c]]_{\emptyset}A$, then $[[c]]_{\emptyset}A$ is in $\mathcal{C}$. A derivation π *determines* the (finite) constant specification $\mathcal{C}$ consisting of formulas of FOLP of the form $[[c]]_{\emptyset}A$ which are conclusions of instances of **Nec** in π. A constant specification is *injective* if $[[c]]_{\emptyset}A_1 \in \mathcal{C}$ and $[[c]]_{\emptyset}A_2 \in \mathcal{C}$, implies $A_1 = A_2$.

2.1 Additional comments

FOLP was introduced in [8]. Artemov and Yavorskaya [9] later proposed a presentation of FOLP that enjoys a natural provability semantics [9, Thm.4 and Thm.6] and that is capable, at the same time, of realizing the full set of first-order $\mathsf{S4}$ theorems [9, Thm.2]: $\mathsf{FOS4} \vdash A$ implies $\mathsf{FOLP} \vdash A^r$, for some normal realization $\bullet^r$. Just like its propositional counterpart, it can internalize its own proofs [9, Thm.1]: $[[x_0]]_{\Xi_0}A_0, \ldots, [[x_n]]_{\Xi_n}A_n \vdash A$ in FOLP implies there exists a proof term t s.t. $[[x_0]]_{\Xi_0}A_0, \ldots, [[x_n]]_{\Xi_n}A_n \vdash [[t(x_0, \ldots, x_n)]]_{\Xi_0 \cup \ldots \cup \Xi_n}A$ in FOLP.

Although arithmetical completeness is unattainable, completeness with respect to a Kripke semantics has been established by Fitting [21]. A further extension of LP that has been considered is one which includes quantification over proof variables. Such a system was studied in [47] and shown not to be axiomatizable. Also related is [46] where the parameter i in the formula $\Box A(i)$ is assumed bound (coined 'binding interpretation' in op.cit.). This system is shown to have a complete axiomatization, however it does not suffice to realize first-order modal logic [9].

3 First-order hypothetical logic of proofs

We now address the Natural Deduction presentation of FOLP, namely FOHLP. The language of FOHLP is similar to that of FOLP except that (1) it is augmented with a set of a *validity variables* $v1^{A_1}_{\Xi_1}, v2^{A_2}_{\Xi_2}, \ldots$ and one of *falsehood variables* $\alpha_1^{B_1}, \alpha_2^{B_2}, \ldots$; and (2) proof terms are replaced by *proof witnesses*. Formulas are as in Definition 2.1, except now s ranges over proof witnesses.

Definition 3.1
Proof witnesses of FOHLP are defined by the following syntax:

$$\begin{array}{rcl} r, s, t & ::= & x^A \,|\, v^A_{\Xi} \\ & | & \lambda x^A.s \,|\, s \cdot t \\ & | & !s \,|\, t\langle v^A_{\Xi'} := r, s\rangle \\ & | & [\alpha^A]s \,|\, \mu\alpha^A.s \\ & | & s + t \\ & | & \mathsf{gen}_i(s) \,|\, \mathsf{ins}^E_i(s) \end{array}$$

A proof witness is one of the following: a *truth variable* x^A, a *validity variable* v^A_{Ξ}, an *abstraction* $\lambda x^A.s$ (x^A is bound with scope s), *application* $s \cdot t$, *bang* $!s$ (which binds all free occurrences of truth and falsehood variables in s), *unbox* $t\langle v^A_{\Xi'} := r, s\rangle$ (v^A_{Ξ} is bound with scope t), *name* $[\alpha^A]s$, *name abstraction* $\mu\alpha^A.s$ (α^A is bound with scope s), *plus* $s + t$, *generalization* $\mathsf{gen}_i(s)$, and *instantiation* $\mathsf{ins}^E_i(s)$. Regarding proof witnesses of the form $t\langle v^A_{\Xi'} := r, s\rangle$ they can be read as 'replace all free occurrences of $v^A_{\Xi'}$ by r in the formula witnessed by t, with s bearing witness to the truth of $[[r]]_{\Xi}A$'.

Definition 3.2
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 $\mathsf{FVT}(A) \cup \mathsf{FVT}(B)$:

$$
\begin{aligned}
\mathsf{FVT}(P(E_1,\dots,E_n)) &\triangleq \emptyset\\
\mathsf{FVT}(\bot) &\triangleq \emptyset\\
\mathsf{FVT}(A\supset B) &\triangleq \mathsf{FVT}(A,B)\\
\mathsf{FVT}([\![s]\!]_{\Xi}A) &\triangleq \mathsf{FVT}(s)\cup\mathsf{FVT}(A)\\
\mathsf{FVT}(\forall i.A) &\triangleq \mathsf{FVT}(A)
\end{aligned}
$$

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:

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

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

We assume the following **variable conventions**: 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. 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 $[\alpha^{[\![r]\!]A\supset\neg B\supset C}]!s+t$.

DEFINITION 3.3 (Free individual variables of formulas and proof witnesses)
The set of free individual variables of a formula A, denoted $\mathsf{FIV}(A)$, is defined as in Definition 2.2. The set of free individual variables of a proof witness ar defined as follows:

$$
\begin{aligned}
\mathsf{FIV}(x^A) &\triangleq \mathsf{FIV}(A)\\
\mathsf{FIV}(v^A_{\Xi}) &\triangleq \Xi\\
\mathsf{FIV}(\lambda x^A.s) &\triangleq \mathsf{FIV}(A)\cup\mathsf{FIV}(s)
\end{aligned}
$$

$$\begin{array}{rcl}
\mathsf{FIV}(s\cdot t) & \triangleq & \mathsf{FIV}(s)\cup\mathsf{FIV}(t)\\
\mathsf{FIV}(!s) & \triangleq & \mathsf{FIV}(s)\\
\mathsf{FIV}(t\langle v^A_\Xi{:=}r,s\rangle) & \triangleq & \mathsf{FIV}(t)\cup\mathsf{FIV}(r)\cup\mathsf{FIV}(s)\cup\Xi\\
\mathsf{FIV}([\alpha^A]s) & \triangleq & \mathsf{FIV}(A)\cup\mathsf{FIV}(s)\\
\mathsf{FIV}(\mu\alpha^A.s) & \triangleq & \mathsf{FIV}(A)\cup\mathsf{FIV}(s)\\
\mathsf{FIV}(s+t) & \triangleq & \mathsf{FIV}(s)\cup\mathsf{FIV}(t)\\
\mathsf{FIV}(\mathsf{gen}_i(s)) & \triangleq & \mathsf{FIV}(s)\backslash\{i\}\\
\mathsf{FIV}(\mathsf{ins}^E_i(s)) & \triangleq & \mathsf{FIV}(s)\backslash\{i\}\cup\mathsf{FIV}(E)
\end{array}$$

Note the clause defining $\mathsf{FIV}(v^A_\Xi)$: all free individual variables that are not in Ξ are considered bound, whereas those that are in Ξ are considered free (disregarding whether they occur in A or not).

Individual variable substitution is defined similarly to that of FOLP (Definition 2.3). The only difference is that the clause for proof constants is dropped and the following new ones are added, where in the clause for $\mathsf{ins}^{E'}_i(s)\{i\leftarrow E\}$ we may assume $i\notin\mathsf{FIV}(E')$ by the variable convention:

$$\begin{array}{rcll}
v^A_\Xi\{i\leftarrow E\} & \triangleq & v^{A\{i\leftarrow E\}}_{(\Xi\backslash\{i\})\cup\mathsf{FIV}(E)}, & \text{if } i\in\Xi\\
v^A_\Xi\{i\leftarrow E\} & \triangleq & v^A_\Xi, & \text{if } i\notin\Xi\\
(t\langle v^A_\Xi{:=}r,s\rangle)\{i\leftarrow E\} & \triangleq & t\{i\leftarrow E\}\langle v^A_\Xi\{i\leftarrow E\}{:=}r\{i\leftarrow E\},s\{i\leftarrow E\}\rangle & \\
(\lambda x^A.s)\{i\leftarrow E\} & \triangleq & \lambda x^{A\{i\leftarrow E\}}.s\{i\leftarrow E\} & \\
([\alpha^A]s)\{i\leftarrow E\} & \triangleq & [\alpha^{A\{i\leftarrow E\}}]s\{i\leftarrow E\} & \\
(\mu\alpha^A.s)\{i\leftarrow E\} & \triangleq & \mu\alpha^{A\{i\leftarrow E\}}.s\{i\leftarrow E\} & \\
\mathsf{ins}^{E'}_i(s)\{i\leftarrow E\} & \triangleq & \mathsf{ins}^{E'}_i(s), & i\notin\mathsf{FIV}(E')\\
\mathsf{ins}^{E'}_j(s)\{i\leftarrow E\} & \triangleq & \mathsf{ins}^{E'\{i\leftarrow E\}}_j(s\{i\leftarrow E\}), & \text{if } j\neq i
\end{array}$$

A **truth context** (Γ) is a set of truth hypotheses $\{x_1^{A_1},\ldots,x_n^{A_n}\}$; a **validity context** (Θ) is a set of validity variables $\{{v_1}^{A_1}_{\Xi_1},\ldots,{v_n}^{A_n}_{\Xi_n}\}$; a **falsehood context** (Δ) is a set of falsehood variables $\{\alpha_1^{A_1},\ldots,\alpha_k^{A_k}\}$. We write $\cdot$ for the empty context. We write $x^A\in\Gamma$ if $\Gamma=\Gamma'\cup\{x^A\}$. Similarly for $v^A_\Xi\in\Theta$ and $\alpha^A\in\Delta$. Free individual variables of truth and falsehood contexts are defined as expected:

$$\begin{array}{rcl}
\mathsf{FIV}(\Gamma) & \triangleq & \{\mathsf{FIV}(A)\mid x^A\in\Gamma\}\\
\mathsf{FIV}(\Delta) & \triangleq & \{\mathsf{FIV}(A)\mid \alpha^A\in\Delta\}\\
\mathsf{FIV}(\Theta) & \triangleq & \bigcup\limits_{v^A_\Xi\in\Theta}\Xi
\end{array}$$

A (FOHLP) **judgement** is an expression of the form:

$$\Theta;\Gamma;\Delta\vdash A\,|\,s$$

It will often be convenient to abbreviate $\Theta;\Gamma;\Delta$ in order to improve readability. We will use $\mathcal{H}$ for this purpose and refer to it as a *composite context*. So the above judgement will also be written $\mathcal{H}\vdash A\,|\,s$. We write $i\notin\mathsf{FIV}(\mathcal{H})$ for $i\notin\mathsf{FIV}(\Theta,\Gamma,\Delta)$. Also we write: $\mathcal{H},x^A$ for $\Theta;\Gamma,x^A;\Delta$, $\mathcal{H},\alpha^A$ for $\Theta;\Gamma;\Delta,\alpha^A$, and $\mathcal{H},v^A_\Xi$ for $\Theta,v^A_\Xi;\Gamma;\Delta$.

Definition 3.4

The **inference schemes** of FOHLP derive judgements (Figure 2) and proof witness equivalence judgements (Figures 3–5). We say $\Theta;\Gamma;\Delta\vdash A\,|\,s$ is **derivable** if there is a derivation of it using these inference schemes and write $\rhd_{\mathsf{FOHLP}}\Theta;\Gamma;\Delta\vdash A\,|\,s$ (or also $\rhd_{\mathsf{FOHLP}}\mathcal{H}\vdash A\,|\,s$) in that case. Similarly for $\mathcal{H}\vdash s\equiv t{:}A$.

$$\frac{}{\mathcal{H}, x^A \vdash A \mid x^A}\;\textsf{Var}$$

$$\frac{\mathcal{H}, x^A \vdash B \mid s}{\mathcal{H} \vdash A \supset B \mid \lambda x^A.s}\;{\supset}\textsf{I} \qquad \frac{\mathcal{H} \vdash A \supset B \mid s \qquad \mathcal{H} \vdash A \mid t}{\mathcal{H} \vdash B \mid s \cdot t}\;{\supset}\textsf{E}$$

$$\frac{}{\mathcal{H}, v^A_{\Xi} \vdash A \mid v^A_{\Xi}}\;\textsf{VarM}$$

$$\frac{\Theta; \cdot; \cdot \vdash A \mid s \quad \Theta; \cdot; \cdot \vdash s \equiv t : A \quad \textsf{FIV}(\Theta) \cap \textsf{FIV}(A) \subseteq \Xi}{\Theta; \Gamma; \Delta \vdash [\![t]\!]_{\Xi} A \mid !t}\;\Box\textsf{I}$$

$$\frac{\mathcal{H} \vdash [\![r]\!]_{\Xi} A \mid s \quad \mathcal{H}, v^A_{\Xi'} \vdash C \mid t \quad \Xi \cap \textsf{FIV}(A) \subseteq \Xi'}{\mathcal{H} \vdash C\{v^A_{\Xi'} \leftarrow r\} \mid t\langle v^A_{\Xi'} := r, s\rangle}\;\Box\textsf{E}$$

$$\frac{\mathcal{H} \vdash A \mid s}{\mathcal{H} \vdash A \mid s + t}\;\textsf{PlusL} \qquad \frac{\mathcal{H} \vdash A \mid t}{\mathcal{H} \vdash A \mid s + t}\;\textsf{PlusR}$$

$$\frac{\mathcal{H}, \alpha^A \vdash \bot \mid s}{\mathcal{H} \vdash A \mid \mu\alpha^A.s}\;\textsf{NAbs} \qquad \frac{\mathcal{H}, \alpha^A \vdash A \mid s}{\mathcal{H}, \alpha^A \vdash \bot \mid [\alpha^A]s}\;\textsf{Name}$$

$$\frac{\mathcal{H} \vdash A \mid s \quad i \notin \textsf{FIV}(\mathcal{H})}{\mathcal{H} \vdash \forall i.A \mid \textsf{gen}_i(s)}\;\forall\textsf{I} \qquad \frac{\mathcal{H} \vdash \forall i.A \mid s}{\mathcal{H} \vdash A\{i \leftarrow E\} \mid \textsf{ins}^E_i(s)}\;\forall\textsf{E}$$

FIGURE 2. Axiom and inference schemes of FOHLP.

The axiom scheme Var states that the judgement $\mathcal{H}, x^A \vdash A \mid x^A$ is evident in itself: 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 $[[t]]_{\Xi}$ modality internalizes meta-level 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 witness t equivalent to s. Evidence for the truth of $[[t]]_{\Xi} A$ is constructed from the (verified) evidence that A is unconditionally true by prefixing it with a bang constructor. $\textsf{FIV}(\Theta) \cap \textsf{FIV}(A) \subseteq \Xi$ is necessary to avoid binding individual variables which are used as free variables in the premises. As mentioned in the introduction, without that restriction we would be able to prove theorems not provable in FOLP.

REMARK 3.5
We may also introduce a less general variant of □I:

$$\frac{\Theta; \cdot; \cdot \vdash A \mid t \quad \textsf{FIV}(\Theta) \cap \textsf{FIV}(A) \subseteq \Xi}{\Theta; \Gamma; \Delta \vdash [[t]]_{\Xi} A \mid !t}\;\Box\textsf{I}'.$$

This variant presents the same problem as its propositional counterpart [5, 14], as equivalence is still required for proof normalization. However, it shall prove useful for some technical results that follow.

The □E scheme allows the discharging of validity hypotheses. In order to discharge the validity hypothesis $v^A_{\Xi'}$, a proof of the validity of A is required. In this system, this requires proving that

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

$$\frac{\Theta; \cdot; \cdot \vdash A \,|\, s \qquad \textsf{FIV}(\Theta) \cap \textsf{FIV}(A) \subseteq \Xi \qquad \Theta, v^A_{\Xi}; \Gamma; \Delta \vdash C \,|\, t}{\Theta; \Gamma; \Delta \vdash\ t\langle v^A_{\Xi} := s, !s\rangle \equiv t\{v^A_{\Xi} \leftarrow s\} \colon C\{v^A_{\Xi} \leftarrow s\}}\ \textsf{Eq-}\gamma$$

$$\frac{\mathcal{H} \vdash A \,|\, s \qquad i \notin \textsf{FIV}(\Theta, \Gamma, \Delta)}{\mathcal{H} \vdash\ \textsf{ins}^E_i(\textsf{gen}_i(s)) \equiv s\{i \leftarrow E\} \colon A\{i \leftarrow E\}}\ \textsf{Eq-}\xi$$

$$\frac{\mathcal{H} \vdash [\![r]\!]_{\Xi} A \,|\, s \qquad \mathcal{H}, v^A_{\Xi'} \vdash C \,|\, u \qquad \Xi \cap \textsf{FIV}(A) \subseteq \Xi'}{\mathcal{H} \vdash\ u\langle v^A_{\Xi'} := r, (s+t)\rangle \equiv u\langle v^A_{\Xi'} := r, s\rangle + t \colon C\{v^A_{\Xi'} \leftarrow r\}}\ \textsf{Eq-}\phi_L$$

$$\frac{\mathcal{H} \vdash [\![r]\!]_{\Xi} A \,|\, t \qquad \mathcal{H}, v^A_{\Xi'} \vdash C \,|\, u \qquad \Xi \cap \textsf{FIV}(A) \subseteq \Xi'}{\mathcal{H} \vdash\ u\langle v^A_{\Xi'} := r, (s+t)\rangle \equiv s + u\langle v^A_{\Xi'} := r, t\rangle \colon C\{v^A_{\Xi'} \leftarrow r\}}\ \textsf{Eq-}\phi_R$$

$$\frac{\mathcal{H} \vdash A \supset B \,|\, r \quad \mathcal{H} \vdash A \,|\, t}{\mathcal{H} \vdash\ (r+s) \cdot t \equiv (r \cdot t) + s \colon B}\ \textsf{Eq-}\psi_L \qquad \frac{\mathcal{H} \vdash A \supset B \,|\, s \quad \mathcal{H} \vdash A \,|\, t}{\mathcal{H} \vdash\ (r+s) \cdot t \equiv r + (s \cdot t) \colon B}\ \textsf{Eq-}\psi_R$$

$$\frac{\mathcal{H} \vdash \forall i.A \,|\, s}{\mathcal{H} \vdash\ \textsf{ins}^E_i(s+t) \equiv \textsf{ins}^E_i(s) + t \colon A\{i \leftarrow E\}}\ \textsf{Eq-}\epsilon_L \qquad \frac{\mathcal{H} \vdash \forall i.A \,|\, t}{\mathcal{H} \vdash\ \textsf{ins}^E_i(s+t) \equiv s + \textsf{ins}^E_i(t) \colon A\{i \leftarrow E\}}\ \textsf{Eq-}\epsilon_R$$

FIGURE 3. Proof witness equivalence (1/2).

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

$$\frac{\mathcal{H}, \alpha^{A \supset B} \vdash \bot \,|\, s \quad \mathcal{H} \vdash A \,|\, t}{\mathcal{H} \vdash\ (\mu\alpha^{A \supset B}.s) \cdot t \equiv \mu\beta^B.s(\!|\, [\alpha^{A \supset B}](\bullet) \leftarrow [\beta^B](\bullet)t \,|\!) \colon B}\ \textsf{Eq-}\zeta$$

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

$$\frac{\mathcal{H}, \alpha^A \vdash A \,|\, s}{\mathcal{H}, \alpha^A \vdash\ [\alpha^A]s + t \equiv ([\alpha^A]s) + t \colon \bot}\ \textsf{Eq-}\chi_L \qquad \frac{\mathcal{H}, \alpha^A \vdash A \,|\, t}{\mathcal{H}, \alpha^A \vdash [\alpha^A]s + t \equiv s + [\alpha^A]t \colon \bot}\ \textsf{Eq-}\chi_R$$

$$\frac{\mathcal{H}, \alpha^A \vdash \bot \,|\, s}{\mathcal{H} \vdash\ \mu\alpha^A.(s+t) \equiv (\mu\alpha^A.s) + t \colon A}\ \textsf{Eq-}\iota_L \qquad \frac{\mathcal{H}, \alpha^A \vdash \bot \,|\, t}{\mathcal{H} \vdash\ \mu\alpha^A.(s+t) \equiv s + \mu\alpha^A.t \colon A}\ \textsf{Eq-}\iota_R$$

FIGURE 4. Proof witness equivalence (2/2).

$[[r]]_{\Xi}A$ is true with proof witness s, for some proof witnesses 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 $[[r]]_{\Xi}A$. The former is then substituted in the place of all free occurrences of $v^A_{\Xi'}$ in the proposition C. This construction is recorded with proof witness $s\langle v^A_{\Xi'} := r, t\rangle$ in the conclusion, meaning that s is proof that r can be used in place of $v^A_{\Xi'}$ in t. This has the practical effect of allowing us to take the witness r out of the box from $[[r]]_{\Xi}A$. The expression $C\{v^A_{\Xi'} \leftarrow r\}$ denotes the substitution of $v^A_{\Xi'}$ by r in C. Two final remarks on $\Box$E, its witness includes s since this is required for the proof that derivable FOHLP formulas are

$$\frac{\mathcal{H}\vdash A\,|\,s}{\mathcal{H}\vdash\ s\equiv s\colon A}\ \mathsf{Eq\text{-}Refl}\qquad\frac{\mathcal{H}\vdash\ s\equiv t\colon A}{\mathcal{H}\vdash\ t\equiv s\colon A}\ \mathsf{Eq\text{-}Symm}$$

$$\frac{\mathcal{H}\vdash\ r\equiv s\colon A\quad\mathcal{H}\vdash\ s\equiv t\colon A}{\mathcal{H}\vdash\ r\equiv t\colon A}\ \mathsf{Eq\text{-}Trans}$$

$$\frac{\mathcal{H},x^A\vdash\ s\equiv t\colon B}{\mathcal{H}\vdash\ \lambda x^A.s\equiv\lambda x^A.t\colon A\supset B}\ \mathsf{Eq\text{-}}\lambda$$

$$\frac{\mathcal{H}\vdash\ s\equiv s'\colon A\supset B\quad\mathcal{H}\vdash\ t\equiv t'\colon A}{\mathcal{H}\vdash\ s\cdot t\equiv s'\cdot t'\colon B}\ \mathsf{Eq\text{-}}\cdot$$

$$\frac{\mathcal{H}\vdash\ s\equiv s'\colon [\![r]\!]_{\Xi}A\qquad\mathcal{H},v^A_{\Xi'}\vdash\ t\equiv t'\colon C\qquad\Xi\cap\mathsf{FIV}(A)\subseteq\Xi'}{\mathcal{H}\vdash\ t\langle v^A_{\Xi'}{:=}r,s\rangle\equiv t'\langle v^A_{\Xi'}{:=}r,s'\rangle\colon C\{v^A_{\Xi'}\leftarrow r\}}\ \mathsf{Eq\text{-}}\langle\rangle$$

$$\frac{\mathcal{H}\vdash\ r\equiv s\colon A}{\mathcal{H}\vdash\ r+t\equiv s+t\colon A}\ \mathsf{Eq\text{-}}+_{\mathrm{L}}\qquad\frac{\mathcal{H}\vdash\ r\equiv s\colon A}{\mathcal{H}\vdash\ t+r\equiv t+s\colon A}\ \mathsf{Eq\text{-}}+_{\mathrm{R}}$$

$$\frac{\mathcal{H},\alpha^A\vdash\ s\equiv t\colon A}{\mathcal{H},\alpha^A\vdash\ [\alpha^A]s\equiv[\alpha^A]t\colon\bot}\ \mathsf{Eq\text{-}}[\alpha]\qquad\frac{\mathcal{H},\alpha^A\vdash\ s\equiv t\colon\bot}{\mathcal{H}\vdash\ \mu\alpha^A.s\equiv\mu\alpha^A.t\colon A}\ \mathsf{Eq\text{-}}\mu\alpha$$

$$\frac{\mathcal{H}\vdash\ s\equiv t\colon A\qquad i\notin\mathsf{FIV}(\mathcal{H})}{\mathcal{H}\vdash\ \mathsf{gen}_i(s)\equiv\mathsf{gen}_i(t)\colon\forall i.A}\ \mathsf{Eq\text{-}gen}$$

$$\frac{\mathcal{H}\vdash\ s\equiv t\colon\forall i.A}{\mathcal{H}\vdash\ \mathsf{ins}^E_i(s)\equiv\mathsf{ins}^E_i(t)\colon A\{i\leftarrow E\}}\ \mathsf{Eq\text{-}ins}$$

FIGURE 5. Equivalence and compatibility schemes.

also derivable in FOLP (Sec. 4) and also for Type Preservation (see validity variable substitution and its use in the reduction rule γ in Definition 5.11). The condition $\Xi\cap\mathsf{FIV}(A)\subseteq\Xi'$ prevents a proof of a formula with free individual variables to be used as proof of a formula where those variables are bound, as discussed in the introduction. The converse can be done safely (just like a proof of $\forall i.P(i)$ can be used to prove $P(i)$), which is why the inclusion is oriented in only one direction.

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 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 $\mathcal{H}$. The reason is that we seek to preserve the *theorems* of FOLP in FOHLP, in particular $[\![s]\!]A\supset[\![s+t]\!]A$, which places no restriction on t.

REMARK 3.6

In the derivation of a judgement $\Theta;\Gamma;\Delta\vdash D\,|\,s$ we assume the following **freshness condition**: for every pair of formulas A, B such that $x^A\in\Gamma$, $v^A_{\Xi}\in\Theta$ or $\alpha^A\in\Delta$:

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

That this entails no loss of generality is reflected in Lemma 3.12.

The schemes defining $\mathcal{H} \vdash s \equiv t : A$ encode equality of derivations as follows from proof normalization [5]. It should be mentioned that the resulting equational theory is **consistent** (Corollary 5.19) in the sense that there exist $\mathcal{H}, A, s$ and t s.t.

- $\mathcal{H} \vdash A \mid s$ is derivable;
- $\mathcal{H} \vdash A \mid t$ is derivable; and
- the judgement $\mathcal{H} \vdash s \equiv t : A$ is *not* derivable.

The schemes in Figure 5 ensure that proof witness equivalence is indeed an equivalence, and is compatible with all operators with the exception of '!'. Intuitively, a proof witness such as $!s$, of a formula such as $[[s]]_{\Xi} A$, supplies *intensional* information on how this formula is proved. For any proof witness t with $t \neq s$, the proof encoded by $!t$ is intensionally different from s and hence cannot be equated with it. In fact $!s$ and $!t$ prove different formulas (since $!t$ proves $[[t]]_{\Xi} A$). This does not present an obstacle for proof normalization 'under' a box type constuctor since the introduction scheme for $\Box$I includes the judgement on proof witness equivalence (*cf.* case of internal reduction reduction under a '!' in Proposition 5.14).

3.1 Basic results

In this section we use $\rhd \Theta; \Gamma; A \vdash \Delta \mid s$ as shorthand for derivability in FOHLP, written $\rhd_{\mathsf{FOHLP}} \Theta; \Gamma; A \vdash \Delta \mid s$. This applies to all judgements in the statements of the results presented below.

LEMMA 3.7 (Weakening and Strengthening)
Suppose $\rhd \Theta; \Gamma; A \vdash \Delta \mid s$. Then:

(1) $\rhd \Theta \cup \Theta'; \Gamma \cup \Gamma'; A \vdash \Delta \cup \Delta' \mid s$; and
(2) $\rhd \Theta \cap \mathsf{FVV}(s); \Gamma \cap \mathsf{FVT}(s); A \vdash \Delta \cap \mathsf{FVF}(s) \mid s$.

LEMMA 3.8 (Weakening for proof witness equivalence)
Suppose $\rhd \Theta; \Gamma; \Delta \vdash s \equiv t : A$. Then also $\rhd \Theta \cup \Theta'; \Gamma \cup \Gamma'; \Delta \cup \Delta' \vdash s \equiv t : A$.

The following *substitution principles* hold.

LEMMA 3.9 (Validity Variable Substitution)
(1) If $\rhd \Theta, v^A_\Xi; \Gamma; \Delta \vdash B \mid s$ and $\rhd \Theta; \cdot; \cdot \vdash A \mid t$, then $\rhd \Theta; \Gamma; \Delta \vdash B\{v^A_\Xi \leftarrow t\} \mid s\{v^A_\Xi \leftarrow t\}$.
(2) If $\rhd \Theta, v^A_\Xi; \Gamma; \Delta \vdash s \equiv r : B$ and $\rhd \Theta; \cdot; \cdot \vdash A \mid t$, then $\rhd \Theta; \Gamma; \Delta \vdash s\{v^A_\Xi \leftarrow t\} \equiv r\{v^A_\Xi \leftarrow t\} : B\{v^A_\Xi \leftarrow t\}$.

LEMMA 3.10 (Individual Variable Substitution)
(1) If $\rhd \Theta; \Gamma; \Delta \vdash D \mid r$, then $\rhd \Theta\{i \leftarrow E\}; \Gamma\{i \leftarrow E\}; \Delta\{i \leftarrow E\} \vdash D\{i \leftarrow E\} \mid r\{i \leftarrow E\}$.
(2) If $\rhd \Theta; \Gamma; \Delta \vdash r_1 \equiv r_2 : D$, then $\rhd \Theta\{i \leftarrow E\}; \Gamma\{i \leftarrow E\}; \Delta\{i \leftarrow E\} \vdash r_1\{i \leftarrow E\} \equiv r_2\{i \leftarrow E\} : D\{i \leftarrow E\}$.

LEMMA 3.11
If $\rhd \Theta; \Gamma; \Delta \vdash s \equiv t : D$, then both $\rhd \Theta; \Gamma; \Delta \vdash D \mid s$ and $\rhd \Theta; \Gamma; \Delta \vdash D \mid t$.

LEMMA 3.12
If $\rhd \Theta; \Gamma, z^B; \Delta \vdash D \mid s$, then there is a proof witness s' such that $\rhd \Theta; \Gamma, y^B; \Delta \vdash D \mid s'$ with y^B a fresh variable.

Similarly, if $\rhd \Theta;\Gamma;\Delta,\alpha^{B} \vdash D|s$, then there is a proof witness s' such that $\rhd \Theta;\Gamma;\Delta,\beta^{B} \vdash D|s'$ with β^{B} a fresh variable.

4 Relating FOLP and FOHLP

All theorems of FOLP can be proved in FOHLP (Section 4.1). This may be shown by introducing a simple translation from formulas in FOLP to formulas of FOHLP and then transforming a proof of theorem A in FOLP to a proof of the translation of A in FOHLP. The reverse translation is more complicated (Section 4.2). Several issues arise when translating proof witnesses. One of them is the translation of lambda abstraction and name abstraction; these must be simulated in FOLP. The other is the translation of the bang and the unbox proof witness constructors; here the problem is upholding the role of variables as registered in the decoration of the modality. These issues require that the reverse translation have as target a simple variant of FOLP that consists in adding a number of FOLP theorems as axioms (cf. Definition 4.3). The new axioms allow **Nec.** to apply to them too.

4.1 From FOLP to FOHLP

Let π be a FOLP-proof. We introduce a simple translation $\underline{\bullet}_{\pi}$, parameterized over π, from formulas in FOLP to those in FOHLP. The derivation π is used to determine the (finite) constant specification $\mathcal{C}_{\pi}$ and, from this, the translation of the constants. For technical convenience, we assume that the formulas in $\mathcal{C}_{\pi}$ are ordered. We define $\mathcal{C}_{\pi}(c) \triangleq \{A \,|\, [[c]]_{\emptyset}A \in \mathcal{C}_{\pi}\}$. Note that $\mathcal{C}_{\pi}(c)$ consists of formulas that are instances of axioms of FOLP. We write $\langle \mathbf{B1}, x^{B}, \Xi, B\rangle$ to denote a proof witness (Figure 6) associated with the formula $([[x^{B}]]_{\Xi}B) \supset B$, the instance of axiom **B1** in the language of FOHLP obtained from instantiating its metavariables (in order of appearance) with x^{B}, Ξ and B, resp. Similar notation is used for the instances of other axiom schemes. If we know that A is an instance of an axiom, we write $\langle A\rangle$ to denote its unique[6] decomposition in terms of the associated axiom scheme and instance variables. For example, $\langle([[x^{B}]]_{\Xi}B) \supset B\rangle = \langle \mathbf{B1}, x^{B}, \Xi, B\rangle$. Translation of formulas and proof terms are defined by mutual recursion.

Definition 4.1
The translation $\underline{\bullet}_{\pi}$ from FOLP proof terms and formulas to FOHLP proof witnesses and formulas is defined as follows:

$$
\begin{array}{rcl@{\qquad}rcl}
\underline{E}_{\pi} & \triangleq & E & \underline{c}_{\pi} & \triangleq & \underline{\langle A_1\rangle}_{\pi} + \ldots + \underline{\langle A_n\rangle}_{\pi} \\
\underline{P(E_1,\ldots,E_n)}_{\pi} & \triangleq & P(E_1,\ldots,E_n) & \underline{x^{A}}_{\pi} & \triangleq & x^{\underline{A}_{\pi}} \\
\underline{\bot}_{\pi} & \triangleq & \bot & \underline{s \cdot t}_{\pi} & \triangleq & \underline{s}_{\pi} \cdot \underline{t}_{\pi} \\
\underline{A \supset B}_{\pi} & \triangleq & \underline{A}_{\pi} \supset \underline{B}_{\pi} & \underline{!s}_{\pi} & \triangleq & !\underline{s}_{\pi} \\
\underline{[[s]]_{\Xi}A}_{\pi} & \triangleq & [[\underline{s}_{\pi}]]_{\Xi}\underline{A}_{\pi} & \underline{s+t}_{\pi} & \triangleq & \underline{s}_{\pi} + \underline{t}_{\pi} \\
\underline{\forall i.A}_{\pi} & \triangleq & \forall i.\underline{A}_{\pi} & \underline{\mathsf{gen}_i(s)}_{\pi} & \triangleq & \mathsf{gen}_i(\underline{s}_{\pi}),
\end{array}
$$

where $\mathcal{C}_{\pi}(c) = \{A_1,\ldots,A_n\}$ and:

[6] There is one exception to uniqueness due to the overlap between axioms **B3a** and **B3b**, namely in the case of $[[s]]_{\Xi}A \supset [[s+s]]_{\Xi}A$. In this case, we always select **B3a** over **B3b**.

$$\begin{array}{rcl}
\langle \mathbf{A1a}, A, B\rangle & \triangleq & (\lambda x^A.\lambda y^B.x^A) \\
\langle \mathbf{A1b}, A, B, C\rangle & \triangleq & (\lambda x^{A\supset B\supset C}.\lambda y^{A\supset B}.\lambda z^A.x^{A\supset B\supset C}\cdot z^A\cdot (y^{A\supset B}\cdot z^A)) \\
\langle \mathbf{A1c}, A\rangle & \triangleq & (\lambda y^{\neg\neg A}.\mu\alpha^A.y^{\neg\neg A}\cdot \lambda x^A.[\alpha^A]x^A) \\
\langle \mathbf{A1d}, A, i, E\rangle & \triangleq & \lambda x^{\forall i.A}.\mathsf{ins}_i^E(x^{\forall i.A}) \\
\langle \mathbf{A1e}, A, B, i\rangle & \triangleq & \lambda x^{\forall i.A\supset B}.\lambda y^{\forall i.A}.\mathsf{gen}_j(\mathsf{ins}_i^j(x^{\forall i.(A\supset B)})\cdot \mathsf{ins}_i^j(y^{\forall i.A})) \\
\langle \mathbf{A1f}, A, i\rangle & \triangleq & \lambda x^A.\mathsf{gen}_i(x^A) \\
\langle \mathbf{A2}, t, \Xi, i, A\rangle & \triangleq & \lambda x^{[\![t]\!]_{\Xi,i}A}.!v^A_\Xi\langle v^A_\Xi{:=}t, x^{[\![t]\!]_{\Xi,i}A}\rangle \\
\langle \mathbf{A3}, t, \Xi, i, A\rangle & \triangleq & \lambda x^{[\![t]\!]_\Xi A}.!v^A_{\Xi,i}\langle v^A_{\Xi,i}{:=}t, x^{[\![t]\!]_\Xi A}\rangle \\
\langle \mathbf{B1}, t, \Xi, A\rangle & \triangleq & \lambda x^{[\![t]\!]_\Xi A}.v^A_\Xi\langle v^A_\Xi{:=}t, x^{[\![t]\!]_\Xi A}\rangle \\
\langle \mathbf{B2}, s, \Xi, A, B, t\rangle & \triangleq & \lambda x^{[\![s]\!]_\Xi A\supset B}.\lambda y^{[\![t]\!]_\Xi A}.!(w^{A\supset B}_\Xi\cdot v^A_\Xi)\langle w^{A\supset B}_\Xi{:=}s, x^{[\![s]\!]_\Xi A\supset B}\rangle\langle v^A_\Xi{:=}t, y^{[\![t]\!]_\Xi A}\rangle \\
\langle \mathbf{B3a}, s, \Xi, A, t\rangle & \triangleq & \lambda x^{[\![s]\!]_\Xi A}.!(v^A_\Xi + t)\langle v^A_\Xi{:=}s, x^{[\![s]\!]_\Xi A}\rangle \\
\langle \mathbf{B3b}, t, \Xi, A, s\rangle & \triangleq & \lambda x^{[\![t]\!]_\Xi A}.!(s + v^A_\Xi)\langle v^A_\Xi{:=}t, x^{[\![s]\!]_\Xi A}\rangle \\
\langle \mathbf{B4}, s, \Xi, A\rangle & \triangleq & \lambda x^{[\![s]\!]_\Xi A}.!!v^A_\Xi\langle v^A_\Xi{:=}s, x^{[\![s]\!]_\Xi A}\rangle \\
\langle \mathbf{B5}, t, \Xi, A, i\rangle & \triangleq & \lambda x^{[\![t]\!]_\Xi A}.!\mathsf{gen}_i(v^A_\Xi)\langle v^A_\Xi{:=}t, x^{[\![t]\!]_\Xi A}\rangle
\end{array}$$

FIGURE 6. Translation of proof constants to proof witnesses.

$$\begin{array}{rclrcl}
\underline{\langle \mathbf{A1a}, A, B\rangle}_\pi & \triangleq & \langle \mathbf{A1a}, \underline{A}_\pi, \underline{B}_\pi\rangle & \underline{\langle \mathbf{A3}, t, \Xi, i, A\rangle}_\pi & \triangleq & \langle \mathbf{A3}, \underline{t}_\pi, \Xi, i, \underline{A}_\pi\rangle \\
\underline{\langle \mathbf{A1b}, A, B, C\rangle}_\pi & \triangleq & \langle \mathbf{A1b}, \underline{A}_\pi, \underline{B}_\pi, \underline{C}_\pi\rangle & \underline{\langle \mathbf{B1}, t, \Xi, A\rangle}_\pi & \triangleq & \langle \mathbf{B1}, \underline{t}_\pi, \Xi, \underline{A}_\pi\rangle \\
\underline{\langle \mathbf{A1c}, A\rangle}_\pi & \triangleq & \langle \mathbf{A1c}, \underline{A}_\pi\rangle & \underline{\langle \mathbf{B2}, s, \Xi, A, B, t\rangle}_\pi & \triangleq & \langle \mathbf{B2}, \underline{s}_\pi, \Xi, \underline{A}_\pi, \underline{B}_\pi, \underline{t}_\pi\rangle \\
\underline{\langle \mathbf{A1d}, A, i, E\rangle}_\pi & \triangleq & \langle \mathbf{A1d}, \underline{A}_\pi, i, E\rangle & \underline{\langle \mathbf{B3a}, s, \Xi, A, t\rangle}_\pi & \triangleq & \langle \mathbf{B3a}, \underline{s}_\pi, \Xi, \underline{A}_\pi, \underline{t}_\pi\rangle \quad , \\
\underline{\langle \mathbf{A1e}, A, B, i\rangle}_\pi & \triangleq & \langle \mathbf{A1e}, \underline{A}_\pi, \underline{B}_\pi, i\rangle & \underline{\langle \mathbf{B3b}, t, \Xi, A, s\rangle}_\pi & \triangleq & \langle \mathbf{B3b}, \underline{t}_\pi, \Xi, \underline{A}_\pi, \underline{s}_\pi\rangle \\
\underline{\langle \mathbf{A1f}, A, i\rangle}_\pi & \triangleq & \langle \mathbf{A1f}, \underline{A}_\pi, i\rangle & \underline{\langle \mathbf{B4}, s, \Xi, A\rangle}_\pi & \triangleq & \langle \mathbf{B4}, \underline{s}_\pi, \Xi, \underline{A}_\pi\rangle \\
\underline{\langle \mathbf{A2}, t, \Xi, i, A\rangle}_\pi & \triangleq & \langle \mathbf{A2}, \underline{t}_\pi, \Xi, i, \underline{A}_\pi\rangle & \underline{\langle \mathbf{B5}, t, \Xi, A, i\rangle}_\pi & \triangleq & \langle \mathbf{B5}, \underline{t}_\pi, \Xi, \underline{A}_\pi, i\rangle
\end{array}$$

Also, we define $\underline{\Gamma}_\pi \triangleq \{x^{\underline{A}_\pi} \mid x^A \in \Gamma\}$.

PROPOSITION 4.2
$\rhd_{\mathsf{FOLP}}\, \Gamma \vdash A$ implies $\rhd_{\mathsf{FOHLP}}\, \cdot; \underline{\Gamma}_\pi; \cdot \vdash \underline{A}_\pi \mid s$, for some proof witness s.

The proof is by induction on the derivation π of $\Gamma \vdash A$; sample cases of the key axioms (**A2**, **A3** and **B5**) and **Nec** are:

- **A2.** $([[t]]_{\Xi,i}A) \supset [[t]]_\Xi A$, if $i \notin \mathsf{FIV}(A)$.

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

The restriction for $\Box\mathsf{I}$ holds, since $\Xi \cap \mathsf{FIV}(A) \subseteq \Xi$. That of $\Box\mathsf{E}$ holds, since $\Xi, i \cap \mathsf{FIV}(A) \subseteq \Xi$ because $i \notin \mathsf{FIV}(A)$.

- **A3.** $([[t]]_\Xi A)\supset[[t]]_{\Xi,i}A$.

$$\dfrac{\dfrac{}{\cdot;x^{[[t]]_\Xi A};\cdot\vdash[[t]]_\Xi A\,|\,x^{[[t]]_\Xi A}}\,\mathsf{Var}\qquad\dfrac{\dfrac{}{v^A_{\Xi,i};\cdot;\cdot\vdash A\,|\,v^A_{\Xi,i}}\,\mathsf{VarM}}{v^A_{\Xi,i};x^{[[t]]_\Xi A};\cdot\vdash[[v^A_{\Xi,i}]]_{\Xi,i}A\,|\,!v^A_{\Xi,i}}\,\Box\mathsf{I}}{\dfrac{\cdot;x^{[[t]]_\Xi A};\cdot\vdash[[t]]_{\Xi,i}A\,|\,!v^A_{\Xi,i}\langle v^A_{\Xi,i}{:=}t,x^{[[t]]_\Xi A}\rangle}{\cdot;\cdot;\cdot\vdash([[t]]_\Xi A)\supset[[t]]_{\Xi,i}A\,|\,\lambda x^{[[t]]_\Xi A}.!v^A_{\Xi,i}\langle v^A_{\Xi,i}{:=}t,x^{[[t]]_\Xi A}\rangle}\,\supset\mathsf{I}}\,\Box\mathsf{E}$$

  The derivation is almost identical to that for **A2**, exchanging the occurrences of Ξ and Ξ,i. The restriction for $\Box\mathsf{I}$ holds, since $\Xi,i\cap\mathsf{FIV}(A)\subseteq\Xi,i$. The restriction for $\Box\mathsf{E}$ holds, since $\Xi\cap\mathsf{FIV}(A)\subseteq\Xi,i$.

- **B5.** $([[t]]_\Xi A)\supset[[\mathsf{gen}_i(t)]]_\Xi\forall i.A$, if $i\notin\Xi$.

$$\dfrac{\dfrac{}{\cdot;x^{[[t]]_\Xi A};\cdot\vdash[[t]]_\Xi A\,|\,x^{[[t]]_\Xi A}}\,\mathsf{Var}\qquad\dfrac{\dfrac{\dfrac{}{v^A_\Xi;\cdot;\cdot\vdash A\,|\,v^A_\Xi}\,\mathsf{VarM}}{v^A_\Xi;\cdot;\cdot\vdash\forall i.A\,|\,\mathsf{gen}_i(v^A_\Xi)}\,\forall\mathsf{I}}{v^A_\Xi;x^{[[t]]_\Xi A};\cdot\vdash[[\mathsf{gen}_i(v^A_\Xi)]]_\Xi\forall i.A\,|\,!\mathsf{gen}_i(v^A_\Xi)}\,\Box\mathsf{I}}{\dfrac{\cdot;x^{[[t]]_\Xi A};\cdot\vdash[[\mathsf{gen}_i(t)]]_\Xi\forall i.A\,|\,!\mathsf{gen}_i(v^A_\Xi)\langle v^A_\Xi{:=}t,x^{[[t]]_\Xi A}\rangle}{\cdot;\cdot;\cdot\vdash([[t]]_\Xi A)\supset[[\mathsf{gen}_i(t)]]_\Xi\forall i.A\,|\,\lambda x^{[[t]]_\Xi A}.!\mathsf{gen}_i(v^A_\Xi)\langle v^A_\Xi{:=}t,x^{[[t]]_\Xi A}\rangle}\,\supset\mathsf{I}}\,\Box\mathsf{E}$$

  The restriction for $\forall\mathsf{I}$ holds, since $i\notin\Xi$. That of $\Box\mathsf{I}$ holds, since $\Xi\cap\mathsf{FIV}(\forall i.A)\subseteq\Xi$. Finally, that of $\Box\mathsf{E}$ holds, since $\Xi\cap\mathsf{FIV}(A)\subseteq\Xi$.

- **Nec**. Then π is of the form $\vdash[[c]]A$, with A an instance of an axiom scheme. Note that, if $\mathcal{C}_\pi(c)=\{A_1,\ldots,A_n\}$, then $A=A_i$ for some $i\in 1..n$. In this case, it is easy to verify that the judgement: $\cdot;\cdot;\cdot\vdash\underline{A_i}_\pi\,|\,\underline{\langle A_i\rangle}_\pi$ can be derived (recall that the proof witness $\underline{\langle A\rangle}_\pi$ is defined in Figure 6). Therefore,

$$\dfrac{\dfrac{\cdot;\cdot;\cdot\vdash\underline{A_i}_\pi\,|\,\underline{\langle A_i\rangle}_\pi}{\cdot;\cdot;\cdot\vdash\underline{A_i}_\pi\,|\,\underline{\langle A_1\rangle}_\pi+\ldots+\underline{\langle A_n\rangle}_\pi}\,(\mathsf{PlusL},\mathsf{PlusR})^*}{\cdot;\cdot;\cdot\vdash[[\underline{\langle A_1\rangle}_\pi+\ldots+\underline{\langle A_n\rangle}_\pi]]\underline{A_i}_\pi\,|\,!(\underline{\langle A_1\rangle}_\pi+\ldots+\underline{\langle A_n\rangle}_\pi)}\,\Box\mathsf{I}$$

4.2 *From FOHLP to FOLP*

We first introduce *Extended* FOLP (EFOLP) which serves as target of our translation, and then address the translation itself. EFOLP differs from FOLP in that some theorems of FOLP are adopted as axioms. Let $S\overset{\vec{i}}{\Rightarrow}T$ be shorthand for $(\vec{i}\cap S)\subseteq T$ and $S\overset{\vec{i}}{\Rightarrow}\neg T$ be shorthand for $\vec{i}\cap S\cap T=\emptyset$. EFOLP is defined as follows.

Definition 4.3 (EFOLP)
The proof terms and formulas of EFOLP are exactly those of FOLP (Definition 2.1). The axiom and inference schemes are those of FOLP (Definition 2.5) modified as follows:

(1) The following two axiom schemes:

A1a.	$A\supset B\supset A$	
A1b.	$(A\supset B\supset C)\supset(A\supset B)\supset A\supset C$	
A1c.	$\neg\neg A\supset A$	
A1dd.	$(\forall\vec{j}.\forall\vec{i}.A)\supset\forall\vec{j}.(A\{\vec{i}\leftarrow\vec{E}\})$	
A1e.	$(\forall i.(A\supset B))\supset(\forall i.A)\supset\forall i.B$	
A1ff.	$\forall\vec{j}.A\supset\forall\vec{j}.\forall i.A,$	if $i\notin\mathsf{FIV}(A)$
A1g.	$\forall\vec{i}.A\supset\forall\vec{j}.A,$	if $\vec{j}$ is a permutation of $\vec{i}$
A1h.	$\forall\vec{i}.A\supset\forall\vec{j}.A,$	$\mathsf{FIV}(A)\overset{\vec{j}}{\Rightarrow}\vec{i}$
A1i.	$\forall\vec{i}.(A\supset B)\supset\forall\vec{j}.A\supset\forall\vec{k}.B,$	$\mathsf{FIV}(A)\overset{\vec{j}}{\Rightarrow}\vec{i},\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\vec{i},(\mathsf{FIV}(A)\cap\mathsf{FIV}(B))\overset{\vec{k}}{\Rightarrow}\vec{j}$
A2.	$(\llbracket t\rrbracket_{\Xi,i}A)\supset\llbracket t\rrbracket_{\Xi}A,$	if $i\notin\mathsf{FIV}(A)$
A3.	$(\llbracket t\rrbracket_{\Xi}A)\supset\llbracket t\rrbracket_{\Xi,i}A$	
A4.	$A\supset A$	
A5.	$A\supset(\llbracket t\rrbracket_{\Xi}B\supset B)$	
A6.	$A\supset(\forall\vec{i}.B\supset B)$	
A7.	$\forall\vec{i}.(A\supset B)\supset\llbracket s\rrbracket_{\Xi}A\supset\forall\vec{k}.B,$	$\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\vec{i},\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\neg\Xi,\mathsf{FIV}(A)\backslash\Xi\subseteq\vec{i}$
A8.	$\llbracket s\rrbracket_{\Xi}A\supset\forall\vec{i}.A,$	$\mathsf{FIV}(A)\overset{\vec{i}}{\Rightarrow}\neg\Xi$
A9.	$\llbracket s\rrbracket_{\Xi}(A\supset B)\supset\forall\vec{j}.A\supset\forall\vec{k}.B$	$\mathsf{FIV}(A)\overset{\vec{j}}{\Rightarrow}\neg\Xi,\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\neg\Xi,(\mathsf{FIV}(A)\cap\mathsf{FIV}(B))\overset{\vec{k}}{\Rightarrow}\vec{j}$
B1.	$(\llbracket t\rrbracket_{\Xi}A)\supset A$	
B2.	$(\llbracket s\rrbracket_{\Xi}(A\supset B))\supset(\llbracket t\rrbracket_{\Xi}A)\supset\llbracket(s\cdot t)\rrbracket_{\Xi}B$	
B3a.	$(\llbracket s\rrbracket_{\Xi}A)\supset\llbracket(s+t)\rrbracket_{\Xi}A$	
B3b.	$(\llbracket t\rrbracket_{\Xi}A)\supset\llbracket(s+t)\rrbracket_{\Xi}A$	
B4.	$(\llbracket t\rrbracket_{\Xi}A)\supset\llbracket !t\rrbracket_{\Xi}\llbracket t\rrbracket_{\Xi}A$	
B5.	$(\llbracket t\rrbracket_{\Xi}A)\supset\llbracket\mathsf{gen}_i(t)\rrbracket_{\Xi}\forall i.A,$	if $i\notin\Xi$

FIGURE 7. Axiom schemes of EFOLP.

A1d. $(\forall i.A)\supset A\{i\leftarrow E\}$

A1f. $A\supset\forall i.A,\qquad$ if $i\notin\mathsf{FIV}(A)$

are replaced by more general ones:

A1dd. $(\forall\vec{j}.\forall\vec{i}.A)\supset\forall\vec{j}.(A\{\vec{i}\leftarrow\vec{E}\})$

A1ff. $\forall\vec{j}.A\supset\forall\vec{j}.\forall i.A,\qquad$ if $i\notin\mathsf{FIV}(A)$

(2) The following new axiom schemes are added:

A1g. $\forall\vec{i}.A\supset\forall\vec{j}.A,\qquad$ if $\vec{j}$ is a permutation of $\vec{i}$

A1h. $\forall\vec{i}.A\supset\forall\vec{j}.A,\qquad\mathsf{FIV}(A)\overset{\vec{j}}{\Rightarrow}\vec{i}$

A1i. $\forall\vec{i}.(A\supset B)\supset\forall\vec{j}.A\supset\forall\vec{k}.B,\qquad\mathsf{FIV}(A)\overset{\vec{j}}{\Rightarrow}\vec{i},\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\vec{i},(\mathsf{FIV}(A)\cap\mathsf{FIV}(B))\overset{\vec{k}}{\Rightarrow}\vec{j}$

A4. $A\supset A$

A5. $A\supset([[t]]_{\Xi}B\supset B)$

A6. $A\supset(\forall\vec{i}.B\supset B)$

A7. $\forall\vec{i}.(A\supset B)\supset[[s]]_{\Xi}A\supset\forall\vec{j}.B,\qquad\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\vec{i},\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\neg\Xi,\mathsf{FIV}(A)\backslash\Xi\subseteq\vec{i}$

A8. $[[s]]_{\Xi}A\supset\forall\vec{i}.A,\qquad\mathsf{FIV}(A)\overset{\vec{i}}{\Rightarrow}\neg\Xi$

A9. $[[s]]_{\Xi}(A\supset B)\supset\forall\vec{j}.A\supset\forall\vec{k}.B\qquad\mathsf{FIV}(A)\overset{\vec{j}}{\Rightarrow}\neg\Xi,\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\neg\Xi,(\mathsf{FIV}(A)\cap\mathsf{FIV}(B))\overset{\vec{k}}{\Rightarrow}\vec{j}$

The full set of axiom schemes is given in Figure 7. Note that they are all theorems of FOLP.

Lemma 4.4
All EFOLP-axioms are FOLP-theorems.

Just like FOLP, EFOLP enjoys internalization of its own derivations. Our formulation below is a slight variant of the Internalization Theorem mentioned in Section 2.1. It differs with respect to it in that the set of free individual variables depends on the formula rather than the hypotheses used to prove it. This eases some proofs (*eg*. Proposition 4.16). If $\Gamma = A_1, \ldots A_n$, then a context of the form $[[u_1]]_{\Xi_1} A_1, \ldots, [[u_n]]_{\Xi_n} A_n$ is referred to as $[[\vec{u}]]_{\vec{\Xi}}\Gamma$. The proof of Lemma 4.5 is by induction on the derivation of $[[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash D$.

Lemma 4.5 (Internalization for EFOLP)
$\rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash D$ implies there exists a proof term r such that $\rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[r]]_{\vec{\Xi}} D$.

Corollary 4.6
$\rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash D$ implies there exists a $r^{\vec{\Xi},D}$ such that $\rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[r^{\vec{\Xi},D}]]_{\vec{\Xi}\cap \mathsf{FIV}(D)} D$.

Proof. Since $[[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[r]]_{\vec{\Xi}} D$ is derivable for some r by Internalization, we can obtain $[[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[r]]_{\vec{\Xi}\cap \mathsf{FIV}(D)} D$ by using **A2** and **MP** as many times as necessary. Take $r^{\vec{\Xi},D} = r$. ■

4.2.1 Stripping and λ-Abstraction in EFOLP

The main property of EFOLP that we require for our translation is the *Stripping Lemma* (Lemma 4.11). It states that if π is a EFOLP-derivation of $\Gamma, x^{[[y^A]]_{\Xi} A} \vdash B$ and $y^A \notin \Gamma$, then there is a EFOLP-derivation π' of $\Gamma, y^A \vdash B_{y^A}$. Here B_{y^A} means stripping B of all modalities whose associated proof term has y^A among its free variables and replacing these modalities by universal quantification over an appropriate set of individial variables.

Definition 4.7
The result of stripping a variable x^C from a formula A, denoted A_{x^C}, is defined inductively as follows:

$$\begin{aligned}
P(E_1, \ldots, E_n)_{x^C} &\triangleq P(E_1, \ldots, E_n) \\
\bot_{x^C} &\triangleq \bot \\
(A \supset B)_{x^C} &\triangleq A_{x^C} \supset B_{x^C} \\
([[s]]_{\Xi} A)_{x^C} &\triangleq \begin{cases} \forall \vec{i}.A_{x^C}, & \text{if } x^C \in \mathsf{FV}(s) \\ [[s]]_{\Xi} A_{x^C}, & \text{otherwise} \end{cases} \\
& \quad \text{where } \vec{i} \triangleq \mathsf{FIV}(A) \setminus \Xi \\
(\forall i.A)_{x^C} &\triangleq \forall i.A_{x^C}
\end{aligned}$$

Stripping does not introduce new free individual variables as may be verified by induction on A:

Lemma 4.8
$\mathsf{FIV}(A_{x^C}) \subseteq \mathsf{FIV}(A)$.

The Stripping Lemma is a key ingredient of the λ-*Abstraction Lemma* (Lemma 4.12) which will allow us to internalise the hypothetical reasoning of FOHLP in EFOLP. A detailed account of the role this lemma plays in our translation is given in Section 4.2.2. The rest of this subsection presents some preliminary results required to prove both the Stripping and the λ-Abstraction lemmas.

Lemma 4.9
Suppose $S' \subseteq S$. Then

(1) $S \xRightarrow{\vec{j}} T$ implies $S' \xRightarrow{\vec{j}} T$
(2) $S \xRightarrow{\vec{j}} \neg T$ implies $S' \xRightarrow{\vec{j}} \neg T$

Proof. Immediate from the definition of $S \xRightarrow{\vec{j}} T$ and $S \xRightarrow{\vec{j}} \neg T$. ∎

Lemma 4.10
Let A be an axiom of EFOLP and let x^B be a variable. Then A_{x^B} is an axiom of EFOLP.

Proof. We consider each axiom scheme.

- **A1**. A is one of the following

A1a.	$A \supset B \supset A$	
A1b.	$(A \supset B \supset C) \supset (A \supset B) \supset A \supset C$	
A1c.	$\neg\neg A \supset A$	
A1d.	$(\forall i.A) \supset A\{i \leftarrow E\}$	
A1dd.	$(\forall \vec{j}.\forall \vec{i}.A) \supset \forall \vec{j}.(A\{\vec{i} \leftarrow \vec{E}\})$	
A1e.	$(\forall i.(A \supset B)) \supset (\forall i.A) \supset \forall i.B$	
A1f.	$A \supset \forall i.A,$	if $i \notin \mathsf{FIV}(A)$
A1ff.	$\forall \vec{j}.A \supset \forall \vec{j}.\forall i.A,$	if $i \notin \mathsf{FIV}(A)$
A1g.	$\forall \vec{i}.A \supset \forall \vec{j}.A,$	if $\vec{j}$ is a permutation of $\vec{i}$
A1h.	$\forall \vec{i}.A \supset \forall \vec{j}.A,$	$\mathsf{FIV}(A) \xRightarrow{\vec{j}} \vec{i}$
A1i.	$\forall \vec{i}.(A \supset B) \supset \forall \vec{j}.A \supset \forall \vec{k}.B$	if $\mathsf{FIV}(A) \xRightarrow{\vec{j}} \vec{i}, \mathsf{FIV}(B) \xRightarrow{\vec{k}} \vec{i}, (\mathsf{FIV}(A) \cap \mathsf{FIV}(B)) \xRightarrow{\vec{k}} \vec{j}.$

  These cases are all immediate except for those that include side conditions on free individual variables, namely **A1ff**, **A1h** and **A1i**. For the former we proceed as follows. First note that A_{x^B} is of the form $\forall j.A' \supset \forall j.\forall i.A'$, for $A' = A_{x^B}$. Thus we must check that $i \notin \mathsf{FIV}(A')$. This follows from Lemma 4.8 and $i \notin \mathsf{FIV}(A)$. **A1h** is similar, except that we resort to both Lemma 4.8 and Lemma 4.9(1).
  In **A1i**, A_{x^B} is of the form $\forall \vec{i}.(A' \supset B') \supset \forall \vec{j}.A' \supset \forall \vec{k}.B'$. This is an instance of **A1i**. The associated conditions follow from $\mathsf{FIV}(A) \xRightarrow{\vec{j}} \vec{i}$, $\mathsf{FIV}(B) \xRightarrow{\vec{k}} \vec{i}$, $(\mathsf{FIV}(A) \cap \mathsf{FIV}(B)) \xRightarrow{\vec{k}} \vec{j}$, Lemma 4.8 and Lemma 4.9(1).
- **A2.** A is $[[t]]_{\Xi,i} A \supset [[t]]_{\Xi} A$, where $i \notin \mathsf{FIV}(A)$. In this case A_{x^B} must be of the one of the forms
  - $[[t]]_{\Xi,i} A' \supset [[t]]_{\Xi} A'$. This is an instance of **A2**, given that $i \notin \mathsf{FIV}(A')$ as follows from Lemma 4.8.
  - $\forall \vec{j}.A' \supset \forall \vec{j}.A'$. Note that here we have the same prefix $\forall \vec{j}$ to the left and right of $\supset$ given that $i \notin \mathsf{FIV}(A)$. This formula is an instance of **A4**.
- **A3.** A is $[[t]]_{\Xi} A \supset [[t]]_{\Xi,i} A$. In this case A_{x^B} must be of one of the forms
  - $[[t]]_{\Xi} A' \supset [[t]]_{\Xi,i} A'$. This is an instance of **A3**.
  - $\forall \vec{j}.A' \supset \forall \vec{j}.A'$, with $i \in \Xi$. This is an instance of **A4**.
  - $\forall \vec{j_1}, i, \vec{j_2}.A' \supset \forall \vec{j_1}, \vec{j_2}.A'$, where $i \notin \Xi$ and $i \in \mathsf{FIV}(A)$. This is an instance of **A1d**.
  - $\forall \vec{j}.A' \supset \forall \vec{j}.A'$ assuming $i \notin \Xi$ and $i \notin \mathsf{FIV}(A)$. This is an instance of **A4**.

- **A4.** A is $A\supset A$. In this case, A_{x^B} is an instance of **A4** itself.
- **A5.** A is $A\supset([\![t]\!]_\Xi B\supset B)$. In this case, A_{x^B} is of one of the forms
  - $A'\supset([\![t]\!]_\Xi B'\supset B')$. This is an instance of **A5**.
  - $A'\supset(\forall\vec{i}.B'\supset B')$, where $\vec{i}=\mathsf{FIV}(B)\backslash\Xi$. This formula is an instance of **A6**.
- **A6.** A is $A\supset(\forall\vec{i}.B\supset B)$. In this case, A_{x^B} is of the form $A'\supset(\forall\vec{i}.B'\supset B')$ and hence an instance of **A6** itself.
- **A7.** A is $\forall\vec{i}.(A\supset B)\supset[\![s]\!]_\Xi A\supset\forall\vec{k}.B$, with $\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\vec{i},\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\neg\Xi$ and $\mathsf{FIV}(A)\backslash\Xi\subseteq\vec{i}$. In this case, A_{x^B} is of one of the forms
  - $\forall\vec{i}.(A'\supset B')\supset[\![s]\!]_\Xi A'\supset\forall\vec{k}.B'$. To verify that this is an instance of **A7**, we must check the conditions $\mathsf{FIV}(B')\overset{\vec{k}}{\Rightarrow}\vec{i},\mathsf{FIV}(B')\overset{\vec{k}}{\Rightarrow}\neg\Xi$ and $\mathsf{FIV}(A')\backslash\Xi\subseteq\vec{i}$. They all follow from the hypotheses and Lemma 4.8.
  - $\forall\vec{i}.(A'\supset B')\supset\forall\vec{j}.A'\supset\forall\vec{k}.B'$, where $\vec{j}=\mathsf{FIV}(A)\backslash\Xi$. This is an instance of **A1i**. For this we must verify that $\mathsf{FIV}(A')\overset{\vec{j}}{\Rightarrow}\vec{i}$, $\mathsf{FIV}(B')\overset{\vec{k}}{\Rightarrow}\vec{i}$ and $(\mathsf{FIV}(A')\cap\mathsf{FIV}(B'))\overset{\vec{k}}{\Rightarrow}\vec{j}$. The first condition follows from the definition of $\vec{j}$ (recall from above that $\vec{j}=\mathsf{FIV}(A)\backslash\Xi$), the hypothesis $\mathsf{FIV}(A)\backslash\Xi\subseteq\vec{i}$ and Lemma 4.8. The second condition follows from $\mathsf{FIV}(B')\overset{\vec{k}}{\Rightarrow}\vec{i}$ and Lemma 4.8. The last condition follows from the definition of $\vec{j}$, the hypothesis $\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\neg\Xi$ – since $\vec{k}\cap\mathsf{FIV}(B)\cap\mathsf{FIV}(A)\subseteq\mathsf{FIV}(A)$ – and Lemma 4.8.
- **A8.** A is $[\![s]\!]_\Xi A\supset\forall\vec{i}.A$, where $\mathsf{FIV}(A)\overset{\vec{i}}{\Rightarrow}\neg\Xi$. In this case, A_{x^B} is of one of the forms
  - $[\![s]\!]_\Xi A'\supset\forall\vec{i}.A'$. This is an instance of **A8** as follows from Lemma 4.8, Lemma 4.9(2) and $\mathsf{FIV}(A)\overset{\vec{i}}{\Rightarrow}\neg\Xi$.
  - $\forall\vec{j}.A'\supset\forall\vec{i}.A'$, where $\vec{j}=\mathsf{FIV}(A)\backslash\Xi$. This formula is an instance of **A1h**. In order to verify $\mathsf{FIV}(A')\overset{\vec{i}}{\Rightarrow}\vec{j}$, assume $k\in\mathsf{FIV}(A')\cap\vec{i}$. Then $k\in\mathsf{FIV}(A)$ from Lemma 4.8. From the condition $\mathsf{FIV}(A)\overset{\vec{i}}{\Rightarrow}\neg\Xi$, we deduce $k\notin\Xi$. Finally, the definition of $\vec{j}$ yields $k\in\vec{j}$, as required.
- **A9.** A is $[\![s]\!]_\Xi(A\supset B)\supset\forall\vec{j}.A\supset\forall\vec{k}.B$ where $\mathsf{FIV}(A)\overset{\vec{j}}{\Rightarrow}\neg\Xi$, $\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\neg\Xi$ and $(\mathsf{FIV}(A)\cap\mathsf{FIV}(B))\overset{\vec{k}}{\Rightarrow}\vec{j}$. In this case, A_{x^B} if of one of the forms:
  - $[\![s]\!]_\Xi(A'\supset B')\supset\forall\vec{i}.A'\supset\forall\vec{j}.B'$. This is an instance of **A9**. Indeed, the conditions $\mathsf{FIV}(A')\overset{\vec{j}}{\Rightarrow}\neg\Xi$, $\mathsf{FIV}(B')\overset{\vec{k}}{\Rightarrow}\neg\Xi$ and $(\mathsf{FIV}(A')\cap\mathsf{FIV}(B'))\overset{\vec{k}}{\Rightarrow}\vec{j}$ follow from Lemma 4.8 and Lemma 4.9(2).
  - $\forall\vec{i}.(A'\supset B')\supset\forall\vec{j}.A'\supset\forall\vec{k}.B'$, where $\vec{i}=\mathsf{FIV}(A\supset B)\backslash\Xi$. To verify that this formula is an instance of **A1i**, we must check that $\mathsf{FIV}(A')\overset{\vec{j}}{\Rightarrow}\vec{i}$, $\mathsf{FIV}(B')\overset{\vec{k}}{\Rightarrow}\vec{i}$ and $(\mathsf{FIV}(A')\cap\mathsf{FIV}(B'))\overset{\vec{k}}{\Rightarrow}\vec{j}$. This follows from $\mathsf{FIV}(A)\overset{\vec{j}}{\Rightarrow}\neg\Xi$, $\mathsf{FIV}(B)\overset{\vec{k}}{\Rightarrow}\neg\Xi$, $(\mathsf{FIV}(A)\cap\mathsf{FIV}(B))\overset{\vec{k}}{\Rightarrow}\vec{j}$ and Lemma 4.8.
- **B1.** A is $[\![t]\!]_\Xi A\supset A$. In this case, A_{x^B} is of one of the forms
  - $[\![t]\!]_\Xi A'\supset A'$ or
  - $\forall\vec{i}.A'\supset A'$, where $\vec{i}=\mathsf{FIV}(A)\backslash\Xi$. This formula is an instance of **A1dd**.
- **B2.** A is $[\![s]\!]_\Xi(A\supset B)\supset[\![t]\!]_\Xi A\supset[\![s\cdot t]\!]_\Xi B$. In this case, A_{x^B} is of one of the following forms where $\vec{i}=\mathsf{FIV}(A\supset B)\backslash\Xi,\vec{j}=\mathsf{FIV}(A)\backslash\Xi$ and $\vec{k}=\mathsf{FIV}(B)\backslash\Xi$.

- $[[s]]_{\Xi}(A'\supset B')\supset[[t]]_{\Xi}A'\supset[[s\cdot t]]_{\Xi}B'$. This formula is an instance of **B2**.
- $\forall\vec{i}.(A'\supset B')\supset[[t]]_{\Xi}A'\supset\forall\vec{k}.B'$, with $\vec{i}=\mathsf{FIV}(A\supset B)\setminus\Xi$ and $\vec{k}=\mathsf{FIV}(B)\setminus\Xi$. This formula is an instance of **A7**. For that we must verify $\mathsf{FIV}(B')\overset{\vec{k}}{\Rightarrow}\vec{i}$, $\mathsf{FIV}(B')\cap\vec{k}\cap\Xi=\emptyset$ and $\mathsf{FIV}(A')\setminus\Xi\subseteq\vec{i}$. The first two conditions follow from Lemma 4.8 and the definitions of $\vec{i}$ and $\vec{k}$. The latter follows from Lemma 4.8 and the definition of $\vec{i}$.
- $[[s]]_{\Xi}(A'\supset B')\supset\forall\vec{j}.A'\supset\forall\vec{k}.B'$, with $\vec{j}=\mathsf{FIV}(A)\setminus\Xi$ and $\vec{k}=\mathsf{FIV}(B)\setminus\Xi$. This is an instance of **A9**. We verify the associated conditions: $\mathsf{FIV}(A')\overset{\vec{j}}{\Rightarrow}\neg\Xi$, $\mathsf{FIV}(B')\overset{\vec{k}}{\Rightarrow}\neg\Xi$ and $(\mathsf{FIV}(A')\cap\mathsf{FIV}(B'))\overset{\vec{k}}{\Rightarrow}\vec{j}$. They all follow from Lemma 4.8 and the definitions of $\vec{j}$ and $\vec{k}$.
- $\forall\vec{i}.(A'\supset B')\supset\forall\vec{j}.A'\supset\forall\vec{k}.B'$. This is an instance of **A1i**. The associated conditions, $\mathsf{FIV}(A')\overset{\vec{j}}{\Rightarrow}\vec{i}$, $\mathsf{FIV}(B')\overset{\vec{k}}{\Rightarrow}\vec{i}$ and $(\mathsf{FIV}(A')\cap\mathsf{FIV}(B'))\overset{\vec{k}}{\Rightarrow}\vec{j}$, follow from the definitions of $\vec{i}$, $\vec{j}$ and $\vec{k}$.

- **B3a.** A is $[[s]]_{\Xi}A\supset[[(s+t)]]_{\Xi}A$. In this case, A_{x^B} is of one of the forms:
  - $[[s]]_{\Xi}A'\supset[[(s+t)]]_{\Xi}A'$. This is an instance of **B3a**.
  - $[[s]]_{\Xi}A'\supset\forall\vec{i}.A'$, where $\vec{i}=\mathsf{FIV}(A)\setminus\Xi$. This is an instance of **A8**. Note that the associated condition $\mathsf{FIV}(A')\overset{\vec{i}}{\Rightarrow}\neg\Xi$ follows immediately from the definition of $\vec{i}$.
  - $\forall\vec{i}.A'\supset\forall\vec{i}.A'$. This formula is an instance of **A4**.

- **B3b.** A is $[[t]]_{\Xi}A\supset[[(s+t)]]_{\Xi}A$. In this case, A_{x^B} is either of the form
  - $[[t]]_{\Xi}A'\supset[[(s+t)]]_{\Xi}A'$ or
  - $[[t]]_{\Xi}A'\supset\forall\vec{i}.A'$, where $\vec{i}=\mathsf{FIV}(A)\setminus\Xi$, or
  - $\forall\vec{i}.A'\supset\forall\vec{i}.A'$.

  These are dealt with in a similar way to the previous case.
- **B4.** A is $[[t]]_{\Xi}A\supset[[!t]]_{\Xi}[[t]]_{\Xi}A$. In this case, A_{x^B} is of one of the forms
  - $[[t]]_{\Xi}A'\supset[[!t]]_{\Xi}[[t]]_{\Xi}A'$. This formula is an instance of **B4**.
  - $\forall\vec{i}.A'\supset\forall\vec{i}.A'$. This formula is an instance of **A4**.

- **B5.** A is $[[t]]_{\Xi}A\supset[[\mathsf{gen}_i(t)]]_{\Xi}\forall i.A$ where $i\notin\Xi$. In this case, A_{x^B} is of one of the forms
  - $[[t]]_{\Xi}A'\supset[[\mathsf{gen}_i(t)]]_{\Xi}\forall i.A'$. This formula is an instance of **B5**.
  - $\forall\vec{j}.A'\supset\forall\vec{k}.\forall i.A'$, where $\vec{j}=\mathsf{FIV}(A)\setminus\Xi$ and $\vec{k}=\mathsf{FIV}(\forall i.A)\setminus\Xi$. We consider two cases.
    - $*$ First suppose $i\in\mathsf{FIV}(A')$. Then since $i\in\mathsf{FIV}(A)$ (by Lemma 4.8), from the definitions of $\vec{j}$ and $\vec{k}$ we deduce $\{\vec{j}\}=\{\vec{k},i\}$. Thus we have an instance of **A1g**.
    - $*$ Suppose now that $i\notin\mathsf{FIV}(A')$. Then $\vec{j}=\vec{k}$ and the second case is an instance of **A1ff**.

■

LEMMA 4.11 (Stripping)
Suppose π is a EFOLP-derivation of $\Gamma,x^{[[y^A]]_{\Xi}A}\vdash B$, $y^A\notin\Gamma$. Then there is a EFOLP-derivation π' of $\Gamma,y^A\vdash B_{y^A}$.

PROOF. By induction on π.

- If $B=[[y^A]]_{\Xi}A$ and π is obtained by using the hypothesis $x^{[[y^A]]_{\Xi}A}$, then $B_{y^A}=A$ 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 $z^B \in \Gamma$, 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 $B_{y^A} = B$.
- If π is obtained by using an axiom, then by Lemma 4.10, B_{y^A} is also an axiom.
- If π is obtained by applying **MP**:

$$\dfrac{\dfrac{\cdots}{\Gamma, x^{[[y^A]]_\Xi A} \vdash D \supset B} \qquad \dfrac{\cdots}{\Gamma, x^{[[y^A]]_\Xi A} \vdash D}}{\Gamma, x^{[[y^A]]_\Xi A} \vdash B}\, MP$$

  By the induction hypothesis, we have derivations of $\Gamma, y^A \vdash D_{y^A} \supset B_{y^A}$ and $\Gamma, y^A \vdash D_{y^A}$. Therefore, by **MP**, we obtain a derivation of $\Gamma, y^A \vdash B_{y^A}$.
- If π is obtained by applying **Gen**, then B is of the form $\forall i.D$ with $i \notin \mathsf{FIV}(\Gamma, x^{[[y^A]]_\Xi A})$, and there is a derivation of $\Gamma, x^{[[y^A]]_\Xi A} \vdash D_{y^A}$. By the induction hypothesis we can derive $\Gamma, y^A \vdash D_{y^A}$. And, since $\mathsf{FIV}(A) \subseteq \Xi$, then $i \notin \mathsf{FIV}(\Gamma, y^A)$. The result is obtained by **Gen**.
- If π is obtained by applying **Nec**, then B is of the form $[[c]]D$ with c a proof constant and D is an instance of an axiom. By Lemma 4.10, D_{y^A} is also an instance of an axiom. Therefore, $[[c]]D_{y^A}$ is derivable. Note that here the same constant has been used despite the fact that D and D_{y^A} may be instances of *different* axioms.

■

LEMMA 4.12 (λ-Abstraction)
If $\rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}} \Gamma, y^{[[x^A]]_{\mathsf{FIV}(A)} A} \vdash [[s(\vec{u}, x^A)]]_{\mathsf{FIV}(B)} B$ with $x^A \notin \Gamma$ and $x^A \notin \mathsf{FV}(B)$, then there exists a proof term $t_\lambda^{A \supset B}$ such that $\rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}} \Gamma \vdash [[t_\lambda^{A \supset B}]]_{\vec{\Xi} \cap \mathsf{FIV}(A \supset B)} (A \supset B)$.

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:

$$\begin{array}{lll}
(a) & [[\vec{u}]]_{\vec{\Xi}} \Gamma, y^{[[x^A]]_{\mathsf{FIV}(A)} A} \vdash [[c]](B \supset A \supset B) & (\mathbf{A1a}, \mathbf{Nec}) \\
(b) & [[\vec{u}]]_{\vec{\Xi}} \Gamma, y^{[[x^A]]_{\mathsf{FIV}(A)} A} \vdash [[c]]_{\mathsf{FIV}(A) \cup \mathsf{FIV}(B)} (B \supset A \supset B) & (a, \mathbf{A3}^*, \mathbf{MP}^*) \\
(c) & [[\vec{u}]]_{\vec{\Xi}} \Gamma, y^{[[x^A]]_{\mathsf{FIV}(A)} A} \vdash [[s(\vec{u}, x^A)]]_{\mathsf{FIV}(B)} B & (\text{Hypothesis}) \\
(d) & [[\vec{u}]]_{\vec{\Xi}} \Gamma, y^{[[x^A]]_{\mathsf{FIV}(A)} A} \vdash [[s(\vec{u}, x^A)]]_{\mathsf{FIV}(A) \cup \mathsf{FIV}(B)} B & (c, \mathbf{A3}^*, \mathbf{MP}^*) \\
(e) & [[\vec{u}]]_{\vec{\Xi}} \Gamma, y^{[[x^A]]_{\mathsf{FIV}(A)} A} \vdash [[c \cdot s(\vec{u}, x^A)]]_{\mathsf{FIV}(A) \cup \mathsf{FIV}(B)} (A \supset B) & (b, d, \mathbf{B2}, \mathbf{MP}^*) \\
(f) & [[\vec{u}]]_{\vec{\Xi}} \Gamma, y^{[[x^A]]_{\mathsf{FIV}(A)} A} \vdash [[x^A]]_{\mathsf{FIV}(A)} A & (\text{using } y^{[[x^A]]_{\mathsf{FIV}(A)} A}) \\
(g) & [[\vec{u}]]_{\vec{\Xi}} \Gamma, y^{[[x^A]]_{\mathsf{FIV}(A)} A} \vdash [[x^A]]_{\mathsf{FIV}(A) \cup \mathsf{FIV}(B)} A & (f, \mathbf{A3}^*, \mathbf{MP}^*) \\
(h) & [[\vec{u}]]_{\vec{\Xi}} \Gamma, y^{[[x^A]]_{\mathsf{FIV}(A)} A} \vdash [[c \cdot s(\vec{u}, x^A) \cdot x^A]]_{\mathsf{FIV}(A) \cup \mathsf{FIV}(B)} B & (e, g, \mathbf{B2}, \mathbf{MP}^*) \\
(i) & [[\vec{u}]]_{\vec{\Xi}} \Gamma, y^{[[x^A]]_{\mathsf{FIV}(A)} A} \vdash [[c \cdot s(\vec{u}, x^A) \cdot x^A]]_{\mathsf{FIV}(B)} B & (h, \mathbf{A2}^*, \mathbf{MP}^*)
\end{array}$$

*As many times as required.

We reason as follows:

$$\begin{array}{ll}
[[\vec{u}]]_{\vec{\Xi}} \Gamma, y^{[[x^A]]_{\mathsf{FIV}(A)} A} \vdash [[s(\vec{u}, x^A)]]_{\mathsf{FIV}(B)} B & (\text{Hypothesis}) \\
[[\vec{u}]]_{\vec{\Xi}} \Gamma, x^A \vdash B & (\text{Stripping}, x^A \in s(\vec{u}, x^A), x^A \notin \Gamma, \mathsf{FIV}(B) \backslash \mathsf{FIV}(B) = \emptyset) \\
[[\vec{u}]]_{\vec{\Xi}} \Gamma \vdash A \supset B & (\text{Deduction for } \mathsf{EFOLP}) \\
[[\vec{u}]]_{\vec{\Xi}} \Gamma \vdash [[r^{\vec{\Xi}, A \supset B}]]_{\vec{\Xi} \cap \mathsf{FIV}(A \supset B)} (A \supset B) & (\text{Corollary } 4.6)
\end{array}$$

Take $t_\lambda^{A \supset B} = r^{\vec{\Xi}, A \supset B}$. ■

COROLLARY 4.13 (μ-Abstraction)
Suppose $\rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}}\Gamma, y^{[[\alpha^{\neg A}]]_{\mathsf{FIV}(A)}\neg A} \vdash [[s(\vec{u},\alpha^{\neg A})]]\bot$ with $\alpha^{\neg A} \notin \Gamma$. Then $[[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[t_{\mu}^{A}]]_{\vec{\Xi}\cap\mathsf{FIV}(A)}A$, where $t_{\mu}^{A} \triangleq c\cdot t_{\lambda}^{\neg\neg A}$.

PROOF. We reason as follows:

$$\begin{array}{ll}
[[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[t_{\lambda}^{\neg\neg A}([[\vec{u}]]_{\vec{\Xi}}\Gamma)]]_{\vec{\Xi}\cap\mathsf{FIV}(A)}(\neg\neg A) & (\lambda\text{-Abstraction}) \\
[[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[c]](\neg\neg A \supset A) & (\textbf{A1c}, \textbf{Nec}) \\
[[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[c]]_{\vec{\Xi}\cap\mathsf{FIV}(A)}(\neg\neg A \supset A) & (\textbf{A3} \text{ and } \textbf{MP} \text{ as many times as needed}) \\
[[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[c\cdot t_{\lambda}^{\neg\neg A}([[\vec{u}]]_{\vec{\Xi}}\Gamma)]]_{\vec{\Xi}\cap\mathsf{FIV}(A)}A & (\textbf{B2}, \textbf{MP} \text{ twice})
\end{array}$$

■

LEMMA 4.14 (!-Abstraction)
Suppose $\rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[s]]_{\vec{\Xi}\cap\mathsf{FIV}(A)}A$. Then there exists a proof term $t_{!}^{\Xi,A}$ such that $\rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[t_{!}^{\Xi,A}]]_{\vec{\Xi}\cap\Xi}[[s]]_{\Xi}A$, for any Ξ such that $\vec{\Xi}\cap\mathsf{FIV}(A) \subseteq \Xi$.

PROOF. We reason as follows:

$$\begin{array}{ll}
[[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[s]]_{\vec{\Xi}\cap\mathsf{FIV}(A)}A & (\text{Hypothesis}) \\
[[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[s]]_{\Xi}A & (\textbf{A3}^*, \textbf{MP}^*, \vec{\Xi}\cap\mathsf{FIV}(A) \subseteq \Xi) \\
[[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[r^{\vec{\Xi},[[s]]_{\Xi}A}]]_{\vec{\Xi}\cap\Xi}[[s]]_{\Xi}A & (\text{Corollary 4.6})
\end{array}$$

* As many times as required. Take $t_{!}^{\Xi,A} = r^{\vec{\Xi},[[s]]_{\Xi}A}$.

Note: if $\Xi \subseteq \vec{\Xi}$, then we can take $t_{!}^{\Xi,A} = !s$ and the result holds by **B4** instead of Corollary 4.6. ■

LEMMA 4.15 (Substitution)
$\Gamma \vdash [[s]]_{\Xi}A$, $\Gamma, y^{[[x^{A}]]_{\Xi'}A} \vdash B$, $\Xi\cap\mathsf{FIV}(A) \subseteq \Xi'$ and $x^{A} \notin \mathsf{FVT}(\Gamma)$ implies $\Gamma \vdash B\{x^{A} \leftarrow s\}$.

4.2.2 Translation from FOHLP to EFOLP

We now address the main result of this section, namely the translation of formulas provable in FOHLP into formulas provable in EFOLP. We proceed in two stages: first we shall define the translation between formulas in both languages and then we prove the main result, namely:

PROPOSITION 4.16
If $\rhd_{\mathsf{FOHLP}} \Theta;\Gamma;\Delta \vdash D|s$, then $\rhd_{\mathsf{EFOLP}} \Theta^{\star}\cup\Gamma^{\star}\cup\Delta^{\star} \vdash [[s^{\star}]]_{\mathsf{FIV}(\mathcal{H}^{\star})\cap\mathsf{FIV}(D^{\star})}D^{\star}$.

For the first stage, we introduce the defining clauses of the translation in a step-by-step manner until we obtain the complete definition. We begin by showing how to translate formulas, contexts and proof terms *without* considering the proof terms constructors lambda and name abstractions, unbox and bang. We the add clauses for lambda and name abstraction. Finally, we add clauses for bang.

For the second stage, the proof of Proposition 4.16 itself, we shall proceed by induction on derivations in FOHLP. We assume that derivations in FOHLP use the more simple modal introduction scheme $\Box\mathsf{I}'$ (*cf.* Remark 3.5) instead of $\Box\mathsf{I}$. A consequence of this is that if $\rhd_{\mathsf{FOHLP}} \Theta;\Gamma;\Delta \vdash A|s$, then we may assume that the derivation does not make use of the equivalence rules. That we may adopt this assumption without loss of generality follows from Lemma 3.11 (whose proof resorts to $\Box\mathsf{I}'$ rather than $\Box\mathsf{I}$).normal form.

Translating formulas, contexts and judgements. The translation $\bullet^\star$ from FOHLP to FOLP is defined as follows for formulas and contexts:

$$\begin{array}{rcl} P(E_1,\dots,E_n)^\star & \triangleq & P(E_1,\dots,E_n) \\ \bot^\star & \triangleq & \bot \\ (A\supset B)^\star & \triangleq & A^\star\supset B^\star \\ \forall i.A^\star & \triangleq & \forall i.A^\star \\ [\![s]\!]_\Xi A^\star & \triangleq & [\![s^\star]\!]_\Xi A^\star \end{array} \qquad \begin{array}{rcl} \cdot^\star & \triangleq & \cdot \\ (\Theta, v^A_\Xi)^\star & \triangleq & \Theta^\star, [\![v^{A^\star}]\!]_\Xi A^\star \\ (\Gamma, x^A)^\star & \triangleq & \Gamma^\star, [\![x^{A^\star}]\!]_{\mathsf{FIV}(A^\star)} A^\star \\ (\Delta, \alpha^A)^\star & \triangleq & \Delta^\star, [\![\alpha^{\neg A^\star}]\!]_{\mathsf{FIV}(A^\star)} \neg A^\star \end{array}$$

Remark 4.17
For every formula A, $\mathsf{FIV}(A) = \mathsf{FIV}(A^\star)$. Note that FOHLP-proof witnesses and FOLP-proof terms play no role in the definition of the free individual variables of a formula.

The translation of a FOHLP-judgement $\Theta;\Gamma;\Delta \vdash A\,|\,s$ is defined as:

$$(\Theta;\Gamma;\Delta \vdash A\,|\,s)^\star \triangleq \Theta^\star, \Gamma^\star, \Delta^\star \vdash [\![s^\star]\!]_{\mathsf{FIV}(\Theta^\star\cup\Gamma^\star\cup\Delta^\star)\cap\mathsf{FIV}(A^\star)} A^\star$$

Towards translation of proof witnesses. For proof witnesses (disregarding lambda and name abstractions, unbox and bang) we have:

$$\begin{array}{rcl} (x^A)^\star & \triangleq & x^{A^\star} \\ (v^A_\Xi)^\star & \triangleq & v^{A^\star} \\ (s\cdot t)^\star & \triangleq & s^\star\cdot t^\star \\ ([\alpha^A]s)^\star & \triangleq & \alpha^{\neg A^\star}\cdot s^\star \end{array} \qquad \begin{array}{rcl} (s+t)^\star & \triangleq & s^\star + t^\star \\ \mathsf{gen}_i(s)^\star & \triangleq & \mathsf{gen}_i(s^\star) \\ \mathsf{ins}^E_i(s)^\star & \triangleq & c\cdot s^\star \end{array}$$

In the clause for $\mathsf{ins}^E_i(s)$ we assume $[\![c]\!]_\emptyset A \in \mathcal{C}$, for all formulas A which are instances of axiom scheme **A1dd** (which we recall is $(\forall\vec{j}.\forall\vec{i}.A)\supset\forall\vec{j}.(A\{\vec{i}\leftarrow\vec{E}\})$).

Translating lambda and name abstraction. We now explain how we address lambda abstraction (name abstraction is addressed similarly). Suppose that the last scheme applied in the derivation π 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 induction hypothesis of our forthcoming proof (Proposition 4.16) will yield derivability in EFOLP of:

$$\Theta^\star\cup\Gamma^\star, [\![x^{A^\star}]\!]_{\mathsf{FIV}(A^\star)} A^\star \cup \Delta^\star \vdash [\![s^\star]\!]_{\mathsf{FIV}(\Theta^\star\cup\Gamma^\star\cup\Delta^\star)\cap\mathsf{FIV}(B^\star)} B^\star. \qquad (3)$$

However, we are after derivability of $\Theta^\star\cup\Gamma^\star\cup\Delta^\star \vdash [\![t]\!]_{\mathsf{FIV}(\Theta^\star\cup\Gamma^\star\cup\Delta^\star)\cap\mathsf{FIV}(A^\star\supset B^\star)}(A^\star\supset B^\star)$, for an appropriate proof term t. Building a derivation of this judgement requires three steps:

(1) We first need to 'drop' the outermost modalities of $[\![x^{A^\star}]\!]_{\mathsf{FIV}(A^\star)} A^\star$ and $[\![s^\star]\!]_{\mathsf{FIV}(\Theta^\star\cup\Gamma^\star\cup\Delta^\star)\cap\mathsf{FIV}(B^\star)} B^\star$ from (3). This is achieved via the Stripping Lemma (Lemma 4.11).
(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 EFOLP in order to deduce the appropriate proof term t. This is achieved via the Internalization Lemma (Lemma 4.5).

These three steps conform the content of the λ-Abstraction Lemma (Lemma 4.12). Note that t is thus a function of the original EFOLP derivation of (3). In turn, (3) is obtained from analysing the FOHLP derivation π, and may contain multiple FOHLP derivations of an FOHLP judgement.[7] Thus we shall assume in our proof of Proposition 4.16 (and Corollary 4.18) that π is *canonical* in the sense that multiple occurrences of a judgement in π all have the exact same proof. The clauses defining the translation of lambda $(\lambda x^A.s)^\star$ and name abstraction $(\mu\alpha^A.s)^\star$, are as follows:

$$\begin{array}{rcll}
(\lambda x^A.s)^\star & \triangleq & t_\lambda^{A^\star\supset B^\star}, & \text{if there exists a } \mathsf{EFOLP}\text{-context } [[\vec{u}]]_{\vec{\Xi}}\Gamma, \text{ a formula } B \text{ and a fresh} \\
 & & & y^{[[x^{A^\star}]]_{\mathsf{FIV}(A)}A^\star} \text{ s.t. } \rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}}\Gamma, y^{[[x^{A^\star}]]_{\mathsf{FIV}(A)}A^\star} \vdash [[s^\star]]_{\mathsf{FIV}([[\vec{u}]]_{\vec{\Xi}}\Gamma)\cap\mathsf{FIV}(B^\star)}B^\star. \\
(\lambda x^A.s)^\star & \triangleq & d\cdot d, & \text{otherwise.} \\
(\mu\alpha^A.s)^\star & \triangleq & t_\mu^{A^\star}, & \text{if there exists a } \mathsf{EFOLP}\text{-context } [[\vec{u}]]_{\vec{\Xi}}\Gamma \text{ and a fresh } y^{[[\alpha^{\neg A^\star}]]_{\mathsf{FIV}(A^\star)}A^\star} \text{ s.t.} \\
 & & & \rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}}\Gamma, y^{[[\alpha^{\neg A^\star}]]_{\mathsf{FIV}(A^\star)}A^\star} \vdash [[s^\star]]_\emptyset \bot. \\
(\mu\alpha^A.s)^\star & \triangleq & d\cdot d, & \text{otherwise.}
\end{array}$$

Here we assume $[[d]]_\emptyset A \in \mathcal{C}$, for all formulas A which are instances of axiom scheme **A1c**, the axiom scheme of classical logic $\neg\neg A \supset A$. In our use of this translation (Proposition 4.16) the conditions of the first and third clauses shall be met when dealing with modalities that are introduced using $\Box\mathsf{I}$ and in which the translated abstraction that occurs in the internalized proof witness is proved in π itself; the second and fourth cases are used when these abstractions that occur in modalities do not represent valid proofs.[8] The proof terms defined by the first and third clauses all depend on the form that the assumed EFOLP derivation takes. Since there are non-linear constraints in our terms (*cf.* $\supset\mathsf{E}$ in Figure 2 has A in positive and negative positions), hence the reason for the assumption that π be canonical.

Translating bang. Regarding the clause for $(!t)^\star$, defining it simply as $!t^\star$ presents technical difficulties when addressing the case $\Box\mathsf{I}'$. Indeed, suppose the FOHLP derivation ends in:

$$\frac{\Theta;\cdot;\cdot\vdash A\,|\,t \qquad \mathsf{FIV}(\Theta)\cap\mathsf{FIV}(A)\subseteq\Xi}{\Theta;\Gamma;\Delta\vdash[[t]]_\Xi A\,|\,!t}\;\Box\mathsf{I}'.$$

The induction hypothesis yields:

$$\Theta^\star\vdash[[t^\star]]_{\mathsf{FIV}(\Theta^\star)\cap\mathsf{FIV}(A^\star)}A^\star$$

from which we can obtain the following, given the condition $\mathsf{FIV}(\Theta)\cap\mathsf{FIV}(A)\subseteq\Xi$ of $\Box\mathsf{I}'$:

$$\Theta^\star\vdash[[t^\star]]_\Xi A^\star$$

But then **B4** yields:

$$\Theta^\star\vdash[[!t^\star]]_\Xi[[t^\star]]_\Xi A^\star$$

However we are after:

$$\Theta^\star\vdash[[!t^\star]]_{\mathsf{FIV}(\Theta^\star\cup\Gamma^\star\cup\Delta^\star)\cap\Xi}[[t^\star]]_\Xi A^\star$$

Unfortunately, it is not sound to simply discard the variables in Ξ in order to obtain $\mathsf{FIV}(\Theta^\star\cup\Gamma^\star\cup\Delta^\star)\cap\Xi$. A similar situation arises if we define $t\langle v_{\Xi}^{A}{:=}r,s\rangle$ as $t^\star\{v^{A^\star}\leftarrow r^\star\}$. We thus define $(!t)^\star$ and

[7] Since we assume $\Box\mathsf{I}'$ rather than $\Box\mathsf{I}$, the sole source of this multiplicity is PlusL and PlusR.

[8] For example, $\cdot;x^{[[\lambda z^A.z\cdot z]]_\Xi B};\cdot\vdash[[\lambda z^A.z\cdot z]]_\Xi B\,|\,x^{[[\lambda z^A.z\cdot z]]_\Xi B}$.

$(t\langle v^A_{\Xi}{:=}r,s\rangle)^\star$ as follows:

$$
\begin{array}{rcll}
(!t)^\star & \triangleq & t_!^{\Xi,A^\star}, & \text{if there exists a } \mathsf{EFOLP}\text{-context } [[\vec{u}]]_{\vec{\Xi}}\Gamma \text{ and a formula } A \text{ s.t.} \\
 & & & \rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[t^\star]]_{\mathsf{FIV}([[\vec{u}]]_{\vec{\Xi}}\Gamma)\cap\mathsf{FIV}(A^\star)} A^\star \text{ and} \\
 & & & \mathsf{FIV}([[\vec{u}]]_{\vec{\Xi}}\Gamma)\cap\mathsf{FIV}(A^\star)\subseteq\Xi. \\
(!t)^\star & \triangleq & !t^\star, & \text{otherwise.} \\
(t\langle v^A_{\Xi}{:=}r,s\rangle)^\star & \triangleq & r^{\vec{\Xi},C^\star\{v^{A^\star}\leftarrow r^\star\}}, & \text{if there exists a } \mathsf{EFOLP}\text{-context } [[\vec{u}]]_{\vec{\Xi}}\Gamma \text{ and a formula } C \text{ s.t.} \\
 & & & \rhd_{\mathsf{EFOLP}} [[\vec{u}]]_{\vec{\Xi}}\Gamma \vdash [[t^\star\{v^{A^\star}\leftarrow r^\star\}]]_{(\mathsf{FIV}([[\vec{u}]]_{\vec{\Xi}}\Gamma)\cup\Xi)} C^\star\{v^{A^\star}\leftarrow r^\star\}. \\
(t\langle v^A_{\Xi}{:=}r,s\rangle)^\star & \triangleq & t^\star\{v^{A^\star}\leftarrow r^\star\}, & \text{otherwise.}
\end{array}
$$

This completes the definition of the translation. We now focus on the proof of Proposition 4.16 whose statement, we recall from above, reads:

If $\rhd_{\mathsf{FOHLP}}\mathcal{H}\vdash D\,|\,s$, then $\rhd_{\mathsf{EFOLP}}\mathcal{H}^\star\vdash[[s^\star]]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(D^\star)}D^\star$, where $\mathcal{H}^\star$ is shorthand for $\Theta^\star\cup\Gamma^\star\cup\Delta^\star$.

Proof. By induction on the derivation of $\mathcal{H}\vdash D\,|\,s$. As mentioned in the beginning of this subsection, we assume that the derivation does not resort to proof witness equivalence. We analyze the last rule used.

- Case Var. $\mathcal{H}\vdash D\,|\,s$ is $\Theta;\Gamma',x^A;\Delta\vdash A\,|\,x^A$. Trivially $\rhd_{\mathsf{EFOLP}}\Theta^\star\cup\Gamma^\star\cup\Delta^\star\vdash[[x^{A^\star}]]_{\mathsf{FIV}(A^\star)}A^\star$. Since $[[x^{A^\star}]]_{\mathsf{FIV}(A^\star)}A^\star\in\Gamma^\star$, then $\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star)=\mathsf{FIV}(A^\star)$.
- Case VarM. In this case $s=v^D_{\Xi}$, $\Theta=\Theta',v^D_{\Xi}$ and hence $\mathcal{H}=\Theta',v^D_{\Xi};\Gamma;\Delta$. $\mathcal{H}^\star\vdash[[v^{D^\star}]]_{\Xi}D^\star$ is derivable in EFOLP since $v^{D^\star}\in\mathcal{H}^\star$. Note also that $\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(D^\star)=\mathsf{FIV}(D^\star)$. We can use **A2** and **A3** as necessary (along with **MP**) to derive $\mathcal{H}^\star\vdash[[v^{D^\star}]]_{\mathsf{FIV}(D^\star)}D^\star$.
- Case $\supset\mathsf{I}$. The derivation ends in:

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

  By the induction hypothesis we can derive:

  $$\Theta^\star\cup\Gamma^\star,[[x^{A^\star}]]_{\mathsf{FIV}(A)}A^\star\cup\Delta^\star\vdash[[s^\star]]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(B^\star)}B^\star. \tag{4}$$

  Thus, our translation requires that we prove:

  $$\mathcal{H}^\star\vdash[[t_\lambda^{A^\star\supset B^\star}]]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star\supset B^\star)}(A^\star\supset B^\star). \tag{5}$$

  in EFOLP in order to conclude. From (4) and possibly multiple uses of **A2**, **A3** and **MP**:

  $$\Theta^\star\cup\Gamma^\star,[[x^{A^\star}]]_{\mathsf{FIV}(A^\star)}A^\star\cup\Delta^\star\vdash[[s^\star]]_{\mathsf{FIV}(B^\star)}B^\star.$$

  By our freshness convention, we know that $x^A\notin\mathcal{H}$ and $x^A\notin\mathsf{FVT}(B)$. Therefore, $x^{A^\star}\notin\mathcal{H}^\star$ and $x^{A^\star}\notin\mathsf{FV}(B^\star)$. We then resort to the λ-Abstraction Lemma (4.12) to obtain $t_\lambda^{A^\star\supset B^\star}$ s.t.

  $$\rhd_{\mathsf{EFOLP}}\mathcal{H}^\star\vdash[[t_\lambda^{A^\star\supset B^\star}]]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star\supset B^\star)}(A^\star\supset B^\star).$$

- Case $\supset\mathsf{E}$. The derivation ends in:

  $$\frac{\Theta;\Gamma;\Delta\vdash A\supset B\,|\,s\qquad\Theta;\Gamma;\Delta\vdash A\,|\,t}{\Theta;\Gamma;\Delta\vdash B\,|\,s\cdot t}\supset\mathsf{E}.$$

By the induction hypothesis both of the following judgements are derivable in EFOLP:

(1) $\mathcal{H}^\star \vdash [\![s^\star]\!]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star\supset B^\star)}(A\supset B)^\star$ and
(2) $\mathcal{H}^\star \vdash [\![t^\star]\!]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star)}A^\star$

We can derive $\mathcal{H}^\star \vdash [\![t^\star]\!]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star\supset B^\star)}A^\star$ by using **A3** and **MP** as many times as required (keep in mind that $\mathsf{FIV}(A) = \mathsf{FIV}(A^\star) \subseteq \mathsf{FIV}(A^\star \supset B^\star)$). Then, using **B2** and **MP** twice, we derive $\mathcal{H}^\star \vdash [\![(s^\star \cdot t^\star)]\!]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star\supset B^\star)}B^\star$.
Note that $A^\star$ is the same on both sides, since we are assuming canonical derivations and thus translations are unique.

- Case $\Box\mathsf{I}'$. In this case $D = [\![t]\!]_\Xi A$ and the derivation ends in:

$$\frac{\Theta; \cdot; \cdot \vdash A \mid t \qquad \mathsf{FIV}(\Theta)\cap\mathsf{FIV}(A)\subseteq\Xi}{\Theta;\Gamma;\Delta\vdash [\![t]\!]_\Xi A \mid !t}\ \Box\mathsf{I}'.$$

We reason as follows, where * in step (c) means **A3** and **MP** are used possibly multiple times:

(a) $\Theta^\star \vdash [\![t^\star]\!]_{\mathsf{FIV}(\Theta^\star)\cap\mathsf{FIV}(A^\star)}A^\star$ (IH)
(b) $\Theta^\star \vdash [\![t_!^{\Xi,A^\star}]\!]_{\mathsf{FIV}(\Theta^\star)\cap\Xi}[\![t]\!]_\Xi A^\star$ (Lemma 4.14, $\mathsf{FIV}(\Theta^\star)\cap\mathsf{FIV}(A^\star)\subseteq\Xi$)
(c) $\Theta^\star\cup\Gamma^\star\cup\Delta^\star \vdash [\![t_!^{\Xi,A}]\!]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\Xi}[\![t^\star]\!]_\Xi A^\star$ (**A3** and **MP**)*

We know that $t_!^{\Xi,A}$ is the correct for translation for $!t$, since $\rhd_{\mathsf{EFOLP}}\,\Theta^\star \vdash [\![t^\star]\!]_{\mathsf{FIV}(\Theta^\star)\cap\mathsf{FIV}(A)}A^\star$ and $\mathsf{FIV}(\Theta^\star)\cap\mathsf{FIV}(A)\subseteq\Xi$.

- Case $\Box\mathsf{E}$. The derivation ends in:

$$\frac{\Theta;\Gamma;\Delta\vdash [\![r]\!]_\Xi A \mid s' \qquad \Theta, v^A_{\Xi'};\Gamma;\Delta\vdash C \mid t \qquad \Xi\cap\mathsf{FIV}(A)\subseteq\Xi'}{\Theta;\Gamma;\Delta\vdash C\{v^A_{\Xi'}\leftarrow r\} \mid t\langle v^A_{\Xi'} := r, s'\rangle}\ \Box\mathsf{E}$$

with $D = C\{v^A_{\Xi'}\leftarrow r\}$ and $s = t\langle v^A_{\Xi'} := r, s'\rangle$.
By the induction hypothesis both of the following judgements are derivable in EFOLP:

(1) $\mathcal{H}^\star \vdash [\![s'^\star]\!]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\Xi}[\![r^\star]\!]_\Xi A^\star$
(2) $\mathcal{H}^\star, [\![v^{A^\star}]\!]_{\Xi'}A^\star \vdash [\![t^\star]\!]_{(\mathsf{FIV}(\mathcal{H}^\star)\cup\Xi')\cap\mathsf{FIV}(C^\star)}C^\star$

We now reason as follows:

(a) $\mathcal{H}^\star \vdash ([\![s'^\star]\!]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\Xi}[\![r^\star]\!]_\Xi A^\star)\supset([\![r^\star]\!]_\Xi A^\star)$ (**B1**)
(b) $\mathcal{H}^\star \vdash [\![r^\star]\!]_\Xi A^\star$ ((a), **MP**)
(c) $\mathcal{H}^\star \vdash [\![t^\star\{v^{A^\star}\leftarrow r^\star\}]\!]_{((\mathsf{FIV}(\mathcal{H}^\star)\cup\Xi')\cap\mathsf{FIV}(C^\star))}C^\star\{v^{A^\star}\leftarrow r^\star\}$ (Lemma 4.15, (b), (2))
(d) $\mathcal{H}^\star \vdash C^\star\{v^{A^\star}\leftarrow r^\star\}$ (**B1**, **MP**)
(e) $\mathcal{H}^\star \vdash [\![r^{\mathsf{FIV}(\mathcal{H}^\star), C^\star\{v^{A^\star}\leftarrow r^\star\}}]\!]_{(\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(C^\star))}C^\star\{v^{A^\star}\leftarrow r^\star\}$(Corollary 4.6)

By Remark 2.4, $\mathsf{FIV}(C^\star) = \mathsf{FIV}(C^\star\{v^{A^\star}\leftarrow r^\star\})$.
We know that $r^{\mathsf{FIV}(\mathcal{H}^\star), C^\star\{v^{A^\star}\leftarrow r^\star\}}$ is the correct translation for $t\langle v^A_{\Xi'} := r, s'\rangle$, since $\mathcal{H}^\star \vdash [\![t^\star\{v^{A^\star}\leftarrow r^\star\}]\!]_{((\mathsf{FIV}(\mathcal{H}^\star)\cup\Xi')\cap\mathsf{FIV}(C^\star))}C^\star\{v^{A^\star}\leftarrow r^\star\}$ is derivable in EFOLP by (c), and therefore so is $\mathcal{H}^\star \vdash [\![t^\star\{v^{A^\star}\leftarrow r^\star\}]\!]_{\mathsf{FIV}(\mathcal{H}^\star)\cup\Xi'}C^\star\{v^{A^\star}\leftarrow r^\star\}$.

- Case PlusL (PlusR is similar and hence ommitted). The derivation ends in:

$$\frac{\Theta;\Gamma;\Delta\vdash A \mid s}{\Theta;\Gamma;\Delta\vdash A \mid s+t}\ \mathsf{PlusL}.$$

By the induction hypothesis $\rhd_{\mathsf{EFOLP}} \mathcal{H}^\star \vdash [[s^\star]]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star)} A^\star$. Thus, by **B3a** and **MP**, also $\rhd_{\mathsf{EFOLP}} \mathcal{H}^\star \vdash [[s^\star + t^\star]]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star)} A^\star$.

- Case NAbs. The derivation ends in:

$$\frac{\Theta;\Gamma;\Delta,\alpha^A \vdash \bot \,|\, s}{\Theta;\Gamma;\Delta \vdash A \,|\, \mu\alpha^A.s}\ \mathsf{NAbs}.$$

By the induction hypothesis, $\rhd_{\mathsf{EFOLP}} \mathcal{H}^\star, [[\alpha^{\neg A^\star}]]_{\mathsf{FIV}(A^\star)} A^\star \vdash [[s^\star]]_{\emptyset} \bot$, and thus $\mu\alpha^A.s^\star = t_\mu^{A^\star} = c_{A^\star}^{\mathbf{A1c}} \cdot t_\lambda^{\neg\neg A}$. By our freshness convention, we know that $\alpha^A \notin \mathcal{H}$, therefore $\alpha^{\neg A^\star} \notin \mathcal{H}^\star$ and by the μ-Abstraction Corollary (4.13), $\mathcal{H}^\star \vdash [[t_\mu^{A^\star}]]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star)} A^\star$ is derivable in EFOLP.

- Case Name. The derivation ends in:

$$\frac{\Theta;\Gamma;\Delta,\alpha^A \vdash A \,|\, s}{\Theta;\Gamma;\Delta,\alpha^A \vdash \bot \,|\, [\alpha^A]s}\ \mathsf{Name}.$$

By the induction hypothesis, $\rhd_{\mathsf{EFOLP}} \mathcal{H}^\star, x^{[[\alpha^{\neg A^\star}]]_{\mathsf{FIV}(A^\star)}\neg A^\star} \vdash [[s^\star]]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star)} A^\star$.
Note that $\mathsf{FIV}(\mathcal{H}^\star, x^{[[\alpha^{\neg A^\star}]]_{\mathsf{FIV}(A^\star)}\neg A^\star}) \cap \mathsf{FIV}(A^\star) = \mathsf{FIV}(A^\star)$. We reason as follows:

$$\begin{array}{lll}
(1) & \mathcal{H}^\star, x^{[[\alpha^{\neg A^\star}]]_{\mathsf{FIV}(A^\star)}\neg A^\star} \vdash [[\alpha^{\neg A^\star}]]_{\mathsf{FIV}(A^\star)} \neg A^\star & (\text{hypothesis } x^{[[\alpha^{\neg A^\star}]]_{\mathsf{FIV}(A^\star)}\neg A^\star}) \\
(2) & \mathcal{H}^\star, x^{[[\alpha^{\neg A^\star}]]_{\mathsf{FIV}(A^\star)}\neg A^\star} \vdash [[s^\star]]_{\mathsf{FIV}(A^\star)} A^\star & (\text{IH}) \\
(3) & \mathcal{H}^\star, x^{[[\alpha^{\neg A^\star}]]_{\mathsf{FIV}(A^\star)}\neg A^\star} \vdash [[\alpha^{\neg A^\star} \cdot s^\star]]_{\mathsf{FIV}(A^\star)} \bot & (\mathbf{B2} \text{ and } \mathbf{MP} \text{ twice}) \\
(4) & \mathcal{H}^\star, x^{[[\alpha^{\neg A^\star}]]_{\mathsf{FIV}(A^\star)}\neg A^\star} \vdash [[\alpha^{\neg A^\star} \cdot s^\star]] \bot & (\mathbf{A2} \text{ and } \mathbf{MP} \text{ as required})
\end{array}$$

- Case $\forall\mathsf{I}$. The derivation ends in:

$$\frac{\Theta;\Gamma;\Delta \vdash A \,|\, t \quad i \notin \mathsf{FIV}(\Theta,\Gamma,\Delta)}{\Theta;\Gamma;\Delta \vdash \forall i.A \,|\, \mathsf{gen}_i(t)}\ \forall\mathsf{I}$$

with $D = \forall i.A$ and $s = \mathsf{gen}_i(t)$. By the induction hypothesis, $\rhd_{\mathsf{EFOLP}} \mathcal{H}^\star \vdash [[t^\star]]_{\mathsf{FIV}(\mathcal{H}^\star)\cap\mathsf{FIV}(A^\star)} A^\star$. Since $i \notin \mathsf{FIV}(\mathcal{H})$, then $i \notin \mathsf{FIV}(\mathcal{H}^\star)$, and thus we can obtain the result by **B5**, **A2**, and **MP** (twice).

- Case $\forall\mathsf{E}$. The derivation ends in:

$$\frac{\Theta;\Gamma;\Delta \vdash \forall i.A \,|\, t}{\Theta;\Gamma;\Delta \vdash A\{i \leftarrow E\} \,|\, \mathsf{ins}_i^E(t)}\ \forall\mathsf{E}$$

with $D = A\{i \leftarrow E\}$ and $s = \mathsf{ins}_i^E(t)$. Let $\Xi = \mathsf{FIV}(\mathcal{H}^\star) \cap \mathsf{FIV}(\forall i.A^\star)$ and $\Xi' = \mathsf{FIV}(\mathcal{H}^\star) \cap \mathsf{FIV}(A^\star\{i \leftarrow E\})$. By the induction hypothesis, $\rhd_{\mathsf{EFOLP}} \mathcal{H}^\star \vdash [[t^\star]]_{\Xi} \forall i.A^\star$.
Since $\mathsf{FIV}(\forall i.A^\star) \subseteq \mathsf{FIV}(A^\star\{i \leftarrow E\})$, then $\rhd_{\mathsf{EFOLP}} \mathcal{H}^\star \vdash [[t^\star]]_{\Xi'} \forall i.A^\star$ by using **A3** and **MP** as many times as required.
We reason as follows, where * indicates multiple uses of an axiom:

$$\begin{array}{ll}
\text{(a) } \mathcal{H}^\star \vdash \forall i.A^\star \supset A^\star\{i \leftarrow E\} & (\mathbf{A1d}) \\
\text{(b) } \mathcal{H}^\star \vdash [[c_{A^\star,i,E}^{\mathbf{A1d}}]] \forall i.A^\star \supset A^\star\{i \leftarrow E\} & (\mathbf{Nec}) \\
\text{(c) } \mathcal{H}^\star \vdash [[c_{A^\star,i,E}^{\mathbf{A1d}}]]_{\Xi'} \forall i.A^\star \supset A^\star\{i \leftarrow E\} & (\mathbf{A3}^*, \mathbf{MP}^*)
\end{array}$$

(d) $\mathcal{H}^\star \vdash [\![c^{\mathbf{A1d}}]\!]_{\Xi'}\forall i.A^\star \supset A^\star\{i \leftarrow E\} \supset [\![t^\star]\!]_{\Xi'}\forall i.A^\star \supset [\![(c^{\mathbf{A1d}} \cdot t^\star)]\!]_{\Xi'}A^\star\{i \leftarrow E\}$ **(B2)**
(e) $\mathcal{H}^\star \vdash [\![t^\star]\!]_{\Xi'}\forall i.A^\star \supset [\![(c^{\mathbf{A1d}} \cdot t^\star)]\!]_{\Xi'}A^\star\{i \leftarrow E\}$ **(MP)**
(f) $\mathcal{H}^\star \vdash [\![c^{\mathbf{A1d}} \cdot t^\star]\!]_{\Xi'}A^\star\{i \leftarrow E\}$ **(MP)**

■

COROLLARY 4.18
If $\rhd_{\mathsf{FOHLP}} \cdot;\cdot;\cdot \vdash A \,|\, s$, then $\rhd_{\mathsf{EFOLP}} \cdot \vdash [\![s^\star]\!]_{\mathsf{FIV}(A)}A^\star$ and $\rhd_{\mathsf{EFOLP}} \cdot \vdash A^\star$.

5 Term assignment

The λ^{FOLP}-calculus, our proposed term assignment for FOHLP, consists of a grammar that describes the valid terms (Definition 5.1), the typing rules (Definition 5.3) and the reduction rules (Definition 5.11).

The proof witnesses of FOHLP do not encode derivations unequivocally. For instance, the proof witness $x^A + y^A$ ensures that A is true if we assume both x^A and y^A, but it does not tell us which hypothesis was used in order to derive it. Similarly, $!v^A_\Xi$ can be used to verify that $[\![v^A_\Xi]\!]_{\Xi'}A$ is true assuming v^A_Ξ as a validity hypothesis, but this may have been derived in an infinite number of ways, using $\Box\mathsf{I}$ with any witness which is equivalent to v^A_Ξ (e.g., v^A_Ξ itself, $(\lambda x^A.x^A)\cdot v^A_\Xi$, $\mu\alpha^A.[\alpha^A]v^A_\Xi$, etc.). So we introduce further information into proof witnesses to obtain λ^{FOLP}**-terms**.

DEFINITION 5.1
The terms of λ^{FOLP} are given by the following grammar:

$$\begin{array}{rcl}
M,N & ::= & x^A \\
& | & v^A_\Xi \\
& | & (\lambda x^A.M^B)^{A\supset B} \\
& | & (M^{A\supset B}N^A)^B \\
& | & (!M^A)^{[\![s]\!]_\Xi A} \\
& | & (M^B\langle v^A_{\Xi'} := r, N^{[\![r]\!]_\Xi A}\rangle)^{B\{v^A_{\Xi'} \leftarrow r\}} \\
& | & ([\alpha^A]M^A)^\perp \\
& | & (\mu\alpha^A.M^\perp)^A \\
& | & (M^A +_{\mathrm{L}} s)^A \\
& | & (s +_{\mathrm{R}} N^B)^B \\
& | & (\mathsf{gen}_i(M^A))^{\forall i.A} \\
& | & (\mathsf{ins}^E_i(M^{\forall i.A}))^{A\{i\leftarrow E\}}
\end{array}$$

The connection between λ^{FOLP}-terms and FOHLP-derivations should be clear from the notation. The term $(M^A +_{\mathrm{L}} s)^A$ encodes a proof of A which appends the witness s to a previous proof of A—encoded by M^A—by using PlusL. Analogously, $(s +_{\mathrm{R}} M^A)^A$ encodes the proof which results from appending s to a proof of A by PlusR. Also the terms $(!v^A_\Xi)^{[\![v^A_\Xi]\!]_\Xi A}$, $(!v^A_\Xi)^{[\![(\lambda x^A.x^A)\cdot v^A_\Xi]\!]_\Xi A}$ and $(!v^A_\Xi)^{[\![v^A_\Xi]\!]_{\Xi\cup\Xi'} A}$ encode different derivations, in which $\Box\mathsf{I}$ is used in different ways to prove different formulas. We often drop superindices in terms for the sake of readability.

$$\frac{}{\mathcal{H}, x^A \vdash x^A \mid x^A}\ \textsf{T-Var}$$

$$\frac{\mathcal{H}, x^A \vdash M^B \mid s}{\mathcal{H} \vdash (\lambda x^A.M^B)^{A\supset B} \mid \lambda x^A.s}\ \textsf{T-}\supset\textsf{I} \qquad \frac{\mathcal{H} \vdash M^{A\supset B} \mid s \quad \mathcal{H} \vdash N^A \mid t}{\mathcal{H} \vdash (M^{A\supset B} N^A)^B \mid s \cdot t}\ \textsf{T-}\supset\textsf{E}$$

$$\frac{}{\mathcal{H}, v^A_{\Xi} \vdash v^A_{\Xi} \mid v^A_{\Xi}}\ \textsf{T-VarM}$$

$$\frac{\Theta; \cdot; \cdot \vdash M^A \mid s \qquad \Theta; \cdot; \cdot \vdash\ s \equiv t : A \qquad \mathsf{FIV}(\Theta) \cap \mathsf{FIV}(A) \subseteq \Xi}{\Theta; \Gamma; \Delta \vdash (!M^A)^{[\![t]\!]_\Xi A} \mid !t}\ \textsf{T-}\Box\textsf{I}$$

$$\frac{\mathcal{H} \vdash M^{[\![r]\!]_\Xi A} \mid s \qquad \mathcal{H}, v^A_{\Xi'} \vdash N^C \mid t \qquad \Xi \cap \mathsf{FIV}(A) \subseteq \Xi'}{\mathcal{H} \vdash N^C \langle v^A_{\Xi'} {:=} r, M^{[\![r]\!]_\Xi A} \rangle^{C\{v^A_{\Xi'} \leftarrow r\}} \mid t \langle v^A_{\Xi'} {:=} r, s \rangle}\ \textsf{T-}\Box\textsf{E}$$

$$\frac{\mathcal{H} \vdash M^A \mid s}{\mathcal{H} \vdash (M +_{\mathrm{L}} t)^A \mid s + t}\ \textsf{T-PlusL} \qquad \frac{\mathcal{H} \vdash N^B \mid t}{\mathcal{H} \vdash (s +_{\mathrm{R}} N)^B \mid s + t}\ \textsf{T-PlusR}$$

$$\frac{\mathcal{H}, \alpha^A \vdash M^\perp \mid s}{\mathcal{H} \vdash (\mu\alpha^A.M)^A \mid \mu\alpha^A.s}\ \textsf{T-NAbs} \qquad \frac{\mathcal{H}, \alpha^A \vdash M^A \mid s}{\mathcal{H}, \alpha^A \vdash ([\alpha^A]M)^\perp \mid [\alpha^A]s}\ \textsf{T-Name}$$

$$\frac{\mathcal{H} \vdash M^A | s \quad i \notin \mathsf{FIV}(\mathcal{H})}{\mathcal{H} \vdash \mathsf{gen}_i(M)^{\forall i.A} \mid \mathsf{gen}_i(s)}\ \textsf{T-}\forall\textsf{I} \qquad \frac{\mathcal{H} \vdash M^{\forall i.A} \mid s}{\mathcal{H} \vdash \mathsf{ins}^E_i(M)^{A\{i \leftarrow E\}} \mid \mathsf{ins}^E_i(s)}\ \textsf{T-}\forall\textsf{E}$$

FIGURE 8. Typing rules for λ^{FOLP}.

REMARK 5.2
Some information regarding the derivations these terms encode is still left out, since our terms do not encode the equivalence rules used to derive the second premise of $\textsf{T-}\Box\textsf{I}$, nor the contexts used in the derivations (we may have assumed additional hypotheses which were never used). However, these terms provide us with enough information to reason about the proof normalization process and other properties of the metatheory. A term assignment where complete information is recorded in the terms may be consulted in [10].

Free variables of validity ($\mathsf{FVV}(\bullet)$), truth ($\mathsf{FVT}(\bullet)$) and falsehood ($\mathsf{FVF}(\bullet)$), as well as free individual variables over terms are defined analogously to those for proof witnesses, and the notational conventions extend to terms as expected.

DEFINITION 5.3
Typing judgements in λ^{FOLP} take the form $\Theta; \Gamma; \Delta \vdash M^A \,|\, s$. The typing rules that define which such judgements are derivable are given in Figure 8. They arise from the inference schemes of FOHLP of Figure 2; hence every well-typed term encodes a derivation in FOHLP modulo the equivalence rules, and every FOHLP-derivation can be encoded by a term. In particular, note that if $\Theta; \Gamma; \Delta \vdash M^A \,|\, s$ is derivable with the typing rules of λ^{FOLP}, then $\Theta; \Gamma; \Delta \vdash A | s$ is derivable in FOHLP. We write

$\mathcal{H} \vdash M^A | s$ to abbreviate $\Theta; \Gamma; \Delta \vdash M^A | s$. Also, we write $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta \vdash M^A | s$ to indicate that the typing judgement $\Theta; \Gamma; \Delta \vdash M^A | s$ is derivable.

We now list some *substitution principles*.

Lemma 5.4 (Validity Variable Substitution)

(1) If both $\rhd_{\lambda\mathsf{FOLP}} \Theta, v^A_\Xi; \Gamma; \Delta \vdash M^B | s$ and $\rhd_{\lambda\mathsf{FOLP}} \Theta; \cdot; \cdot \vdash N^A | t$, then $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta \vdash M\{v^A_\Xi \leftarrow N^A, t\}^{B\{v^A_\Xi \leftarrow t\}} | s\{v^A_\Xi \leftarrow t\}$.

(2) If both $\rhd_{\mathsf{FOHLP}} \Theta, v^A_\Xi; \Gamma; \Delta \vdash s \equiv r : B$ and $\rhd_{\lambda\mathsf{FOLP}} \Theta; \cdot; \cdot \vdash N^A | t$, then $\rhd_{\mathsf{FOHLP}} \Theta; \Gamma; \Delta \vdash s\{v^A_\Xi \leftarrow t\} \equiv r\{v^A_\Xi \leftarrow t\} : B\{v^A_\Xi \leftarrow t\}$.

Lemma 5.5 (Validity Variable Substitution with Equivalence)
If

(1) $\rhd_{\lambda\mathsf{FOLP}} \Theta, v^A_\Xi; \Gamma; \Delta \vdash M^B | s$;
(2) $\rhd_{\lambda\mathsf{FOLP}} \Theta; \cdot; \cdot \vdash N^A | r$; and
(3) $\rhd_{\mathsf{FOHLP}} \Theta; \cdot; \cdot \vdash r \equiv t : A$,

then there exists s' such that:

(1) $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta \vdash M^B\{v^A_\Xi \leftarrow N^A, t\}^{B\{v^A_\Xi \leftarrow t\}} | s'$; and
(2) $\rhd_{\mathsf{FOHLP}} \Theta; \Gamma; \Delta \vdash s' \equiv s\{v^A_\Xi \leftarrow t\} : B\{v^A_\Xi \leftarrow t\}$.

Lemma 5.6 (Individual Variable Substitution)

(1) If $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta \vdash M^D | r$, then $\rhd_{\lambda\mathsf{FOLP}} \Theta\{i \leftarrow E\}; \Gamma\{i \leftarrow E\}; \Delta\{i \leftarrow E\} \vdash M\{i \leftarrow E\}^{D\{i \leftarrow E\}} | r\{i \leftarrow E\}$.

(2) If $\rhd_{\mathsf{FOHLP}} \Theta; \Gamma; \Delta \vdash r_1 \equiv r_2 : D$, then $\rhd_{\mathsf{FOHLP}} \Theta\{i \leftarrow E\}; \Gamma\{i \leftarrow E\}; \Delta\{i \leftarrow E\} \vdash r_1\{i \leftarrow E\} \equiv r_2\{i \leftarrow E\} : D\{i \leftarrow E\}$.

Lemma 5.7 (Truth Variable Substitution)
If $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma, y^A; \Delta \vdash M^B | s$ and $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta \vdash N^A | t$, then $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta \vdash M\{y^A \leftarrow N^A\}^B | s\{y^A \leftarrow t\}$.

Lemma 5.8 (Falsehood Variable Renaming)
If $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta, \alpha^A, \beta^A \vdash M^B | s$, then we also have $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta, \beta^A \vdash M\{\alpha^A \leftarrow \beta^A\}^B | s\{\alpha^A \leftarrow \beta^A\}$.

Lemma 5.9 (Structural Substitution)
If $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta, \alpha^{A \supset B} \vdash M^D | s$ and $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta \vdash N^A | t$, then $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta, \beta^B \vdash M(\!| [\alpha^{A \supset B}](\bullet) \leftarrow [\beta^B](\bullet) N^A |\!)^D | s(\!| [\alpha^{A \supset B}](\bullet) \leftarrow [\beta^B](\bullet) t |\!)$.

Lemma 5.10 (Inversion)
Suppose $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta \vdash N^D | r$.

- If $N^D = x^A$, then $x^A \in \Gamma$, $r = x^A$ and $D = A$;
- If $N^D = v^A_\Xi$, then $v^A_\Xi \in \Theta$, $r = v^A_\Xi$ and $D = A$;
- If $N^D = (\lambda x^A . M^B)^{A \supset B}$, then $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma, x^A; \Delta \vdash M^B | s$ for some s, $r = \lambda x^A . s$ and $D = A \supset B$;
- If $N^D = (M_1^{A \supset B} M_2^A)^B$, then both $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta \vdash M_1^{A \supset B} | s$ and $\rhd_{\lambda\mathsf{FOLP}} \Theta; \Gamma; \Delta \vdash M_2^A | t$ for some s and t, $r = s \cdot t$ and $D = B$;
- If $N^D = (!M^A)^{[[t]]_\Xi A}$, then both $\rhd_{\lambda\mathsf{FOLP}} \Theta; \cdot; \cdot \vdash M^A | s$ and $\rhd_{\mathsf{FOHLP}} \Theta; \cdot; \cdot \vdash s \equiv t : A$, for some s, $\mathsf{FIV}(\Theta) \cap \mathsf{FIV}(A) \subseteq \Xi$, $r = !t$ and $D = [[t]]_\Xi A$;

- If $N^D = (M_2^B \langle v^A_{\Xi'} {:=} r', M_1^{\llbracket r' \rrbracket \Xi A} \rangle)^{B\{v^A \leftarrow r^A\}}$, then both $\rhd_{\lambda\mathsf{FOLP}}\, \Theta; \Gamma; \Delta \vdash M_1^{\llbracket r' \rrbracket \Xi A} \,|\, s$ and $\rhd_{\lambda\mathsf{FOLP}}\, \Theta, v^A_{\Xi'}; \Gamma; \Delta \vdash M_2^B \,|\, t$ for some s and t, $r = t\langle v^A_{\Xi'} {:=} r, s\rangle$, $\Xi \cap \mathsf{FIV}(A) \subseteq \Xi'$ and $D = B\{v^A \leftarrow r^A\}$;
- If $N^D = ([\alpha^A]M^A)^{\bot}$, then $\exists\ \Delta', s$ s.t. $\Delta = \Delta', \alpha^A$, $\rhd_{\lambda\mathsf{FOLP}}\, \Theta; \Gamma; \Delta', \alpha^A \vdash M^A \,|\, s$, $r = [\alpha^A]s$, and $D = \bot$;
- If $N^D = (\mu\alpha^A.M^{\bot})^A$, then $\rhd_{\lambda\mathsf{FOLP}}\, \Theta; \Gamma; \Delta, \alpha^A \vdash M^{\bot} \,|\, s$ for some s, $r = \mu\alpha^A.s$, and $D = A$;
- If $N^D = (M^A +_{\mathrm{L}} t)^A$, then $\rhd_{\lambda\mathsf{FOLP}}\, \Theta; \Gamma; \Delta \vdash M^A \,|\, s$ for some s, $r = s + t$, and $D = A$;
- If $N^D = (s +_{\mathrm{R}} M^B)^B$, then $\rhd_{\lambda\mathsf{FOLP}}\, \Theta; \Gamma; \Delta \vdash M^B \,|\, t$ for some t, $r = s + t$, and $D = B$;
- If $N^D = (\mathsf{gen}_i(M^A))^{\forall i.A}$, then $\rhd_{\lambda\mathsf{FOLP}}\, \Theta; \Gamma; \Delta \vdash M^A \,|\, s$ for some s, $i \notin \mathsf{FIV}(\Theta, \Gamma, \Delta)$, $r = \mathsf{gen}_i(s)$ and $D = \forall i.A$;
- If $N^D = (\mathsf{ins}_i^E(M^{\forall i.A}))^{A\{i \leftarrow E\}}$, then $\rhd_{\lambda\mathsf{FOLP}}\, \Theta; \Gamma; \Delta \vdash M^{\forall i.A} \,|\, s$ for some s, $r = \mathsf{ins}_i^E(s)$ and $D = A\{i \leftarrow E\}$.

DEFINITION 5.11
Reduction in λ^{FOLP}, denoted $\to$, is defined as the compatible closure of the following two groups of rules:

- Principal rules:

$$\begin{array}{lcll}
\beta: (\lambda x^A.M^B)N^A & \to & M^B\{x^A \leftarrow N^A\} & \\
\mu: [\beta^A]\mu\alpha^A.M^{\bot} & \to & M^{\bot}\{\alpha^A \leftarrow \beta^A\} & \\
\zeta: (\mu\alpha^{A\supset B}.M^{\bot})N^A & \to & \mu\beta^B.M^{\bot}\llparenthesis [\alpha^{A\supset B}](\bullet) \leftarrow [\beta^B](\bullet)N^A \rrparenthesis & \\
\theta: \mu\alpha^A.[\alpha^A]M^A & \to & M^A, & \text{if } \alpha^A \notin \mathsf{FVF}(M^A) \\
\gamma: M^B\langle v^A_{\Xi} {:=} r, !N^A\rangle & \to & M^B\{v^A_{\Xi} \leftarrow N^A, r\}, & \text{if } \mathsf{FVT}(N^A) = \mathsf{FVF}(N^A) = \emptyset \\
\xi: \mathsf{ins}_i^E(\mathsf{gen}_i(M^A)) & \to & (M^A)\{i \leftarrow E\} &
\end{array}$$

- Permutative rules:

$$\begin{array}{lcll}
\psi_L: (M^{A\supset B} +_{\mathrm{L}} t)^{A\supset B} N^A & \to & (M^{A\supset B}N^A)^B +_{\mathrm{L}} t & \\
\psi_R: (s +_{\mathrm{R}} M^{A\supset B})^{A\supset B} N^A & \to & s +_{\mathrm{R}} (M^{A\supset B}N^A)^B & \\
\chi_L: [\beta^A](M^A +_{\mathrm{L}} t)^A & \to & ([\beta^A]M^A)^{\bot} +_{\mathrm{L}} t & \\
\chi_R: [\beta^B](s +_{\mathrm{R}} N^B)^B & \to & s +_{\mathrm{R}} ([\beta^B]N^B)^{\bot} & \\
\phi_L: M^B\langle v^A_{\Xi'} {:=} r, (N^{\llbracket r \rrbracket \Xi A} +_{\mathrm{L}} t)\rangle & \to & (M^B\langle v^A_{\Xi'} {:=} r, N^{\llbracket r \rrbracket \Xi A}\rangle)^{B\{v^A_{\Xi'} \leftarrow r^A\}} +_{\mathrm{L}} t & \\
\phi_R: M^B\langle v^A_{\Xi'} {:=} r, (s +_{\mathrm{R}} N^{\llbracket r \rrbracket \Xi A})\rangle & \to & s +_{\mathrm{R}} (M^B\langle v^A_{\Xi'} {:=} r, N^{\llbracket r \rrbracket \Xi A}\rangle)^{B\{v^A_{\Xi'} \leftarrow r^A\}} & \\
\epsilon_L: \mathsf{ins}_i^E(M^{\forall i.A} +_{\mathrm{L}} t) & \to & \mathsf{ins}_i^E(M^{\forall i.A}) +_{\mathrm{L}} t & \\
\epsilon_R: \mathsf{ins}_i^E(s +_{\mathrm{R}} M^{\forall i.A}) & \to & s +_{\mathrm{R}} \mathsf{ins}_i^E(M^{\forall i.A}) & \\
\iota_L: \mu\alpha^A.(M^{\bot} +_{\mathrm{L}} t)^{\bot} & \to & (\mu\alpha^A.M^{\bot}) +_{\mathrm{L}} t, & \text{if } \alpha^A \notin \mathsf{FVF}(t) \\
\iota_R: \mu\alpha^A.(s +_{\mathrm{R}} N^{\bot})^{\bot} & \to & s +_{\mathrm{R}} (\mu\alpha^A.N^{\bot}), & \text{if } \alpha^A \notin \mathsf{FVF}(s)
\end{array}$$

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. We write $\twoheadrightarrow$ for the reflexive-transitive closure of $\to$ and $\to^+$ for the transitive closure of $\to$. Rules μ, ζ and θ are inherited from Parigot's $\lambda\mu$-calculus. Rules β, γ and ξ encode proof normalization steps. For example, the γ rule encodes the step in which the derivation:

$$\dfrac{\dfrac{\dfrac{\pi_1}{\Theta;\cdot;\cdot\vdash N^A\,|\,r} \quad \Theta;\cdot;\cdot\vdash r\equiv t:A \quad \mathsf{FIV}(\Theta)\cap\mathsf{FIV}(A)\subseteq\Xi'}{\mathcal{H}\vdash(!N^A)^{[[t]]_{\Xi'}A}\,|\,!t}\,\Box\mathsf{I} \qquad \dfrac{\pi_2}{\mathcal{H},v^A_\Xi\vdash M^B\,|\,s} \quad \Xi\cap\mathsf{FIV}(A)\subseteq\Xi'}{\mathcal{H}\vdash M^B\langle v^A_\Xi:=t,!N^A\rangle^{B\{v^A_\Xi\leftarrow t\}}\,|\,s\langle v^A_\Xi:=t,!t\rangle}\,\Box\mathsf{E}$$

is transformed into the derivation given by the Validity Variable Substitution Principle (Lemma 5.4) applied to π_1 and π_2:

$$\mathcal{H}\vdash M\{v^A_\Xi\leftarrow N^A,t\}^{B\{v^A_\Xi\leftarrow t\}}\,|\,s',$$

where s' is equivalent to $s\{v^A_\Xi\leftarrow t\}$. The purpose of the permutative rules is to avoid operators '$+_L$' and '$+_R$' from blocking reductions. They push the sums outside, unveiling inner redexes. For example: $((\lambda x^A.y^B)^{A\supset B}+_{\mathrm{L}}t)^{A\supset B}z^A\to_{\psi_L}((\lambda x^A.y^B)^{A\supset B}z^A)^B+_{\mathrm{L}}t\to_\beta y^B+_{\mathrm{L}}t$.

5.1 *Basic results*

The relation $\to$ is confluent. This is a consequence of the fact that all critical pairs may be closed (*cf.* [14], where confluence of the term assignment for LP is proved; note moreover that no new critical pairs are added with respect to that system). Strong normalization of $\to$ is addressed in Section 5.2 (*cf.* Proposition 5.25). We now focus on type preservation and consistency of $\equiv$.

LEMMA 5.12
If $\Theta;\Gamma;\Delta\vdash M^A\,|\,s$ is derivable, then $\mathsf{FVT}(s)\subseteq\mathsf{FVT}(M^A)$ and $\mathsf{FVF}(s)\subseteq\mathsf{FVF}(M^A)$.

PROOF. By induction on the derivation of $\Theta;\Gamma;\Delta\vdash M^A\,|\,s$. The T-Var and T-VarM cases are straightforward. For T-□I, $\mathsf{FVT}(M^A)=\mathsf{FVF}(M^A)=\mathsf{FVT}(s)=\mathsf{FVF}(s)=\cdot$. In all other cases, the result is obtained by induction hypothesis and basic set operations. ■

LEMMA 5.13
If $\rhd_{\lambda\mathsf{FOLP}}\Theta;\Gamma;\Delta\vdash M^D\,|\,s$ and $M^D\to N^D$ by reducing a redex at the root of M^D, then $\rhd_{\lambda\mathsf{FOLP}}\Theta;\Gamma;\Delta\vdash N^D\,|\,s'$ for some witness s' such that $\Theta;\Gamma;\Delta\vdash s\equiv s':D$.

PROOF. By case analysis on the reduction rule that was used. We supply a sample case.

- γ: $M^D=M_1^B\langle v^A_{\Xi'}:=r,(!M_2^A)^{[[r]]_\Xi A}\rangle$, $N^D=M_1^B\{v^A_{\Xi'}\leftarrow M_2^A,r\}$ and $\mathsf{FVT}(M_2^A)=\mathsf{FVF}(M_2^A)=\emptyset$. By Inversion Lemma (twice), $D=B\{v^A_\Xi\leftarrow r\}$, $s=!r\langle v^A_{\Xi'}:=r,t\rangle$ and there is a witness r' such that $\mathsf{FIV}(\Theta)\cap\mathsf{FIV}(A)\subseteq\Xi$, $\Xi\cap\mathsf{FIV}(A)\subseteq\Xi'$, and $\Theta;\cdot;\cdot\vdash r'\equiv r:A$ as well as $\Theta;\cdot;\cdot\vdash M_2^A\,|\,r'$ and $\Theta,v^A_{\Xi'};\Gamma;\Delta\vdash M_1^B\,|\,t$ are derivable.

  By Lemma 5.5, we can derive $\Theta;\Gamma;\Delta\vdash M_1^B\{v^A_{\Xi'}\leftarrow M_2^A,r\}^{B\{v^A_{\Xi'}\leftarrow r\}}\,|\,s'$ and $\Theta;\Gamma;\Delta\vdash s'\equiv t\{v^A_{\Xi'}\leftarrow r\}:B\{v^A_{\Xi'}\leftarrow r\}$ for some witness s'; and, by Eq-Symm, we derive $\Theta;\Gamma;\Delta\vdash t\{v^A_{\Xi'}\leftarrow r\}\equiv s':B\{v^A_{\Xi'}\leftarrow r\}$. By Eq-$\gamma$ -since $\mathsf{FIV}(\Theta)\cap\mathsf{FIV}(A)\subseteq\Xi'$-, we can derive $\Theta;\Gamma;\Delta\vdash s\equiv t\{v^A_{\Xi'}\leftarrow r\}:B\{v^A_{\Xi'}\leftarrow r\}$. And finally, by Eq-Trans, $\Theta;\Gamma;\Delta\vdash s\equiv s':B\{v^A_{\Xi'}\leftarrow r\}$.

Note that s and s' are the same as the witnesses s and t for the corresponding equivalence rule from Lemma 3.11. ■

PROPOSITION 5.14 (Type Preservation)
If $\rhd_{\lambda\mathsf{FOLP}}\,\Theta;\Gamma;\Delta\vdash M^B\,|\,s$ and $M^B\to N^B$, then there exists a proof witness s' such that $\rhd_{\lambda\mathsf{FOLP}}\,\Theta;\Gamma;\Delta\vdash N^B\,|\,s'$ and $\rhd_{\mathsf{FOHLP}}\,\Theta;\Gamma;\Delta\vdash s\equiv s':B$.

PROOF. By induction on M^B. If the reduction takes place at the root, then the result holds by Lemma 5.13. We illustrate a sample case of an internal reduction.

- If $M^B=(!M_1^A)^{[[r]]_{\Xi}A}$: in this case $B=[[r]]_{\Xi}A$, $N^B=(!N_1^A)^{[[r]]_{\Xi}A}$ where $M_1^A\to N_1^A$ and, by the Inversion Lemma, there is a witness t such that both $\Theta;\cdot;\cdot\vdash M_1^A\,|\,t$ and $\Theta;\cdot;\cdot\vdash t\equiv r:A$ are derivable, $\mathsf{FIV}(\Theta)\cap\mathsf{FIV}(A)\subseteq\Xi$ and $s=!t$.
  By the induction hypothesis, we can derive $\Theta;\cdot;\cdot\vdash N_1^A\,|\,t'$ and $\Theta;\cdot;\cdot\vdash t\equiv t':A$.
  By $\mathsf{Eq\text{-}Symm}$ and $\mathsf{Eq\text{-}Trans}$, we obtain $\Theta;\cdot;\cdot\vdash t'\equiv r:A$. And, by $\mathsf{T\text{-}\Box I}$, $\Theta;\Gamma;\Delta\vdash (!N_1^A)^{[[r]]_{\Xi}A}\,|\,!r$. $\Theta;\Gamma;\Delta\vdash t'\equiv r:A$ is obtained by Weakening.

■

COROLLARY 5.15
If $\rhd_{\lambda\mathsf{FOLP}}\,\Theta;\Gamma;\Delta\vdash(!M^B)^A\,|\,t$ and $M^B\to N^B$, then $\Theta;\Gamma;\Delta\vdash(!N^B)^A\,|\,t$ is derivable.

PROOF. By the Inversion Lemma, $A=[[r]]_{\Xi}B$, $t=!r$ 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 5.14, there is an s' such that both $\Theta;\cdot;\cdot\vdash N^B\,|\,s'$ and $\Theta;\cdot;\cdot\vdash s'\equiv s:B$ are derivable, and $\Theta\cap\mathsf{FIV}(A)\subseteq\Xi$. 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 $\Theta;\Gamma;\Delta\vdash(!N^B)^{[[r]]_{\Xi}B}\,|\,!r$. ■

We now address consistency of proof witness equality $\mathcal{H}\vdash s\equiv t:A$. For this we first define the notion of proof witness associated with a term.

DEFINITION 5.16
The proof witness associated with a term M^A, denoted $\mathsf{w}(M^A)$, is defined as follows:

$$
\begin{array}{lcl}
\mathsf{w}(x^A) & \triangleq & x^A\\
\mathsf{w}(v^A_{\Xi}) & \triangleq & v^A_{\Xi}\\
\mathsf{w}((\lambda x^A.M^B)^{A\supset B}) & \triangleq & \lambda x^A.\mathsf{w}(M^B)\\
\mathsf{w}((M^{A\supset B}N^A)^B) & \triangleq & \mathsf{w}(M^{A\supset B})\cdot\mathsf{w}(N^A)\\
\mathsf{w}((!M^A)^{[[s]]_{\Xi}A}) & \triangleq & !s\\
\mathsf{w}((M^B\langle v^A_{\Xi'}:=r,N^{[[r]]_{\Xi}A}\rangle)^{B\{v^A_{\Xi'}\leftarrow r\}}) & \triangleq & (\mathsf{w}(M^B)\langle v^A_{\Xi'}:=r,\mathsf{w}(N^{[[r]]_{\Xi}A})\rangle)\\
\mathsf{w}(([\alpha^A]M^A)^{\perp}) & \triangleq & [\alpha^A]\mathsf{w}(M^A)\\
\mathsf{w}((\mu\alpha^A.M^{\perp})^A) & \triangleq & \mu\alpha^A.\mathsf{w}(M^{\perp})\\
\mathsf{w}((M^A+_{\mathrm{L}}t)^A) & \triangleq & \mathsf{w}(M^A)+t\\
\mathsf{w}((s+_{\mathrm{R}}N^B)^B) & \triangleq & s+\mathsf{w}(N^B)\\
\mathsf{w}((\mathsf{gen}_i(M^A))^{\forall i.A}) & \triangleq & \mathsf{gen}_i(\mathsf{w}(M^A))\\
\mathsf{w}((\mathsf{ins}_i^E(M^{\forall i.A}))^{A\{i\leftarrow E\}}) & \triangleq & \mathsf{ins}_i^E(\mathsf{w}(M^{\forall i.A}))
\end{array}
$$

REMARK 5.17
The proof witness $\mathsf{w}(M^A)$ associated with a term M^A is the only one such that the judgement $\Theta;\Gamma;\Delta\vdash M^A\,|\,\mathsf{w}(M^A)$ is derivable for some Θ,Γ,Δ.

LEMMA 5.18
If $\rhd_{\lambda\mathsf{FOLP}}\,\Theta;\Gamma;\Delta\vdash s\equiv t:B$, then there are terms M_1, M_2, M_3 s.t.:

(1) $\rhd_{\lambda\mathsf{FOLP}}\,\Theta;\Gamma;\Delta\vdash M_1^B\,|\,s$;

(2) $\rhd_{\lambda^{\mathsf{FOLP}}} \Theta;\Gamma;\Delta \vdash M_2^B \,|\, t$;
(3) $M_1 \twoheadrightarrow M_3$; and
(4) $M_2 \twoheadrightarrow M_3$.

PROOF. Since there may be more than one candidate for M_1 and M_2, we will assume that the derivations we are working with are **canonical** in the following sense:

- Whenever either (T-)PlusL or (T-)PlusR can be used to prove the same formula, we use (T-)PlusL. This eliminates the possibility of two different terms encoding a proof with a witness of the form $s'+t'$. (T-)PlusR may still be used to derive judgements of the form $\Theta';\Gamma';\Delta' \vdash (s' +_{\mathrm{R}} M^{A'})^{A'} \,|\, s'+t'$ when $\Theta';\Gamma';\Delta' \vdash A' \,|\, s'$ is not derivable.
- We use (T-)□I’ instead of (T-)□I, in order to avoid the possibility of multiple (in fact infinite) terms encoding a proof with a witness of the form $!s'$.

This way, if $\rhd_{\mathsf{FOHLP}} \Theta';\Gamma';\Delta' \vdash A \,|\, r$, there exactly one term M $\Theta';\Gamma';\Delta' \vdash M^A \,|\, r$ has a canonical derivation (this is straightforward by induction on s, since canonical derivations are syntax-driven). In order to preserve this invariant, we will ensure that the derivations we construct are also canonical in this sense (by using T-□I’ instead of T-□I, and not using T-PlusR unless this rule was used in the original derivation).
The proof is by induction on the derivation of $\Theta;\Gamma;\Delta \vdash s \equiv t : B$. We exhibit a sample case.

- Eq-γ: $s = t'\langle v^A_\Xi := s', !s' \rangle$, $t = t'\{v^A_\Xi \leftarrow s'\}$, $B = C\{v^A_\Xi \leftarrow s'\}$, both $\Theta;\cdot;\cdot \vdash N^A \,|\, s'$ and $\Theta, v^A_\Xi;\Gamma;\Delta \vdash M^C \,|\, t'$ are derivable by hypothesis for some M^C and N^A, and $\mathsf{FIV}(\Theta) \cap \mathsf{FIV}(A) \subseteq \Xi$.
Let $\Xi_1 = \mathsf{FIV}(\Theta)$. Since $\Xi_1 \cap \mathsf{FIV}(A) \subseteq \Xi_1$, then by T-□I, we get $\Theta;\Gamma;\Delta \vdash (!N^A)^{[[s']]_{\Xi_1} A} \,|\, !s'$ – note that we use the same proof witness s' on both sides of the equivalence, which is the same as using T-□I’, and thus the derivation is maintained canonical. Now, by T-□E, we can derive $\Theta;\Gamma;\Delta \vdash M^C \langle v^A_\Xi := s', (!N^A)^{[[s']]_{\Xi_1} A} \rangle^{C\{v^A_\Xi \leftarrow s'\}} \,|\, t' \langle v^A_\Xi := s', !s' \rangle$.
Take $M_1 = M^C \langle v^A_\Xi := s', (!N^A)^{[[s']]_{\Xi_1} A} \rangle$ and $M_2 = M_3 = M^C\{v^A_\Xi \leftarrow N^A, s'\}$.
The judgement $\Theta;\Gamma;\Delta \vdash M_2^{C\{v^A_\Xi \leftarrow s'\}} \,|\, t'\{v^A_\Xi \leftarrow s'\}$ can be obtained from $\Theta, v^A_\Xi;\Gamma;\Delta \vdash C \,|\, t'$ and the hypotheses by Lemma 3.9, and $M_1 \rightarrow_\gamma M_2$.

■

COROLLARY 5.19
The $\equiv$ theory for FOHLP is consistent.

PROOF. Suppose that we can derive $\cdot;\{x^A, y^A\};\cdot \vdash x^A \equiv y^A : A$. By Lemma 5.18, there are M_1, M_2 and M_3 oth $\cdot;\{x^A, y^A\};\cdot \vdash M_1^A \,|\, x^A$ and $\cdot;\{x^A, y^A\};\cdot \vdash M_2^A \,|\, y^A$ are derivable, and $M_1 \twoheadrightarrow M_3$ and $M_2 \twoheadrightarrow M_3$. By Remark 5.17, $x^A = \mathsf{w}(M_1)$ and $y^A = \mathsf{w}(M_2)$. By Definition 5.16, M_1 can only be x^A and M_2 can only be y^A. But both x^A and M_2 and y^A are normal forms, so M_3 cannot exist. Therefore, $\cdot;\{x^A, y^A\};\cdot \vdash x^A \equiv y^A : A$ is not derivable. Since $\cdot;\{x^A, y^A\};\cdot \vdash A \,|\, x^A$ and $\cdot;\{x^A, y^A\};\cdot \vdash A \,|\, y^A$ are both derivable (by Var), then the $\equiv$ theory is consistent. ■

5.2 *Strong normalization*

In order to prove strong normalization of term reduction, we follow our development for the propositional setting [14]. This relies on mapping λ^{FOLP}-terms into terms of Parigot’s $\lambda\mu$-calculus with unit type ($\lambda\mu^1$) and then resorting to the known fact that $\lambda\mu^1$ is SN. The reduction rules of

$\lambda\mu^{\mathsf{1}}$ with unit type are the same as those of $\lambda\mu$ (Section 1.3 plus β). $\lambda\mu^{\mathsf{1}}$-judgements take the form $M:\Gamma\vdash\Delta$, with M a $\lambda\mu^{\mathsf{1}}$-term, Γ a truth context and Δ a falsehood context. The typing rules are those introduced in Section 1.3 plus the axiom Unit that reads, $\texttt{unit}:\Gamma\vdash\mathbf{1};\Delta$.

The mapping $\llparenthesis\cdot\rrparenthesis$ associates types (formulas) and terms (proofs) in λ^{FOLP} with types and terms in $\lambda\mu^{\mathsf{1}}$. The modal type $[[s]]_{\Xi}A$ is mapped to a functional type whose domain is the unit type $\mathbf{1}$ and whose co-domain is the mapping of A. Since $\lambda\mu^{\mathsf{1}}$ has truth and falsehood variables but not validity variables, the mapping of validity variables will rely on a new set of truth variables in $\lambda\mu^{\mathsf{1}}$. Individual variables and expressions are ignored.

Definition 5.20
We first translate types:

$$\begin{array}{rcl}
\llparenthesis P(E)\rrparenthesis & \triangleq & P \\
\llparenthesis\bot\rrparenthesis & \triangleq & \bot \\
\llparenthesis A\supset B\rrparenthesis & \triangleq & \llparenthesis A\rrparenthesis\supset\llparenthesis B\rrparenthesis \\
\llparenthesis[[s]]_{\Xi}A\rrparenthesis & \triangleq & \mathbf{1}\supset\llparenthesis A\rrparenthesis \\
\llparenthesis\forall i.A\rrparenthesis & \triangleq & \mathbf{1}\supset\llparenthesis A\rrparenthesis.
\end{array}$$

For terms we translate as follows:

$$\begin{array}{rcll}
\llparenthesis x^{A}\rrparenthesis & \triangleq & x^{\llparenthesis A\rrparenthesis} & \\
\llparenthesis v^{A}_{\Xi}\rrparenthesis & \triangleq & (x_v^{\mathbf{1}\supset\llparenthesis A\rrparenthesis})\texttt{unit} & \\
\llparenthesis(\lambda x^{A}.M^{B})^{A\supset B}\rrparenthesis & \triangleq & \lambda x^{\llparenthesis A\rrparenthesis}.\llparenthesis M^{B}\rrparenthesis & \\
\llparenthesis(M^{A\supset B}N^{B})^{B}\rrparenthesis & \triangleq & \llparenthesis M^{A\supset B}\rrparenthesis\llparenthesis N^{B}\rrparenthesis & \\
\llparenthesis(!M^{A})^{[[s]]_{\Xi}A}\rrparenthesis & \triangleq & \lambda x^{\mathbf{1}}.\llparenthesis M^{A}\rrparenthesis x^{\mathbf{1}}, & x^{\mathbf{1}}\text{ fresh} \\
\llparenthesis(M^{B}\langle v^{A}_{\Xi'}:=r,N^{[[r]]_{\Xi}A}\rangle)^{B\{v^{A}_{\Xi'}\leftarrow r\}}\rrparenthesis & \triangleq & (\lambda x_v^{\mathbf{1}\supset\llparenthesis A\rrparenthesis}.\llparenthesis M^{B}\rrparenthesis)\llparenthesis N^{[[r]]_{\Xi}A}\rrparenthesis & \\
\llparenthesis([\alpha^{A}]M^{A})^{\bot}\rrparenthesis & \triangleq & [\alpha^{\llparenthesis A\rrparenthesis}]\llparenthesis M^{A}\rrparenthesis & \\
\llparenthesis(\mu\alpha^{A}.M^{\bot})^{A}\rrparenthesis & \triangleq & \mu\alpha^{\llparenthesis A\rrparenthesis}.\llparenthesis M^{\bot}\rrparenthesis & \\
\llparenthesis(M^{A}+_{\mathrm{L}}t)^{A}\rrparenthesis & \triangleq & \llparenthesis M^{A}\rrparenthesis & \\
\llparenthesis(s+_{\mathrm{R}}M^{A})^{A}\rrparenthesis & \triangleq & \llparenthesis M^{A}\rrparenthesis & \\
\llparenthesis\mathsf{gen}_i(M^{A})\rrparenthesis & \triangleq & \lambda x_i^{\mathbf{1}}.\llparenthesis M^{A}\rrparenthesis & \\
\llparenthesis\mathsf{ins}_i^{E}(M^{\forall i.A})\rrparenthesis & \triangleq & \llparenthesis M^{\forall i.A}\rrparenthesis\texttt{unit}. &
\end{array}$$

The translation maps typable λ^{FOLP}-terms to typable $\lambda\mu^{\mathsf{1}}$-terms, as expected. This result is proved by induction on the derivation of a given judgement $\Theta;\Gamma;\Delta\vdash M^{A}\,|\,s$ and relies on the fact that $\llparenthesis\bullet\rrparenthesis$ commutes with the various notions of substitutions.

Lemma 5.21
If $\rhd_{\lambda^{\mathsf{FOLP}}}\Theta;\Gamma;\Delta\vdash M^{A}\,|\,s$, then $\llparenthesis M\rrparenthesis:\llparenthesis\Theta\rrparenthesis\cup\llparenthesis\Gamma\rrparenthesis\vdash\llparenthesis A\rrparenthesis,\llparenthesis\Delta\rrparenthesis$ is derivable in $\lambda\mu^{\mathsf{1}}$.

Some sample cases of the proof are:

- Case $\mathsf{T\text{-}VarM}$: $M=v^{A}_{\Xi}$, $\Theta=\Theta',v^{A}_{\Xi}$, $\llparenthesis M\rrparenthesis=(x_v^{\mathbf{1}\supset\llparenthesis A\rrparenthesis})\texttt{unit}$ and $\llparenthesis\Theta\rrparenthesis=\llparenthesis\Theta'\rrparenthesis,x_v^{\mathbf{1}\supset\llparenthesis A\rrparenthesis}$. We can construct the following derivation in $\lambda\mu^{\mathsf{1}}$:

$$\dfrac{\dfrac{}{x_v^{\mathbf{1}\supset\llparenthesis A\rrparenthesis}:\llparenthesis\Theta'\rrparenthesis,x_v^{\mathbf{1}\supset\llparenthesis A\rrparenthesis}\cup\llparenthesis\Gamma\rrparenthesis\vdash\mathbf{1}\supset\llparenthesis A\rrparenthesis,\llparenthesis\Delta\rrparenthesis}\,\mathsf{Ax}\qquad\dfrac{}{\texttt{unit}:\llparenthesis\Theta'\rrparenthesis,x_v^{\mathbf{1}\supset\llparenthesis A\rrparenthesis}\cup\llparenthesis\Gamma\rrparenthesis\vdash\mathbf{1},\llparenthesis\Delta\rrparenthesis}\,\mathsf{Unit}}{(x_v^{\mathbf{1}\supset\llparenthesis A\rrparenthesis})\texttt{unit}:\llparenthesis\Theta'\rrparenthesis,x_v^{\mathbf{1}\supset\llparenthesis A\rrparenthesis}\cup\llparenthesis\Gamma\rrparenthesis\vdash\llparenthesis A\rrparenthesis,\llparenthesis\Delta\rrparenthesis}\,{\supset}\mathsf{E}$$

- Case $\mathsf{T}\text{-}\Box\mathsf{I}$: $M = (!N^B)^{[[r]]_\Xi B}$, $A = [[r]]_\Xi B$, $\Theta = \Theta_1 \cup \Theta_2$, $\llparenthesis M \rrparenthesis = \lambda x^{\mathbf{1}}.\llparenthesis N^B \rrparenthesis$, $\llparenthesis A \rrparenthesis = \mathbf{1} \supset \llparenthesis B \rrparenthesis$ and, by Weakening and the induction hypothesis, $\llparenthesis N^B \rrparenthesis : \llparenthesis \Theta \rrparenthesis \vdash \llparenthesis B \rrparenthesis$ is derivable in $\lambda\mu^1$. We can derive $\lambda x^{\mathbf{1}}.\llparenthesis N^B \rrparenthesis : \llparenthesis \Theta \rrparenthesis \vdash \mathbf{1} \supset \llparenthesis B \rrparenthesis$ by Weakening and $\supset\mathsf{I}$, and then obtain $\lambda x^{\mathbf{1}}.\llparenthesis N^B \rrparenthesis : \llparenthesis \Theta \rrparenthesis \cup \llparenthesis \Gamma \rrparenthesis \vdash \mathbf{1} \supset \llparenthesis B \rrparenthesis, \llparenthesis \Delta \rrparenthesis$ by Weakening.
- Case $\mathsf{T}\text{-}\Box\mathsf{E}$: $(M = M_1^C \langle v_r^B := \Xi', M_2^{[[r]]_\Xi B} \rangle)^{C\{v_{\Xi'}^B \leftarrow r\}}$, $A = C\{v_{\Xi'}^B \leftarrow r\}$, $\llparenthesis M \rrparenthesis = \lambda x_v^{\mathbf{1} \supset \llparenthesis B \rrparenthesis}.\llparenthesis M_2^{[[r]]_\Xi B} \rrparenthesis \llparenthesis M_1^C \rrparenthesis$. Note that $\llparenthesis A \rrparenthesis = \llparenthesis C \rrparenthesis$. This follows from the fact that $\llparenthesis C\{v_\Xi^A \leftarrow r\} \rrparenthesis = \llparenthesis C \rrparenthesis$. We can construct the following derivation: It may be proved by exhibiting a polynomial interpretation over the non-negative integers that ensures that reduction terminates.

LEMMA 5.22
For all λ^{FOLP}-terms M and N, if $M \to N$ in λ^{FOLP} *without* the use of permutative rules, then $\llparenthesis M \rrparenthesis \to^+ \llparenthesis N \rrparenthesis$ in $\lambda\mu^1$. That is, $\llparenthesis M \rrparenthesis$ reduces to $\llparenthesis N \rrparenthesis$ in 1 or more steps.

LEMMA 5.23
For all λ^{FOLP}-terms M and N, if $M \to N$ in λ^{FOLP} using *only* permutative rules, then $\llparenthesis M \rrparenthesis = \llparenthesis N \rrparenthesis$.

One last result before proceeding to the proof of SN. It may be proved by exhibiting a polynomial interpretation over the non-negative integers that ensures that reduction terminates.

LEMMA 5.24
Permutative reduction is SN.

PROPOSITION 5.25
Every typable λ^{FOLP}-term is SN.

PROOF. By contradiction. Assume that there is an infinite reduction sequence starting from a typable λ^{FOLP}-term M_0. We distinguish between principal reductions ($\xrightarrow{\text{B}}$) and permutative reductions ($\xrightarrow{\text{P}}$) within this sequence. Since, by Lemma 5.24, 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:

$$M_0 \overset{\text{P}}{\twoheadrightarrow} M_0' \xrightarrow{\text{B}} M_1 \overset{\text{P}}{\twoheadrightarrow} M_1' \xrightarrow{\text{B}} M_2 \overset{\text{P}}{\twoheadrightarrow} M_2' \xrightarrow{\text{B}} \cdots$$

Additionally, by Lemma 5.23, $\llparenthesis M_i \rrparenthesis = \llparenthesis M_i' \rrparenthesis$ for every i. Also, by Lemma 5.22, we know that for every i, $\llparenthesis M_i \rrparenthesis \to^+ \llparenthesis M_{i+1} \rrparenthesis$ in $\lambda\mu^1$. We can therefore construct an infinite $\lambda\mu^1$-reduction sequence:

$$\llparenthesis M_0 \rrparenthesis \to^+ \llparenthesis M_1 \rrparenthesis \to^+ \llparenthesis M_2 \rrparenthesis \to^+ \cdots$$

However, M_0 is typable in λ^{FOLP} and, by Proposition 5.14, so is every M_i. Since the mapping preserves typability (Lemma 5.21), then we have an infinite reduction sequence of typable $\lambda\mu^1$-terms. This is absurd, since reduction of typable $\lambda\mu^1$-terms is SN. Therefore, there cannot be an infinite reduction sequence starting from a typable λ^{FOLP}-term. ■

6 Related work

Modal Logic. There are numerous efforts in uncovering computational interpretations of modal logic. Among those we know of, we mention those we consider most relevant.

In [20], Kripke models were given a process interpretation, in which models were viewed as collections of computational states, and the binary relations as computational actions that transform one state into another. This interpretation—along with the knowledge interpretation, among others—is discussed further in [15].

[39] introduced $\lambda^{\rightarrow\Box}$, a proof term calculus for the intuitionistic modal logic $\mathsf{S4}$, which was further developed in [18, 19] to serve as a model for staged computation. Pfenning and Davies also introduced a functional language based on $\lambda^{\rightarrow\Box}$, named $\mathtt{Mini\text{-}ML}^{\Box}$.

[29] introduced a set of modal typed λ-calculi, based on natural deduction presentations of positive fragments of the modal logics K, $\mathsf{K4}$, KT and $\mathsf{S4}$. The authors proved the confluence and normalization of the respective reductions.

In [41], a modal logic of belief is used as a base to construct models of distributed systems, where axioms can be added to the logic and treated as *trust specifications*. Thus modal formulas are used to model trust and security issues in a distributed system.

[31] provided a new interpretation of modal logic $\mathsf{S4}$, in which the $\Box$ and $\Diamond$ modalities also describe mobility and locality in a distributed computation. Based on Kripke's 'possible worlds' semantics, worlds are seen as processes in a spatially distributed configuration. Here necessity describes a term that is well-typed *anywhere*, and possibility a term that is well-typed *somewhere*. This way, typing is used to determine the permissible mobility of terms among processes. This type theory characterizing the mobility and locality of program terms in a distributed computation was further developed in [30]. A similar interpretation, based on $\mathsf{S5}$, was used in [33] to introduce *Lambda 5*, a foundational language for spatially distributed programming which also addresses both mobility of code and locality of resources.

In [24], a new intuitionistic (hybrid) modal logic is defined, and its proofs are interpreted as distributed programs. Their logic is used to model remote procedure calls, broadcast commands, commands to use portable code, and invocation of agents which can find their way to safe locations for their execution.

Logic of proofs. There is less work in the case of LP.

A lambda calculus where information on *how* a result is computed (cf. Lévy labelling [27]) rather than just *what* the result is, dubbed the *intensional lambda calculus*, is explored in [5] via the Curry–Howard methodology.

A calculus with *computation trails* [10, 11]. The judgement $\Theta;\Gamma\vdash s\equiv t:B$ is encoded and reflected in the term assignment for $\Box\mathsf{I}$ and understood as a computation trail or computation history with applications to modeling history-based access control [6] and history-based information flow [12].

A calculus of *certified mobile units* which enriches mobile code with certificates (representing type derivations) is presented in [13]. 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.

Also there is [25]. That work introduces a modal logic of *interactive proofs* with the purpose of modelling communication within a multi-agent environment. In this setting, proofs are seen as messages shared by agents with partial knowledge yet unlimited computing capabilities, each agent serving as an oracle for the others, with only the communication medium having perfect knowledge. Proofs depend on the agents' knowledge, which is expanded through interaction with other agents. All logical conclusions of known facts are assumed to be known. Variants of this logic are developed in [26].

7 Conclusions and future work

We have developed a presentation of FOLP based on hypothetical reasoning, dubbed FOHLP. The work builds, on the one hand, on Parigot's Classical Natural Deduction and, on the other, on prior work on hypothetical presentations of (Propositional) LP [5, 10, 13, 14]. This yields a Natural Deduction formalism for proving FOLP theorems. A term assignment is proposed whose reduction rules arise from normalization of derivations in FOHLP: derivations are represented as terms and normalization steps on derivations are encoded as reduction steps over terms. The resulting lambda calculus, the λ^{FOLP}-calculus, is shown to enjoy Type Preservation and Strong Normalization. Regarding avenues for further research, we mention the following.

LP and FOLP through Contextual Modal Type Theory. Inference schemes in Natural Deduction presentations typically uphold the invariant that all free variables are declared in the hypotheses. The PlusL scheme:

$$\frac{\Theta;\Gamma;\Delta\vdash A\,|\,s}{\Theta;\Gamma;\Delta\vdash A\,|\,s+t}\,\mathsf{PlusL}$$

fails in this respect. Although we have argued (*cf.* Section 3) that this is required in order to prove all FOLP-theorems in FOHLP, it seems reasonable to explore truth dependent modalities [35] at the possible cost of capturing a subset of LP-theorems. The modality $\Box A$ is replaced by $[\Gamma]A$ which informally may be read as $\Box(\Gamma\supset A)$. That is, validity of A is dependent on the truth of the hypotheses in Γ. A sample of three inference schemes of the resulting *Contextual Modal Logic* [35] are as follows:

$$\frac{\Theta;\Gamma_1\vdash A}{\Theta;\Gamma_2\vdash[\Gamma_1]A}\,\Box\mathsf{I}\qquad\frac{\Theta;\Gamma_1\vdash[\Gamma_2]A\quad \Theta,v::A[\Gamma_2];\Gamma_1\vdash C}{\Theta;\Gamma_1\vdash C}\,\Box\mathsf{E}^v$$

$$\frac{\Theta_1,v::A[\Gamma_1],\Theta_2;\Gamma_2\vdash\Gamma_1}{\Theta_1,v::A[\Gamma_1],\Theta_2;\Gamma_2\vdash A}\,\mathsf{mvar}$$

Rather than proving **A4** (*i.e.* $[[t]]A\supset[[s+t]]A$) one would prove a formula of the form:

$$[[\Gamma,\Delta.s]]A\supset[[\Gamma,\Delta.s+t]]A$$

Note that t would be allowed to have free variables in Γ,Δ.

Logical framework based on FOHLP. It would be interesting to develop a logical framework based on FOHLP. The Beluga framework [40] may provide relevant inspiration for this purpose, since Beluga itself is based on [35], and it allows the use of multiple contexts as well as dependent types.

Type inference techniques for realization. We think that a fresh look at the realization of S4 in the setting of HLP [14] and FOHLP could be an interesting avenue for exploration. It should be noted that this is a non-trivial problem in the presence of inference schemes which mix polarities such as $\supset$E, hence the reason why the first such proof [1, 3] relied on a cut-free sequent calculus presentation of LP. Indeed, all known realization proofs, to the best of the authors' knowledge, rely on presentations where related[9] occurrences of a □ do *not* occur both in positive and negative positions. We think it could be interesting to put the well-developed type-inference technology to work *but*

[9] See notion of 'family' in [1].

to infer the decorations of boxes rather than to infer types. We suspect relations with higher-order unification may appear along the way.

Natural Deduction for other justification logics. Adapt the ideas of this article to other justification logics.

Acknowledgements

To LIA INFINIS and PICT 2012-2747 (Agencia Nacional de Promoción Científica y Tecnológica, Ministerio de Ciencia, Tecnología e Innovación Productiva).

References

[1] S. N. Artëmov. Explicit provability and constructive semantics. *Bulletin of Symbolic Logic*, **7**, 1–36, 2001.

[2] S. Artemov. Justification logic. In *Logics in Artificial Intelligence*, Vol. 5293 of *Lecture Notes in Computer Science*, S. Hlldobler, C. Lutz and H. Wansing, eds, pp. 1–4. Springer, 2008.

[3] S. N. Artëmov. Operational modal logic. *Technical Report MSI 95-29*, Cornell University, 1995.

[4] S. N. Artëmov. The logic of justification. *The Review of Symbolic Logic*, **1**, 477–513, 2008.

[5] S. N. Artëmov and E. Bonelli. The intensional lambda calculus. In *LFCS*, pp. 12–25. Springer, 2007.

[6] M. Abadi and C. Fournet. Access control based on execution history. In *Proceedings of the 10th Annual Network and Distributed System Security Symposium*, pp. 107–121. The Internet Society, 2003.

[7] S. N. Artëmov and R. Iemhoff. The basic intuitionistic logic of proofs. *Journal of Symbolic Logic*, **72**, 439–451, 2007.

[8] S. N. Artëmov and T. Yavorskaya (Sidon). On first order logic of proofs. *Moscow Mathematical Journal*, **1**, 475–490, 2001.

[9] S. N. Artëmov and T. Yavorskaya (Sidon). First-order logic of proofs. *Technical Report TR–2011005*, CUNY Ph.D. Program in Computer Science, 2011.

[10] F. Bavera and E. Bonelli. Justification logic and history based computation. In *ICTAC*, pp. 337–351. Springer, 2010.

[11] F. Bavera and E. Bonelli. Justification logic and audited computation. *Journal of Logic and Computation*, 2015. doi: 10.1093/logcom/exv037.

[12] A. Banerjee and D. A. Naumann. 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, 2005.

[13] E. Bonelli and F. Feller. Justification logic as a foundation for certifying mobile computation. *Annals of Pure and Applied Logic*, **163**, 935–950, 2012.

[14] E. Bonelli and G. Steren. Hypothetical logic of proofs. *Logica Universalis*, **8**, 103–140, 2014.

[15] P. Blackburn, J. Van Benthem et al. Modal logic: a semantic perspective. *Handbook of Modal Logic*, **3**, 1–84, 2006.

[16] E. Dashkov. Arithmetical completeness of the intuitionistic logic of proofs. *Journal of Logic and Computation*, **21**, 665–682, 2011.

[17] R. Davies and F. Pfenning. A judgmental reconstruction of modal logic. *Mathematical Structures in Computer Science*, **11**, 511–540, 2001.

[18] R. Davies and F. Pfenning. A modal analysis of staged computation. In *POPL*, pp. 258–270, 1996.

[19] R. Davies and F. Pfenning. A modal analysis of staged computation. *Journal of ACM*, **48**, 555–604, 2001.

[20] E. W. Dijkstra. *A Discipline of Programming*, Vol. 4. Prentice-Hall Englewood Cliffs, 1976.

[21] M. Fitting. Possible world semantics for first-order logic of proofs. *Annals of Pure and Applied Logic*, **165**, 225–240, 2014.

[22] H. Geuvers and G. I. Jojgov. Open proofs and open terms: a basis for interactive logic. In *Computer Science Logic, 16th International Workshop, CSL 2002, 11th Annual Conference of the EACSL, Edinburgh, Scotland, UK, September 22–25, 2002, Proceedings*, Vol. 2471 of *Lecture Notes in Computer Science*, J. C. Bradfield, ed., pp. 537–552. Springer, 2002.

[23] K. Gödel. Eine interpretation des intuitionistischen aussagenkalküls. *Ergebnisse eines mathematischen Kolloquiums*, **4**, 39–40, 1933.

[24] L. Jia and D. Walker. Modal proofs as distributed programs. In *Programming Languages and Systems*, Vol. 2986 of *Lecture Notes in Computer Science*, D. Schmidt, ed., pp. 219–233. Springer, 2004.

[25] S. Kramer. A logic of interactive proofs (formal theory of knowledge transfer). *arXiv preprint arXiv:1201.3667*, 2012.

[26] S. Kramer. Logic of negation-complete interactive proofs (formal theory of epistemic deciders). *Electronic Notes in Theoretical Computer Science*, **300**, 47–70, 2014.

[27] J.-J. Lévy. *Réductions correctes et optimales dans le lambda-calcul*. PhD Thesis, Paris 7, 1978.

[28] P. Martin-Löf. *An Intuitionistic Theory of Types*. Bibliopolis, 1984.

[29] S. Martini and A. Masini. A computational interpretation of modal proofs. In *Proof Theory of Modal Logic*, H. Wansing, ed., pp. 213–241. Springer, 1996.

[30] J. Moody. Logical mobility and locality types. In *Logic Based Program Synthesis and Transformation*, Vol. 3573 of *Lecture Notes in Computer Science*, S. Etalle, ed., pp. 69–84. Springer, 2005.

[31] J. Moody. Modal logic as a basis for distributed computation. *Technical Report CMU-CS-03-194*, Carnegie Mellon University, 2003.

[32] D. Miller and A. Tiu. A proof theory for generic judgments. *ACM Transactions on Computational Logic*, **6**, 749–783, 2005.

[33] T. Murphy, K. Crary, R. Harper, F. Pfenning et al. A symmetric modal lambda calculus for distributed computing. In *Logic in Computer Science, 2004. Proceedings of the 19th Annual IEEE Symposium on*, pp. 286–295. IEEE, 2004.

[34] J. C. C. McKinsey and A. Tarski. Some theorems about the sentential calculi of lewis and heyting. *The Journal of Symbolic Logic*, **13**, 1–15, 1948.

[35] A. Nanevski, F. Pfenning and B. Pientka. Contextual modal type theory. *ACM Transactions on Computational Logic*, **9**, 23:1–23:49, 2008.

[36] I. E. Orlov. The logic of compatibility of propositions. *Matematicheskii Sbornik*, **35**, 263–286, 1925.

[37] M. Parigot. $\lambda\mu$-calculus: an algorithmic interpretation of classical natural deduction. In *Logic Programming and Automated Reasoning*, Vol. 624 of *Lecture Notes in Computer Science*, A. Voronkov, ed., pp. 190–201. Springer, 1992.

[38] M. Parigot. Proofs of strong normalisation for second order classical natural deduction. *The Journal of Symbolic Logic*, **62**, 1461–1479, 1997.

[39] F. Pfenning and H.-C. Wong. On a modal λ-calculus for s4. *Electronic Notes in Theoretical Computer Science*, **1**, 515–534, 1995.

[40] B. Pientka. Beluga: programming with dependent types, contextual data, and contexts. In *Functional and Logic Programming*, M. Blume, N. Kobayashi and G. Vidal, eds, pp. 1–12. Springer, 2010.

[41] P. V. Rangan. An axiomatic basis of trust in distributed systems. In *Security and Privacy, 1988. Proceedings, 1988 IEEE Symposium on*, pp. 204–211. IEEE, 1988.

[42] A. Saurin. On the relations between the syntactic theories of lambda-mu-calculi. In *Computer Science Logic, 22nd International Workshop, CSL 2008, 17th Annual Conference of the EACSL, Bertinoro, Italy, September 16–19, 2008. Proceedings*, Vol. 5213 of *Lecture Notes in Computer Science*, M. Kaminski and S. Martini, eds, pp. 154–168. Springer, 2008.

[43] A. Saurin. Typing streams in the $\lambda\mu$-calculus. *ACM Transactions on Computational Logic (TOCL)*, **11**, 28, 2010.

[44] R. M. Solovay. Provability interpretations of modal logic. *Israel Journal of Mathematics*, **25**, 287–304, 1976.

[45] M. H. Sørensen and P. Urzyczyn. *Lectures on the Curry–Howard isomorphism*, Vol. 149 of *Studies in Logic and the Foundations of Mathematics*. Elsevier Science, 2006.

[46] R. E. Yavorsky. On arithmetical completeness of first-order logics of provability. In *Advances in Modal Logic 3, Papers from the Third Conference on 'Advances in Modal logic', held in Leipzig (Germany) in October 2000*, F. Wolter, H. Wansing, M. de Rijke and M. Zakharyaschev, eds, pp. 1–16. World Scientific, 2000.

[47] R. E. Yavorsky. Provability logics with quantifiers on proofs. *Annals of Pure and Applied Logic*, **113**, 373–387, 2001.

Received 14 December 2014