
Submitted Version
Available from Middlesex University's Research Repository at http://eprints.mdx.ac.uk/13947/

Copyright:
Middlesex University Research Repository makes the University's research available electronically.

Copyright and moral rights to this thesis/research project are retained by the author and/or other copyright owners. The work is supplied on the understanding that any use for commercial gain is strictly forbidden. A copy may be downloaded for personal, non-commercial, research or study without prior permission and without charge. Any use of the thesis/research project for private study or research must be properly acknowledged with reference to the work’s full bibliographic details.

This thesis/research project may not be reproduced in any format or medium, or extensive quotations taken from it, or its content changed in any way, without first obtaining permission in writing from the copyright holder(s).

If you believe that any material held in the repository infringes copyright law, please contact the Repository Team at Middlesex University via the following email address:
eprints@mdx.ac.uk

The item will be removed from the repository while any claim is being investigated.
J-Calc: A typed lambda calculus for Intuitionistic Justification Logic

Konstantinos Pouliasis\textsuperscript{1,2,5}

\textit{Department of Computer Science}
\textit{The Graduate Center at City University of New York, NY, USA}

Giuseppe Primiero\textsuperscript{3,4,5}

\textit{Department of Computer Science}
\textit{Middlesex University}
\textit{United Kingdom}

Abstract

In this paper we offer a system J-Calc that can be regarded as a typed \( \lambda \)-calculus for the \( \{\to, \bot\} \) fragment of Intuitionistic Justification Logic. We offer different interpretations of J-Calc, in particular, as a two phase proof system in which we proof check the validity of deductions of a theory \( T \) based on deductions from a stronger theory \( T' \) and computationally as a type system for separate compilations. We establish some first metatheoretic results.

Keywords: Typed \( \lambda \)-calculus, Justification Logic, Modular Programming.

1 Introduction

A plausible reading of Gödel’s incompleteness results ([18]) is that the notion of “validity” diverges from that of “truth within a specific theory”: given a theory that includes enough arithmetic, there are statements whose validity can only be established in a theory of larger proof-strength. This phenomenon can be shown even

\textsuperscript{1} This research is part of Konstantinos Pouliasis’ PhD study as a Enhanced Chancellor Fellow at the Graduate Center of the City University of New York under the supervision of Prof. Sergei Artemov. He is indebted to Prof. Sergei Artemov’s advisement and guidance during his academic journey.

\textsuperscript{2} Email: Kpouliasis@gc.cuny.edu

\textsuperscript{3} This research was conducted while Giuseppe Primiero was a Post-Doctoral Fellow of the Research Foundation Flanders (FWO) at the Centre for Logic and Philosophy of Science, Ghent University Belgium. He gratefully acknowledges the financial support.

\textsuperscript{4} Email: G.Primiero@mdx.ac.uk

\textsuperscript{5} Both authors are indebted to the constructive comments of the anonymous referees of the Intuitionistic Modal Logic and Applications Workshop, 2013.
with non-Gödelian arguments in the relation e.g. between \( \Delta_0 \) and \( \Sigma_1 \) arithmetic \cite{27}, \( \Sigma_1 \) and PA, PA and ZF, etc. \cite{29,15}. The very same issues arise in automated theorem proving. A good example is given by type systems and interactive theorem provers (e.g. Coq, Agda) of the typed functional paradigm. In such systems, when termination of functions has to be secured, one might need to invoke stronger proof principles. The need for reasoning about two kinds of proof objects within a type system is apparent most of all when one wants to establish non-admissibility results for a theory \( T \) that can, in contrast, be proved in some stronger \( T' \). The type system, then, has to reconcile the existence of a proof object of some type \( \phi \) in some \( T' \) and a proof object of type \( \neg \exists s. Prov_T(s, \phi) \) that witnesses the non-provability of \( \phi \) (in \( T \)).

In this work, we argue that the explicit modality of Justification Logic \cite{7} can be used to axiomatize relations between objects of two different calculi such as those mentioned above. It is well known that the provability predicate can be axiomatized using a modality \cite{14}, \cite{9}. The Logic of Proofs \( \text{LP} \) \cite{3} goes further and provides explicit proof terms (proof polynomials) to inhabit judgments on validity. By translating reasoning in Intuitionistic Propositional Calculus (IPC) to classical proofs, \( \text{LP} \) obtains a classical semantics for IPC through a modality (inducing a BHK semantics). In this paper we axiomatize the relation between the two kinds of proof objects explicitly, by creating a modal type theory that reasons about bindings or linking of objects from two calculi: a lower-level theory \( T \), formulated as IPC with Church-style \( \lambda \)-terms representing intuitionistic proof objects; and a higher-level, possibly stronger and classical (co-)theory \( T' \) fixed as foundational, with justifications expressing its proof objects. The axiomatization of such a (co-)theory follows directly the proof system of Justification Logic (here restricted to its applicative \( K \)-fragment) and is used to interpret classically (meaning truth-functionally) the constructions of the intuitionistic natural deduction. The underlying principle of our linking system is as follows:

\[
\text{constructive necessity} = \text{admissible validity} = \text{truth (in } T \text{)} + \text{validity (in } T' \text{)}
\]

Necessity of a true (in \( T \)) proposition \( P \) is, thus, sensitive to the existence of a proof (witnessed by a justification) of its intended interpretation within \( T' \). We assume an interpretation function on types \( \text{Just} \) that maps the type universe of \( T \) into the type universe of \( T' \). We employ judgments of the kind \( M : P \) (read as “\( M \) is a proof of type \( P \) in \( T' \)”)) that represent truths in \( T \) and judgments of the kind \( j : \text{Just } P \) (to be read as ”\( j \) is a justification of the interpretation of \( P \) in \( T' \)”)) that represent truth in \( T' \) (validity). Incorporating them, the principle can be rewritten in a judgmental fashion:

\[
M : P + j : \text{Just } P \Rightarrow \Box^j P \text{ true }
\]

Notice that the \( \Box \)-types are indexed by justifications (\( \Box^j P \)) being sensitive to the interpretation (\( T' \)) chosen. To complete the picture we need canonical elements of \( \Box^j \)-types. Naturally, witnesses of this kind are \textit{links} between proof objects from \( T \).
and $T'$ with corresponding types ($P$ and $\text{Just } P$). For that reason we introduce a linking witness constructor $\text{Link}$. This is how necessity is introduced: by proof-checking deductions of $T$ with deductions of $T'$, we reason constructively about admissibility of valid (via $T'$) statements in $T$. The principle thus becomes:

$$M : P + j : \text{Just } P \Rightarrow \text{Link}(M, j) : \Box P$$

We show how this principle is admissible in our system.

A possible application of the presented type theory can be a refined type system for programming languages with modular programming constructs or external function calls as we show in section 5. In these kinds of languages (e.g. of the ML family) a program or module can call for external definitions that are implemented elsewhere (in another module or, even in another language). We can read functions within $\Box$-types indexed by justifications as linking processes for such languages that perform the mapping of well–typed constructs importing and using module signatures into their residual programs. By residual programs we mean programs where all instances of module types and function calls are replaced by (i.e. linked to) their actual implementations, which remain hidden in the module. We show with a real example how, with slight modifications, our type system can find a natural application in this setting. Here we focus on the type system itself and not on its operational semantics.

The backbone of this work is the idea of representing the proof theoretic semantics for IPC through modality that stems from [5], [6]. An operational approach to modality related to this work can be found in [4]. The modularity of LP, i.e. its ability to realize other kinds of modal reasoning with proper changes in the axiomatization of proof polynomials, was shown with the development of the family of Justification Logics [7]. This ability is easily seen to be preserved here. Our work incorporates the rich type system and modularity of Justification Logic within the proofs-as-programs doctrine. For that reason, we obtain an extension of the Curry-Howard correspondence ([30], [17]) and adopt the judgmental approach of Intuitionistic Type Theory ([21], [22], [23], [25], [11]). Our system borrows from other modal calculi developed within the judgmental approach (e.g. [28], [19], [1] and especially [13] for the modal logic $K$). A main difference of our system with those systems, as well as with previous $\lambda$-calculi for LP ([2], [10]) is that our type system hosts a two-kinded typing relation for proof objects of corresponding formulae. It can be viewed as an attempt to add proof terms for validity judgments as presented in [28]. The resulting type system adopts dependent typing ([12], [26]) to relate the two kinds of proof objects with modality. The construction of the type universe as well as of justificational terms draws a lot from ideas in [8] and from [16]. Extending typed modal calculi with additional (contextual) terms of dependent typing can be also found in [24].

---

\[ \text{See [20].} \]
2 A road map for the type system

The present system can be viewed as a calculus of reasoning in three interleaving phases. Firstly, reasoning about proof objects in the implicational fragment of an intuitionistic theory $T$ in absence of any metatheoretic assumptions of validity, introduced in Section 3. This calculus is formalized by the turnstile $\Gamma \vdash_{IPC}^7$ where $\Gamma$ contains assumptions on proofs of sentences in $T$. The underlying logic is intuitionistic, the system corresponding to the implicational fragment of simply typed lambda calculus. Secondly, reasoning with justifications, corresponding to reasoning about proof objects in some fixed foundational system: the (co-)theory $T'$, introduced in Section 4. We suppose that $T'$ provides the intended semantics for the intuitionistic system $T$. The corresponding turnstile is $\Delta \vdash J$. Abstracting from any specific metatheory, all that matters from a purely logical point of view is that the theory of the interpretation should – at least – include as much logic as the implicational fragment of $T$ and it should satisfy some minimal conditions for the provability predicate of $T$. Finally, reasoning about existence of links between proof objects in the implicational fragment of both axiomatic systems, introduced in Section 6. This mode of reasoning is axiomatized within the full turnstile $\Delta; \Gamma \vdash JC$. The core of this system is the $\square$-Introduction rule, which allows to express constructive reasoning on linking existence. The idea is – ignoring contextual reasoning for simplicity – that linking a construction in $T$ with a justification of its corresponding type in $T'$ we obtain a proof of a constructive (or, admissible in $T$) validity. The rule in full (i.e. including contexts) corresponds to the construction of a link for a compound term based on existing link on its subterms. The full turnstile $\Gamma; \Delta \vdash$ is, hence, a modal logic that “zips” mutual reasoning between the two calculi. Within this framework we obtain a computational reading for justification logic restricted to $K$ modal reasoning. Before presenting this mutual reasoning at any arbitrary level of nesting (i.e. arbitrary modal types), we first introduce $JC\mathcal{C}_1$ which is a restriction of the type universe up to 1 level of $\square$-nesting.

We fix a countable universe of propositions ($P_i$) that corresponds to sentences of $T$. The elements of this universe can be inhabited either by constructions or justifications. We will need, accordingly, two kinds of inhabitation relations for each proposition. We will be writing $M : \phi$ for a construction $M$ of type $\phi$ in $T$. We will be writing $j : Just \phi$ to express the fact that $j$ is a justification (proof in $T'$) of the proposition $\phi$. When there is no confusion we will be abbreviating this by $j :: \phi$. A construction in $M : \phi$ in $T$ does not entail its necessity: to this aim, a corresponding justification $j : Just \phi$ from $T'$ has to be obtained. Vice versa, the justification $(j)$ of $\phi$ in $T'$ alone entails its validity but not its admissibility in $T$ (constructive necessity). This is expressed by the proposition – type $\square j \phi$. A construction of $\square j \phi$ can be obtained only when the (weaker) theory $T$ actually “responds” with a construction $M$ of the type $\phi$ to the valid fact $\phi$ known from $T'$ by deducing $j$. Hence, once (and only if) we have $j :: \phi$ then $\square j \phi$ can be regarded

---

7 One could alternatively use an additional constant symbol null and write null; $\Gamma \vdash_{IPC}$ to denote reasoning purely in $T$ and, thus, in absence of any metatheoretic environment.
as a well formed proposition. The stronger theory might be able to judge about \( \Box j \phi \) (given \( j :: \phi \)) and prove e.g., \( u :: \Box j \phi \). In that case \( T' \) “knows” that \( \phi \) is admissible in \( T \). In other words, when reasoning with justifications, the universe of types is contextual. To speak about an admissible (or, constructive) necessity of a proposition we require the existence of a corresponding proof object \( j \) in \( T' \) that establishes its validity.

3 Reasoning without foundational assumptions: \( \text{IPC} \)

Reasoning about the implicational fragment of the constructive theory \( (T) \), without formulating provability statements, is done within the implicational fragment of the simply typed lambda calculus. We start by giving the grammar for the metavariable \( \phi \) used in the rules.

\[
\phi ::= P_i | \phi \rightarrow \phi
\]

The calculus is presented by introducing: the universe of types \( \text{Prop}_0 \); rules for constructing well-formed contexts of simple propositional assumptions \( \Gamma_0 \); the rules governing \( \vdash_{\text{IPC}} \).

\[
\begin{align*}
&P_i \in \text{Prop}_0 \quad \text{ATOM}_0 \\
&\phi_1 \in \text{Prop}_0 \quad \phi_2 \in \text{Prop}_0 \quad \text{IMPL}_0 \\
&\text{nil} \vdash_{\text{IPC}} \text{wf} \quad \text{Nil}_0 \\
&\Gamma_0 \vdash_{\text{IPC}} \text{wf} \quad \phi \in \text{Prop}_0 \quad \Gamma_0 \vdash_{\text{IPC}} \phi \quad \text{\text{\Gamma}_0-EXP} \\
&\Gamma_0 \vdash_{\text{IPC}} \text{wf} \quad x : P_i \in \Gamma_0 \quad \Gamma_0 \vdash_{\text{IPC}} x : P_i \quad \text{\Gamma}_0\text{-REFL} \\
&\Gamma_0 \vdash_{\text{IPC}} \lambda x : \phi_1. M : \phi_2 \quad \rightarrow_1 \\
&\Gamma_0 \vdash_{\text{IPC}} M : \phi_1 \rightarrow \phi_2 \\
&\Gamma_0 \vdash_{\text{IPC}} M' : \phi_1 \quad \Gamma_0 \vdash_{\text{IPC}} (MM') : \phi_2 \quad \rightarrow_E
\end{align*}
\]

4 Reasoning in the Presence of Foundations: A calculus of Justifications \( J \)

Reasoning in the presence of minimal foundations corresponds to reasoning on the existence of proof objects in the foundational theory \( T' \). The minimal foundational assumptions from the logical point of view is that \( T' \) “knows” at least as much logic as \( T \) does. The more non-logical axioms in \( T \), the more the specifications \( T' \) should satisfy (one needs stronger foundations to justify stronger theories). Abstracting
from any particular \( T \) and \( T' \), and assuming only that \( T \) incorporates minimal logic, the specifications about existence of proofs in \( T' \) are:

- to have “enough” types to provide – at least – an intended interpretation of every type \( \phi \) of \( T \) to a unique type \( \text{Just} \ \phi \). In other words a subset of the types of \( T' \) should serve as interpretations of types in \( T \);
- to have – at least – proof objects for all the instances of the axiomatic characterization of the IPC fragment described above;\(^8\)
- to include some modus ponens rule which translates as: the existence of proof objects of types \( \text{Just} \ (\phi \rightarrow \psi) \) and of type \( \text{Just} \ \phi \) in \( T' \) should imply the existence of a proof object of the type \( \text{Just} \ \phi \).

### 4.1 Minimal Justification Logic J-Calc\(_1\)

Under these minimal requirements, we develop a minimal justification logic that is able to realize modal reasoning as reasoning on the existence of links between proofs of \( T \) and \( T' \). We first realize modal reasoning restricted to formulæ of degree (i.e. level of \( \square \)-nesting) 1. Such a calculus will be used as a base to build a full modal calculus with justifications for formulæ of arbitrary degree. Here is the grammar for the metavariables appearing below:

\[
\begin{align*}
\phi & := P_1 \mid \Box \phi \mid \phi_1 \rightarrow \phi_2 \\
j & := s_i \mid C \mid j_1 \ast j_2 \\
t & := x_i \mid \lambda x_i : \phi \cdot t \mid J s :: \phi \cdot t \\
C & := K_1[\phi_1, \phi_2] \mid S[\phi_1, \phi_2, \phi_3] \mid C_1 \ast C_2 \\
\pi & := \Pi s :: \phi_1, \phi_2 \mid \Pi \pi :: \phi_1 \cdot \pi \\
T & := \phi \mid \text{Just} \ \phi \mid \pi \\
s & := s_i \\
x & := x_i
\end{align*}
\]

### 4.1.1 Reasoning on minimal foundations J\(_0\)

Reasoning about such a minimal metatheory is axiomatized in its own turnstile (\( \vdash \) \( J_0 \)).\(^9\) Henceforth, judgments on the justificational type universe of \( J_0 \) (corresponding to formulæ in the (co-)theory \( T' \)) together with \( \text{wf} \) predicate for \( \Delta_0 \) contexts go as follows:

---

\(^8\) If we extend our fragment we should extend our specifications accordingly but this can be easily done directly as in full justification logic. We choose to remain within this fragment for economy of presentation.

\(^9\) This is the part of the calculus that corresponds directly to the algebra of justifications restricted to the applicative fragment.
We add logical constants to satisfy the requirement that $J_0$ includes an axiomatic characterization of – at least – a fragment of IPC. Following justification logic, we define a signature of polymorphic constructors including $K$, $S$ from combinatory logic. The values of those constructors are axiomatic constants that witness existence of proofs in $T'$ of all instances of the corresponding logical validities. This axiomatic characterization of intuitionistic logic in $J_0$ together with rule scheme Times (applicativity of justifications) satisfy the minimal requirement for $T'$ to reason logically.

\[
\begin{align*}
\frac{\Delta_0 \vdash J_0 \text{ wf} \quad \Delta_0 \vdash J_0 \phi \in \text{Prop}_0}{\Delta_0 \vdash J_0 \text{ Just } \phi \in \text{jtype}_0} & \quad \text{SIMPLE} \\
\frac{\Delta_0 \vdash J_0 \text{ Just } \phi \in \text{jtype}_0 \quad s \notin \Delta_0}{\Delta_0, s :: \phi \vdash J_0 \text{ wf}} & \quad \text{D0-App} \\
\frac{\Delta_0 \vdash J_0 \text{ wf} \quad s :: \phi \in \Delta}{\Delta_0 \vdash J_0 s :: \phi} & \quad \text{D0-Refl}
\end{align*}
\]

4.1.2 Zipping: $J$-Calc$_1 = \text{IPC} + J_0 + \Box -$Intro

In this section we introduce $J$-Calc$_1$ for reasoning on the existence of links i.e. constructions that witness the existence of proofs both in IPC ($T$) and $J_0$ ($T'$). By constructing a link we have a proof of a constructive necessity of a formula, showing that it is true and valid. Links have types of the form $\Box \downarrow j \phi$ where $j$ is a justification of the appropriate type. $J$-Calc$_1$ realizes modal logic theoremhood in $K$ up to degree 1 (i.e. formulae where its subformula includes up to 1 level of $\Box$).

We start by importing well-formedness judgments for contexts and justificational types ($\Delta_0 \text{Wf}$, $\text{JustWf}$ respectively), and for the Prop$_1$ universe and its contexts:
From justifications of formulas in Prop₀, we can reason about their admissibility in T. Hence, Γ₁ might include assumptions from the sorts Prop₀ and Prop₁. For the inhabitation of Prop₀, Prop₁, we first accumulate intuitionistic reasoning extended to the new type universe (Prop₁), adapting the rules from Section 3:

For relating the two calculi, a lifting rule is formulated for turning strictly Prop₀ judgments to judgments on proof links (Prop₁). In the rule, the ⊤-operator ensures that context list ⊤ Γ includes assumptions strictly in Prop₀. The operator ⊤ can be viewed as the opposite of lift operation applied on context lists erasing one level of boxed assumptions at the top level as described below.

A corresponding iterative let-binding construct (let*) is introduced simultaneously with the context lifting. The purpose of the iterative let binding is to extract the target(s) (T’ terms) of existing links on subterms (x₁...xₙ) of some composite term M in T and compose them to the target of the whole term M creating its residual. We show the operation of this construct in the example from section 5.
\[
\begin{align*}
\text{let}^* \Gamma := \\
\text{match } \Gamma \text{ with} \\
\top & \Rightarrow \text{let } () = () \\
\Gamma', x_i : \Box \phi_i & \Rightarrow \text{(let}^* \Gamma') \text{ in let link}(x_i, j_i) = x_i' \\
\Gamma', \_ & \Rightarrow \text{let}^* \Gamma'
\end{align*}
\]

The $\Box$-Introduction rule goes as follows:

\[
\frac{\vdash \Gamma_1 \vdash M : \phi \quad \Delta_0 ; \Gamma_1 \vdash j :: \phi}{\Delta_0 ; \Gamma_1 \vdash (\text{let}^* \Gamma) \text{ in link} (M, j) : \Box j \phi} \quad \text{Box-Intro}
\]

Finally, under empty $\Gamma_1$, we are permitting abstraction from a non-empty $\Delta_0$. The resulting abstractions ($\text{J-terms}$), as we will see, are the inhabitants of modal types and correspond to linking processes. Their typing is, naturally, of $\Pi$-kind since the typing of a link is sensitive to its target code. We introduce $\Pi$-formation and inhabitation rules:

\[
\frac{\Delta_0, s :: \phi_1; \vdash \text{JC}_1 \phi_2 \in \{\text{Prop}_0, \text{Prop}_1\}}{\Delta_0 ; \vdash \text{JC}_1 \Pi s :: \phi_1. \phi_2 \in \Pi} \quad \text{\Pi-Type}_0
\]

\[
\frac{\Delta_0, s :: \phi_1; \vdash \text{JC}_1 \pi \in \Pi}{\Delta_0 ; \vdash \text{JC}_1 \Pi s :: \phi_1. \pi \in \Pi} \quad \text{\Pi-Type}_1
\]

\[
\frac{\Delta_0, s :: \phi_1; \vdash \text{JC}_1 t : T}{\Delta_0 ; \vdash \text{JC}_1 \Pi s :: \phi. t : \Pi s :: \phi. T} \quad \text{\Pi-Intro}
\]

\[
\frac{\Delta_0 ; \vdash \text{JC}_1 t : \Pi s :: \phi, T \quad \Delta_0 ; \vdash \text{JC}_1 j :: \phi}{\Delta_0 ; \vdash \text{JC}_1 (t, j) : T[s := j]} \quad \text{\Pi-Elim}
\]

5 Computational Motivation: A type system for separate compilation

In this section, we show how J-Calc can be viewed as a type system for program generation in typed languages that support separate compilation (modular programming or external function calls). These languages follow the client/server approach to programming: client code, can refer to code definitions implemented by the server elsewhere; the server can be some module or even another language providing the required function calls, but it needs not know the details of the implementation (encapsulation). A challenge in such a system is to provide a mechanism of separate compilation such that the client (or, source) code is compiled independently of changes in the implementation of the server. In what follows we present J-Calc as
a type system for linking processes in such a setting. Following our language: the 
constructs of \( T \) represent here client (or source) expressions and constructs of \( T' \)
represent target (or server) code expressions. Our linking by way of the \( \square \)-Intro rule 
linking processes generators that consume different implementations from the server 
and link them with constructs of the source. We show, following a textbook exam-
ple for modules, that our type system provides the abstraction required for such a 
language so that client code needs to be compiled once and only, independently of 
the different implementations that the server module might provide.

5.1 Producing generic code

As an example, we will use ML-like module definitions. We start with a definition 
of a module’s public signature (i.e. the operations provided by the server to the 
client). Here we provide the signature for a stack of integers.

```plaintext
module type INTSTACK =
 sig
 type intstack
 val Empty: intstack
 val push : int->intstack->intstack
 val pop: int->intstack->intstack
end;;
```

This signature can be implemented in various ways but our goal is to produce 
generic code from compiling source code only once. We take for example the source 
code expression \( \vdash (\text{push } 2 \text{ Empty}) : \text{intstack} \) and show step-by-step the construc-
tion of generic code following our calculus. First we factorize the usage of the 
signature by rewriting the term:

\[ \vdash \Gamma = x_1 : \text{int} \to \text{intstack} \to \text{intstack}, x_2 : \text{intstack} \vdash (x_1 \ 2 \ x_2) : \text{intstack} \]

Secondly, we assume implementations of “missing” code in the validity context, 
i.e.

\[ \Delta = s_1 :: \text{int} \to \text{intstack} \to \text{intstack}, s_2 :: \text{intstack} \vdash s_1 \times 2 \times s_2 :: \text{intstack} \]

Using the \( \square \)-Intro rule we obtain:

\[ \Delta; \Gamma = x'_1 : \square^{s_1}(\text{int} \to \text{intstack} \to \text{intstack}), x'_2 : \square^{s_2}\text{intstack} \vdash \]

let link\((x_1, s_1) = x'_1 \) in

let link\((x_2, s_2) = x'_2 \) in

link\((x_1 \ 2 \ x_2, s_1 \times 2 \times s_2) : \square^{s_1\times 2\times s_2}\text{intstack} \]
Finally, abstracting we get a linking process generator of typing that is sensitive to the different implementations provided by the server:

\[ \Gamma \vdash J_1.J_2. \lambda x_1'. \lambda x_2'. \text{let }^* \Gamma \text{ in link}(x_1, x_2, s_1 * 2 * s_2) \]

of type:

\[ \Pi s_1. \Pi s_2. \Box^{s_1}(\text{int } \rightarrow \text{intstack } \rightarrow \text{intstack}) \rightarrow \Box^{s_2}\text{intstack } \rightarrow \Box^{s_1*2*s_2}\text{intstack} \]

where

\[ \text{let }^* \Gamma = \text{def let } \text{link}(x_1, s_1) = x_1' \text{ in let } \text{link}(x_2, s_2) = x_2' \]

5.2 Providing implementations

The server might provide different implementations of the \textit{instack} module signature. The two textbook approaches use lists or arrays of integers. Given different implementations, the initial source code has different computational value since the links that it induces change. Schematically:

- \text{push} \xrightarrow{\text{link}} \text{Cons}: \Box^{\text{Cons}}(\text{int } \rightarrow \text{intstack } \rightarrow \text{intstack})
- \text{Empty} \xrightarrow{\text{link}} [\text{\textbar}]: \Box^{[\text{\textbar}]}\text{intstack}
- \text{push 2 Empty} \xrightarrow{\text{link}} \text{Cons 2 [\text{\textbar}]:} \Box^{\text{Cons}*2*[\text{\textbar}]}\text{intstack}

- \text{push} \xrightarrow{\text{link}} \text{Addarr}: \Box^{\text{Addarr}}(\text{int } \rightarrow \text{intstack } \rightarrow \text{intstack})
- \text{Empty} \xrightarrow{\text{link}} \text{Void}: \Box^{\text{Void}}\text{intstack}
- \text{push 2 Empty} \xrightarrow{\text{link}} \text{Addarray 2 Void:} \Box^{\text{Addarr}*2*\text{Void}}\text{intstack}

Both cases are captured by the generic code we produced giving us the ability of \	extit{separate compilation} of source and implementation. In the first case we have:

- \text{Just[\text{intstack}]}=\text{List},
- \text{Just[\text{push}]}= \text{Cons},
- \text{Just[\text{Empty}]}= [\text{\textbar}]

From which we obtain using \Box^{\text{Intro}}:
⊢ link(Empty, []) : □ [] intstack

and

⊢ link(push, Cons) : □ Cons(int → intstack → intstack)

Finally, using linking process generator obtained in the previous section and under standard operational semantics for application (β-reduction) and let-binding evaluation we link the source code to its residual program using the list implementation:

⊢ link(push 2 Empty, Cons*2*[]) : □ Cons*2*[](int → intstack → intstack)

Analogously, using the exact same code generator, closing ∆ with implementations

Just[intstack] = Array
Just[push] = addarr
Just[Empty] = create()

We obtain the links:

link(push, addarr) : □ addarr(int → intstack → intstack)
link(Empty, create()) : □ create() intstack

And from the previous generic judgment under standard operational semantics for application (β-reduction) and let-binding evaluation we link the source code to its residual program using the Array implementation:

link(push 2 Empty, addarr * 2 * create()) ⊢ □ addarr*2*create() intstack

Note that the client code does not need to recompile. Our generic code construction provides the expressive means to evaluate source contextually given different implementations of the module signature.

6 The Full Calculus: J-Calc

J-Calc motivates the generalization to modal reasoning of arbitrary nesting: J-Calc. To allow such generalization, we need justifications of types of the form Just □ J φ.
Let us revise: If $\phi$ is a proposition (or, a sentence in the language of $T$), then $\text{Just } \phi$ corresponds to the intended interpretation of $\phi$ in some (co-)theory $T'$. In $\text{J-Calc}_1$ we could reason logically about the constructive admissibility of (valid according to $T'$) facts of $T$. The existence of a link of a proof in $T$ with an existing proof of the same type in $T'$ would lead to constructions of a type of the form $\Box^i \phi$ with $\phi$ a simple type. To get modal theoremhood of degree 2 or more we have to assume that $T'$ can express the existence of such links in itself. That is to say that $T'$ can express the provability predicates both of $T$ and of itself. Hence, supposing that $j :: \phi$, we can read a justification term of type $\text{Just } \Box^j \phi$ as a witness of a proof in $T'$ of the fact $\exists x. \text{Proof}_{T'}(x, \phi) \land \exists x. \text{Proof}_{T'}(x, \text{Just } \phi)$ expressed in $T'$. We will specify which of those types $T'$ is expected to capture by introducing additional appropriate constants. Having this kind of justifications we can obtain $\text{Prop}_i$ for any finite $i$ as slices of a type universe in a mutual inductive construction. Schematically: $\text{Prop}_0 \Rightarrow \text{Just } \text{Prop}_0 \Rightarrow \text{Prop}_1 \Rightarrow \text{Just } \text{Prop}_1$ and so on. This way we obtain full minimal justification logic. As different kinds of judgments are kept separated by the different typing relations, we do not need to provide distinct calculi as we did for $\text{J-Calc}_1$ but we provide one “zipped” calculus directly.  

6.1 Justificational (Validity) Judgments

The justificational type system has to include: judgments on the wellformedness of contexts ($\text{wf}$); judgments on what $T'$ can reason about ($\text{jtype}$) under the requirement that it is a metatheory of $T$; judgments on the construction of the justificational type universe ($\text{jtype}$) and minimal requirements about its inhabitation (i.e, a minimal signature of logical constants). The grammar of terms is the same as in section 4.1, the difference now is that the restrictions on the $\text{Prop}$ universe are dropped.

We introduce progressively: formation rules for $\text{Prop}$; the formation rule for $\text{jtype}$; rules to build well-formed contexts of propositions and justifications (where we will be abbreviating using the following equational rule: $\text{nil}, s_1 :: \phi_1, s_2 :: \phi_2, \ldots \overset{\text{def}}{=} s_1 :: \phi_1, s_2 :: \phi_2, \ldots$).

---

10 In fact, adjoining $\Gamma$ contexts when reasoning within justifications is pure weakening so we could have kept those judgments separated in a single–context $\vdash$ relation. We gain something though: we can squeeze two premises ($\Delta \vdash j :: \phi, \Delta; \Gamma \vdash \text{wf}$) to a single one ($\Delta; \Gamma \vdash j :: \phi$).

11 Analogous treatments of judgments on the validity of contexts can be found e.g. in [26].
6.1.1 Prop Inhabitation

Here is the first part of logical propositional reasoning of the system.

\[
\frac{\Delta; \Gamma \vdash \text{wf} \quad x : \phi \in \Gamma}{\Delta; \Gamma \vdash x : \phi} \quad \text{Γ-REFL}
\]

\[
\frac{\Delta, \Gamma, x : \phi \vdash M : \phi_2}{\Delta, \Gamma \vdash \lambda x : \phi_1. M : \phi_1 \to \phi_2} \quad \to^I
\]

\[
\frac{\Delta; \Gamma \vdash M : \phi_1 \to \phi_2 \quad \Delta; \Gamma \vdash M' : \phi_1}{\Delta; \Gamma \vdash (MM') : \phi_2} \quad \to^E
\]

6.1.2 jtype Inhabitation

Now we move to the core of the system. In the judgments below we provide the constructions of canonical elements of justificational types (jtype). The judgments reflect the minimal requirements for \( T' \) to be a metatheory of some \( T \) as presented in Section 4.1.1 together with specifications on internalizing proof links reasoning in itself. More specifically, we demand that \( T' \) can capture reasoning on links (between proof objects of \( T \) and itself) within itself and also, internalize modus ponens of \( T \).

To capture these provability conditions we add the constant constructors ! (bang) and Kappa. Although introduction of links is axiomatized in the next section, the judgments concerning the ! and Kappa constructors should be viewed in conjunction with \( \Box - Intro \). They witness the fact that \( T' \) internalizes modus ponens (of \( T \)) and linking existence (again of \( T \)).
\[
\Delta; \Gamma \vdash_{JC} \text{Just} \phi_1 \rightarrow \phi_2 \rightarrow \phi_1 \in \text{jtype}
\]
\[
\Delta; \Gamma \vdash_{JC} K[\phi_1, \phi_2] :: \phi_1 \rightarrow \phi_2 \rightarrow \phi_1^K
\]
\[
\Delta; \Gamma \vdash_{JC} (\phi_1 \rightarrow \phi_2 \rightarrow \phi_3) \rightarrow (\phi_1 \rightarrow \phi_2) \rightarrow (\phi_1 \rightarrow \phi_3) \in \text{jtype}
\]
\[
\Delta; \Gamma \vdash_{JC} S[\phi_1, \phi_2, \phi_3] :: (\phi_1 \rightarrow \phi_2 \rightarrow \phi_3) \rightarrow (\phi_1 \rightarrow \phi_2) \rightarrow (\phi_1 \rightarrow \phi_3)
\]
\[
\Delta; \Gamma \vdash_{JC} \text{Just} (\phi_1 \rightarrow \phi_2 \rightarrow \phi_3) \rightarrow (\phi_1 \rightarrow \phi_2) \rightarrow (\phi_1 \rightarrow \phi_3) \in \text{jtype}
\]
\[
\Delta; \Gamma \vdash_{JC} \text{Kappa}[j, j', \phi_1, \phi_2] :: \Box^j (\phi_1 \rightarrow \phi_2) \rightarrow \Box^j \phi_1 \rightarrow \Box^{j'} \phi_2
\]

6.2 Proof Links

Our next task is to formulate the main rule for the \(K\) modality as a lifting rule for going from reasoning about constructions to reasoning about admissibility of validities via proof linking. To reflect the modal axiom \(K\) in Natural Deduction we have to obtain a rule that reflects the following provability principle:

\[
\phi_1 \text{ true}, \ldots, \phi_n \text{ true} \vdash \phi \text{ true} \quad \phi_1 \text{ valid}, \ldots, \phi_n \text{ valid} \vdash \phi \text{ valid}
\]

\[
\Box \phi_1 \text{ true}, \ldots, \Box \phi_n \text{ true}, \ldots \vdash \Box \phi \text{ true}
\]

\[
\Box \text{-Intro}
\]

We proceed with giving inhabitants analogously to what was explained in Section 4.1.2:\footnote{We prefer this to the mouthful but equivalent:}

\[
\Delta; \Gamma \vdash_{JC} M : \phi \quad \Delta; \Gamma \vdash_{JC} j :: \phi \quad \Box \text{-Intro}
\]

\[
\Delta; \Gamma \vdash_{JC} (\text{let}^* \Gamma) \text{ in link } (M, j) : \Box \phi
\]

\[
\Delta; \Gamma \vdash_{JC} t : \Pi s :: \phi. T \quad \Delta; \Gamma \vdash_{JC} t : \Pi s :: \phi. T \quad \Delta; \Gamma \vdash_{JC} t : \Pi s :: \phi. T \quad \Pi \text{-Intro}
\]

\[
\Delta; \Gamma \vdash_{JC} t[s := j] : \Pi \text{-Elim}
\]

Finally, abstraction from \(\Delta\) contexts over empty \(\Gamma\) contexts applies in the extended type universe:

\[
\Delta, s :: \phi; \Gamma \vdash_{JC} t : T \quad \Pi \text{-Intro}
\]

\[
\Delta; \Gamma \vdash_{JC} t : \Pi s :: \phi. T \quad \Delta; \Gamma \vdash_{JC} t : \Pi s :: \phi. T \quad \Delta; \Gamma \vdash_{JC} t : \Pi s :: \phi. T \quad \Pi \text{-Elim}
\]

\[
\Delta; \Gamma \vdash_{JC} JBox j : \Box \phi
\]

\[
\Delta; \Gamma \vdash_{JC} JBox j : \Box \phi
\]

\[
\Box \text{-Intro}
\]

\[
\forall \phi_i \in \Gamma. \Delta' \vdash_{JC} \Box^j \text{phi}_i \quad \Delta' \vdash_{JC} \Box^j \text{phi}_i \quad \Box^j \phi \vdash_{JC} \Box^j \phi \quad \Box^j \phi \vdash_{JC} \Box^j \phi
\]

\[
\Delta' \vdash_{JC} JBox j : \Box \phi
\]
7 Further Results and Conclusions

Standard meta-theoretical results can be proven for J-Calc. We just mention here that the iterative let operator satisfies standard commutativity with the substitution rule for justifications and that structural rules can be proven. We will be skipping the index in $\vdash_{\text{JC}}$.

**Theorem 1 (Weakening).** J-Calc satisfies Weakening in both modes of reasoning:

(i) If $\Delta; \text{nil} \vdash j :: \phi$, and $\Delta; \Gamma \vdash \text{wf}$ then, $\Delta; \Gamma \vdash j :: \phi$.

(ii) If $\Delta; \Gamma \vdash j :: \phi$, then $\Delta, s :: \phi'; \Gamma \vdash j :: \phi$, with $s$ fresh.

(iii) If $\Delta; \Gamma \vdash M : \phi$, then $\Delta; \Gamma, x : \phi' \vdash M : \phi$, with $x$ fresh.

**Proof.** For all items by structural induction on the derivation trees of the two kinds of constructions. The proof of the first is vacuous since $\Gamma$ contexts are irrelevant in justification formation. As a result, its inverse can also be shown. □

**Theorem 2 (Contraction).** J-Calc satisfies Contraction:

(i) If $\Delta, s :: \phi, t :: \phi; \text{nil} \vdash j :: \phi'$, then $\Delta, u :: \phi; \text{nil} \vdash j[\text{t/u}] :: \phi'$.

(ii) If $\Delta, s :: \phi, t :: \phi; \Gamma \vdash \text{wf}$, then, $\Delta, u :: \phi; \Gamma[\text{t/u}] \vdash \text{wf}$.

(iii) If $\Delta, s :: \phi, t :: \phi; \Gamma \vdash M : \phi'$, then, $\Delta, u :: \phi; \Gamma[\text{t/u}] \vdash M[\text{t/u}] : \phi'[\text{t/u}]$.

(iv) If $\Delta; \Gamma, x : \phi, y : \phi \vdash M : \phi'$, then $\Delta; \Gamma, z : \phi \vdash M[\text{x/y}] : \phi'$.

**Proof.** First item by structural induction on the derivation trees of justifications (validity judgments). Note, as mentioned in the previous theorem, that it can be shown for arbitrary $\Gamma$. For the second, nested induction on the structure of context $\Gamma$ (treated as list) and the complexity of formulas. Vacuously in the nil case. For the non-empty case: case analysis on the complexity of the head formula using the inductive hypothesis on the tail. Cases of interest are with $\Box \phi$ or $\forall \phi$ as subformulae. Use the previous item and judgments for $\text{wf}$ contexts. For the third and the fourth, again by structural induction on the derivation. □

In a similar fashion we can show the more general:

**Theorem 3 (Preservations of Types under Substitution).** J-Calc preserves types under substitution and simultaneous substitution:

(i) If $\Delta; \Gamma, x : \phi \vdash t : T$, and $\Delta; \Gamma \vdash M : \phi$ then $\Delta; \Gamma \vdash t[x/M] : T$

(ii) If $\Delta, s :: \phi, \Delta' ; \Gamma \vdash t : T$, and $\Delta; \Gamma \vdash j :: \phi$ then $\Delta, \Delta'[s/j]; \Gamma[s/j] \vdash t[s/j] : T[s/j]$

We additionally mention that the calculus satisfies permutation for both contexts $\Delta$ and $\Gamma$ with the restriction that the permutations in $\Delta$ should not break the chain of dependencies. Lastly, we mention here that under standard let-binding evaluation and application as $\beta$-reduction within a dependently typed framework, a small step operational semantics has been developed and progress and preservation can be shown.
For future work, we plan to extend the computational relevance of the full calculus (JCalc) by establishing its connection with higher-order module systems (e.g. where module signatures can refer to other module signatures which, in turn, are implemented by a third module). Linking processes in such systems would utilize our type system in full. Cut-elimination results are currently under development.

References


