Admissible Tools in the Kitchen of Intuitionistic Logic

Andrea Condoluci
Department of Computer Science and Engineering
Università di Bologna
Bologna, Italy
andrea.condoluci@unibo.it

Matteo Manighetti
INRIA Saclay & LIX, École Polytechnique
Palaiseau, France
mmanighe@lix.polytechnique.fr

The usual reading of logical implication $A \to B$ as " *if A then B* " fails in intuitionistic logic: there are formulas A and B such that $A \to B$ is not provable, even though B is provable whenever A is provable. Intuitionistic rules apparently don't capture interesting meta-properties of the logic and, from a computational perspective, the programs corresponding to intuitionistic proofs are not powerful enough. Such non-provable implications are nevertheless *admissible*, and we study their behaviour by means of a proof term assignment and related rules of reduction. We introduce **V**, a calculus that is able to represent admissible inferences, while remaining in the intuitionistic world by having normal forms that are just intuitionistic terms. We then extend intuitionistic logic with principles corresponding to admissible rules. As an example, we consider the Kreisel-Putnam logic **KP**, for which we prove the strong normalization and the disjunction property through our term assignment. This is our first step in understanding the essence of admissible rules for intuitionistic logic.

1 Introduction

Proof systems are usually presented inductively by giving axioms and rules of inference, which are respectively the ingredients and the tools for cooking new proofs. For example, when presenting *classical propositional logic* (**CPC**) in *natural deduction*, for each of the usual connectives $\wedge, \vee, \neg, \to, \bot$ one gives a set of standard tools to introduce or remove a connective from a formula in order to obtain a proof.

In their most essential form, we can represent rules as an inference $A_1, ..., A_n \,/\, B$ (read "from $A_1, ..., A_n$ infer B") where $A_1, \ldots, A_n, B$ are schemata of logic formulas. A rule $A_1, \ldots, A_n \,/\, B$ is said to be *admissible* in a proof system if it is in a way redundant, *i.e.* whenever $A_1 \ldots A_n$ are provable, then B is already provable without using that rule. Adding or dropping rules may increase or decrease the amount of proofs we can cook in a proof system. The effect can be dramatic: for example, *classical propositional logic* **CPC** can be obtained by simply adding the rule of *double negation elimination* ($\neg\neg A \,/\, A$) to *intuitionistic propositional logic* **IPC**. Admissible rules are all the opposite: if we decide to utilize one in order to cook something, then we could have just used our ingredients in a different way to reach the same result.

One appealing feature of **CPC** is the fact that it is *structurally complete*: all its admissible rules are *derivable*, in the sense that whenever $A_1, \ldots, A_n \,/\, B$ is an admissible rule, then also the corresponding principle $A_1 \wedge \cdots \wedge A_n \to B$ is provable [4] – *i.e.* the system acknowledges that there's no need for that additional tool, so we can internalize it and use the old tools to complete our reasoning. This is not the case in intuitionistic logic: the mere fact that we *know* that the tool was not needed, doesn't give us any way to show inside the system *why* is that. On the other hand, **IPC** has other wonderful features. Relevant here is the *disjunction property*, fundamental for a constructive system: when a disjunction $A \vee B$ is provable, then one of the disjuncts A or B is provable as well. Our interest is in these intuitionistic admissible rules that are not derivable, in the computational principles they describe, and in the logic systems obtained by explicitly adding such rules to **IPC**.

Berardi, Miquel (Eds.): CL&C 2018
EPTCS 281, 2018, pp. 10–23, doi:10.4204/EPTCS.281.2

Can one effectively identify all intuitionistic admissible rules? The question of whether that set of rules is recursively enumerable was posed by Friedman in 1975, and answered positively by Rybakov in 1984. It was then de Jongh and Visser who exhibited a numerable set of rules (now known as *Visser's rules*) and conjectured that it formed a basis for all the admissible rules of **IPC**. This conjecture was later proved by Iemhoff in the fundamental [6]. Rozière in his Ph.D. thesis [9] reached the same conclusion with a substantially different technique, independently of Visser and Iemhoff. These works elegantly settled the problem of identifying and building admissible rules. However our question is different: *why* are these rules superfluous, and what reduction steps can eliminate them from proofs?

Rozière first posed the question of finding a computational correspondence for his basis of the admissible rules in the conclusion of his thesis, but no work has been done on this ever since. Natural deduction provides a powerful tool to analyse the computational behaviour of logical axioms, thanks to the fact that it gives a simple way to translate axioms into rules and to develop correspondences with λ-calculi. Our plan is therefore to understand the phenomenon of admissibility by equipping proofs with λ-terms and associated reductions in the spirit of the Curry-Howard correspondence. Normalization will show explicitly what role admissible rules play in a proof.

1.1 Visser's Basis

The central role in the developement of the paper is played by Visser's basis of rules. The term *basis* means that any rule that is admissible for **IPC** is obtainable by combining some of the rules of the family with other intuitionistic reasoning. It consists of the following sequence of rules:

$$\text{Visser}_n: \quad (B_i \to C_i)_{i=1\ldots n} \to A_1 \vee A_2 \;/\; \begin{cases} \bigvee_{j=1}^{n} ((B_i \to C_i)_{i=1\ldots n} \to B_j) \\ \vee \\ ((B_i \to C_i)_{i=1\ldots n} \to A_1) \\ \vee \\ ((B_i \to C_i)_{i=1\ldots n} \to A_2) \end{cases}$$

This is read as: for every natural number n, whenever the left part of the rule (a n-ary implication) is provable, then the right part (an $n+2$-ary disjunction) is provable. It forms a basis in the sense that all other admissible rules of **IPC** can be obtained from the combination of rules from this family with the usual rules of intuitionistic logic. It is an infinite family, since Visser_{n+1} cannot be derived from $\text{Visser}_1,\ldots,\text{Visser}_n$ [9].

The importance of Visser's basis is not limited to intuitionistic logic but also applies more generally to intermediate logics, as witnessed by the following:

Theorem 1.1 (Iemhoff [7])**.** If the rules of Visser's basis are admissible in a logic, then they form a basis for the admissible rules of that logic

This theorem also gives us a simple argument to prove the structural completeness of **CPC**: since all the Visser_n rules are provable in **CPC**, they are admissible and therefore they constitute a basis for *all* the admissible rules of **CPC**; but since the Visser_n are derivable, all admissible rules are derivable.

1.2 Contributions and Structure of the Paper

In Section 2 we introduce the natural deduction rules corresponding to Visser's rules, and present the associated λ-calculus **V**: we show that proofs in the new calculus normalize to ordinary intuitionistic

proofs. In the remaining part of the paper, we push further our idea and start adapting our calculus to intermediate logics characterized by axioms derived from admissible rules. In Section 3 we study the well-known *Harrop's rule*, and more precisely the logic **KP** obtained by adding Harrop's principle to **IPC**: we prove good properties like subject reduction, the disjunction property, and strong normalization. In Section 4 we quickly introduce the logic **AD** (obtained by adding the axiom V_1 to **IPC**) as a candidate for future study, and possible extensions to arithmetic. Proofs can be found in the appendices at the end of the paper.

2 Proof Terms for the Admissible Rules: V

In this section, we are going to assign proof terms to all the inferences of Visser's basis in a uniform way. First, we give a natural deduction flavor to the Visser rules. Since the conclusion of the left-hand side of the rules is a disjunction, we model the rules as generalized disjunction eliminations $\vee_E$; "generalized" because the main premise will be the disjunction in the antecedent of the Visser$_n$, but under *n implicative* assumptions. Therefore the rules of inference Visser$_n$ have the form:

$$\dfrac{\begin{array}{cccc}[B_i \to C_i]_{i=1\ldots n} & [(B_i \to C_i)_{i=1\ldots n} \to A_1] & [(B_i \to C_i)_{i=1\ldots n} \to A_2] & [(B_i \to C_i)_{i=1\ldots n} \to B_j]_{j=1\ldots n} \\ \vdots & \vdots & \vdots & \vdots \quad \vdots \\ A_1 \vee A_2 & D & D & D \quad \cdots \quad D\end{array}}{D}$$

In order to keep the rules admissible, we need to restrict the usage of the inference: the additional requirement is that the proofs of the *main* premise (the one on the left with end-formula $A_1 \vee A_2$) must be *closed* proofs, *i.e.* cannot have open assumptions others than the ones discharged by that Visser inference. Otherwise we would be able to go beyond **IPC**, since for example we would prove all the principles corresponding to the admissible rules (as in system **AD**, see Section 4). On the other side, it is straightforward to see that our rules directly correspond to rules of Visser's basis, and that they adequately represent admissibility. We now turn to proof terms:

t,s,u	$::=$	$x,y,z,\ldots \in \mathscr{V} \mid t\,s \mid \lambda x.t$	
	$\mid$	$\mathtt{efq}\,t$	(exfalso)
	$\mid$	$\mathtt{<}t\mathtt{,}s\mathtt{>}$	(pair)
	$\mid$	$\mathtt{proj}_i\,t$	(projection)
	$\mid$	$\mathtt{inj}_i\,t$	(injection)
	$\mid$	$\mathtt{case}[t \parallel y.s_1 \mid y.s_2]$	(case)
	$\mid$	$\mathtt{V}_n[\vec{x}.t \parallel y.s_1 \mid y.s_2 \parallel z.\vec{u}]$	(Visser — in **V** and **AD**)
	$\mid$	$\mathtt{hop}[\vec{x}.t \parallel y.s_1 \mid y.s_2]$	(Harrop — in **KP**)

Figure 1: Proof terms

Since the shape of the rules is the elimination of a disjunction, the proof term associated with this inference will be modeled on the *case analysis* $\mathtt{case}[- \parallel - \mid -]$. The difference will be in the number of assumptions that are bound, and in the number of possible cases. We use the vector notation $\vec{x}.t$ on variables to indicate that a sequence of (indexed) variables $x_1,\ldots,x_n$ is bound, and on terms like $z.\vec{u}$ to indicate a sequence of (indexed) terms $u_1,\ldots,u_n$ on each of which we are binding the variable z. The resulting annotation for a Visser inference is then:

$$\text{Visser}_n\ \frac{\begin{array}{c}\Gamma, y\colon (B_i \to C_i)_{i=1\ldots n} \to A_1 \vdash s_1 : D \\ \Gamma, y\colon (B_i \to C_i)_{i=1\ldots n} \to A_2 \vdash s_2 : D \\ \vec{x}\colon (B_i \to C_i)_{i=1\ldots n} \vdash t\colon A_1 \vee A_2 \qquad \{\Gamma, z\colon (B_i \to C_i)_{i=1\ldots n} \to B_j \vdash u_j : D\}_{j=1\ldots n}\end{array}}{\Gamma \vdash \mathtt{V}_n[\vec{x}.t \parallel y.s_1 \mid y.s_2 \parallel z.\vec{u}] : D}$$

We call **V** the calculus obtained by adding this family of rules of inference to **IPC**. The syntax of **V** can be found in Figure 1, and it includes the usual proof terms for intuitionistic logic [10], plus the proof terms $\mathtt{V}_{-}[- \parallel - \mid - \parallel -]$ for the Visser family.

We now turn to the reduction rules. First of all, we need to define W contexts: intuitively, *contexts* are proof terms with a *hole*, where the hole is denoted by $\Box$, and $E\langle t\rangle$ means replacing the unique hole in the context E with the term t.

Definition 2.1 (Weak head **IPC** contexts)**.** W contexts are defined by the following grammar:

$$W ::= \Box \mid W\,t \mid \mathtt{proj}_i W \mid \mathtt{case}[W \parallel - \mid -].$$

Reduction rules for IPC

–	Beta	$(\lambda x.t)\,s$	$\mapsto$	$t\{s/x\}$	
–	Projection	$\mathtt{proj}_i\langle t_1, t_2\rangle$	$\mapsto$	t_i	
–	Case	$\mathtt{case}[\mathtt{inj}_i t \parallel y.s_1 \mid y.s_2]$	$\mapsto$	$s_i\{t/y\}$	

Additional rules for V

–	Visser-inj	$\mathtt{V}_n[\vec{x}.\mathtt{inj}_i t \parallel y.s_1 \mid y.s_2 \parallel z.\vec{u}]$	$\mapsto$	$s_i\{\lambda\vec{x}.t/y\}$	$(i = 1,2)$
–	Visser-efq	$\mathtt{V}_n[\vec{x}.W\langle \mathtt{efq}\,t\rangle \parallel y.s_1 \mid y.s_2 \parallel z.\vec{u}]$	$\mapsto$	$s_1\{(\lambda\vec{x}.\mathtt{efq}\,t)/y\}$	
–	Visser-app	$\mathtt{V}_n[\vec{x}.W\langle x_j t\rangle \parallel y.s_1 \mid y.s_2 \parallel z.\vec{u}]$	$\mapsto$	$u_j\{\lambda\vec{x}.t/z\}$	$(j = 1\ldots n)$

Figure 2: Reduction rules (**V**)

The reduction rules for the proof terms are given in Figure 2: the first block defines $\mapsto_{\mathbf{IPC}}$ by means of the usual rules for **IPC**, and the second block defines $\mapsto_{\mathbf{V}}$ as $\mapsto_{\mathbf{IPC}}$ plus additional reduction rules for the new construct $\mathtt{V}_n[\vec{x}.t' \parallel \vec{y}.s_1 \mid y.s_2 \parallel z.\vec{u}]$, depending on different shapes that t' might have. Let us explain the intuition. In the first case (*Visser-inj*), the term is the injection $\mathtt{inj}_i t$ with possibly free variables x_i of type $B_i \to C_i$ for $i = 1\ldots n$; in that branch one has chosen to prove one of the two disjuncts A_1 or A_2, and we may just reduce to the corresponding proof s_i, in which we plug the proof t but after binding the free variables $\vec{x}$. In the second case (*Visser-efq*), the disjunction is proved by means of a contradiction, and that contradiction may be used to prove any of the cases $s_1, s_2, \vec{u}$. In the third case (*Visser-app*), the term contains an application with one of the variables bound by the Visser rule on the left hand side, *i.e.* the proof uses one of the Visser assumptions to prove the disjunction. We reduce to the corresponding case u_j, where $\lambda\vec{x}.t$ is substituted for the assumption of type $(B_i \to C_i)_{i=1\ldots n} \to B_j$. The reduction relation $\to_{\mathbf{V}}$ is obtained as usual as the structural closure of the reduction $\mapsto_{\mathbf{V}}$ (and similarly for $\to_{\mathbf{IPC}}$).

As expected, **V**–terms normalize: we prove normalization by providing an evaluation function that reduces **V**–terms to intuitionistic terms. The idea is to define the evaluator by structural recursion on typed terms, and using normalization for **IPC** after each recursive call.

Theorem A.1 (Normalization for **V**)**.** **V** enjoys the normalization property.

The following is a consequence of Lemma A.2:

Theorem 2.1. **V**–terms normalize to **IPC**–terms.

3 Beyond IPC: Harrop's Rule and KP

In the previous section we have been expecially careful in imposing the restriction on the open assumptions for the application of our new rules, in order to keep our calculus inside the intuitionistic world and to obtain precisely a characterization of admissibility. At this point, however, one can legitimately ask: what happens if we lift such restriction, and allow one or more admissible principles inside an extended logic? The system of rules we introduced assumes then a different role, that is the role of providing a simple and modular way to obtain Curry-Howard systems for semi-classical logics arising from the addition to **IPC** of axioms corresponding to admissible principles.

The simplest and oldest studied admissible rule of **IPC** is the rule of *independence of premise*, also known as *Harrop's rule* in its propositional variant [4]:

$$\neg B \to A_1 \vee A_2 \;/\; (\neg B \to A_1) \vee (\neg B \to A_2)$$

The logic that arises by adding it to **IPC** has also been studied, and is known as Kreisel-Putnam logic (**KP**). It was introduced by G. Kreisel and H. Putnam [8] to show a logic stronger than **IPC** that still could satisfy the disjunction property, thus providing a counterexample to the conjecture of Łukasiewicz that **IPC** was the only such logic.

We now proceed to define a Curry-Howard calculus for **KP** as an instance of the system we presented in the previous section. It suffices to realize that Harrop's rule is a particular case of Visser_1 where the formula C is taken to be $\bot$ (note that the third disjunct in this instance of Visser_1 becomes $\neg B \to B$, that implies both the other hypotheses $\neg B \to A_1$ and $\neg B \to A_2$; for this reason we can ignore it). Then we get the following simplified rule in natural deduction:

$$\text{Harrop}\ \frac{\begin{array}{ccc}[\neg B] & [\neg B \to A_1] & [\neg B \to A_2] \\ \vdots & \vdots & \vdots \\ A_1 \vee A_2 & D & D\end{array}}{D}$$

The restriction on the assumptions of the main premise is now gone, and open proofs are allowed. In fact Harrop's principle is provable in our system:

$$\dfrac{\dfrac{\dfrac{[\neg B \to A_1 \vee A_2]_{(2)} \qquad [\neg B]_{(1)}}{A_1 \vee A_2} \quad \text{Harrop} \quad \dfrac{[\neg B \to A_1]_{(1)}}{(\neg B \to A_1) \vee (\neg B \to A_2)} \qquad \dfrac{[\neg B \to A_2]_{(1)}}{(\neg B \to A_1) \vee (\neg B \to A_2)}}{(\neg B \to A_1) \vee (\neg B \to A_2)}\,(1)}{(\neg B \to A_1 \vee A_2) \to (\neg B \to A_1) \vee (\neg B \to A_2)}\,(2)$$

The proof term is a simplified version of the proof term for V_1, where we remove the term corresponding to the trivialized third disjunct:

$$\frac{\Gamma, x\colon \neg B \vdash t\colon A_1 \vee A_2 \qquad \Gamma, y\colon \neg B \to A_1 \vdash s_1\colon D \qquad \Gamma, y\colon \neg B \to A_2 \vdash s_2\colon D}{\Gamma \vdash \mathtt{hop}[x.t \parallel y.s_1 \mid y.s_2]\colon D}$$

By inspecting the reduction rules for **V**, we realize that the rule *Visser-app* has no counterpart in **KP**: since the Harrop assumptions have negated type, their use in proof terms is completely encapsulated in exfalso terms (see Classification, Lemma B.1 below). Therefore the reduction rules for **KP** are the ones for **IPC** (Figure 2) plus the additional rules *Harrop-inj* and *Harrop-efq* in Figure 3. We denote with $\mapsto_{\mathbf{KP}}$ the toplevel reduction for **KP**, and with $\to_{\mathbf{KP}}$ its structural closure.

–	Harrop-inj	$\mathtt{hop}[x.\mathtt{inj}_i t \parallel y.s_1 \mid y.s_2]$	$\mapsto$	$s_i\{\lambda x.t/y\}$
–	Harrop-efq	$\mathtt{hop}[x.W\langle \mathtt{efq}\, t\rangle \parallel y.s_1 \mid y.s_2]$	$\mapsto$	$s_1\{(\lambda x.\mathtt{efq}\, t)/y\}$

Figure 3: Reduction rules (**KP**)

We prove for **KP** the usual properties of *subject reduction*, *classification*, and *strong normalization*. As expected we denote with $\vdash_{\mathbf{KP}}$ the provability in **KP**, but we use simply $\vdash$ when not ambiguous.

Theorem B.1 (Subject reduction for **KP**)**.** If $\Gamma \vdash_{\mathbf{KP}} t : A$ and $t \to_{\mathbf{KP}} s$, then $\Gamma \vdash_{\mathbf{KP}} s : A$.

In order to classify normal forms of **KP**, we need to consider proof terms with possibly open Harrop assumptions: we denote with $\Gamma_\neg$ a *negated* typing context, *i.e.* of the form $\Gamma_\neg = \{x_1 : \neg A_1, \ldots, x_n : \neg A_n\}$. We obtain the following classification of normal forms:

Lemma B.1 (Classification for **KP**)**.** Let $\Gamma_\neg \vdash_{\mathbf{KP}} t : A$ for t in (weak head) normal form and t not $\neg$neutral:

- *Implication*: if $A = B \to C$, then t is an abstraction or a variable in $\Gamma_\neg$;
- *Disjunction*: if $A = B \vee C$, then t is an injection;
- *Conjunction*: if $A = B \wedge C$, then t is a pair;
- *Falsity*: if $A = \bot$, then $t = x\,s$ for some s and some $x \in \Gamma_\neg$.

We prove that **KP** enjoys the strong normalization property, *i.e.* all typable terms are strongly normalizing. We use a modified version of the method of *reducibility candidates* by Girard-Tait [2]. The differences with respect to the usual proof are that Harrop and exfalso terms are added to neutral terms, and that the reductions for `hop` (which involve terms under binders) require special treatment.

Theorem B.2 (Strong normalization of **KP**)**.** If $\Gamma \vdash_{\mathbf{KP}} t : A$, then t is strongly normalizing.

The complete proof is on the appendix. We can now prove the disjunction property:

Lemma 3.1 (Consistency)**.** $\nvdash_{\mathbf{KP}} t : \bot$ for no t.

Proof. Let us assume that there exists t (which we assume in normal form by Theorem B.2) such that $\vdash_{\mathbf{KP}} t : \bot$, and derive a contradiction. We proceed by induction on the size of t. The base case is impossible because by Lemma B.1 t cannot be a variable. As for the inductive case, by Lemma B.1, t is either an exfalso, or $x\,u \in \Gamma_\neg$ for some $x \in \Gamma_\neg$. In the former case $t = \mathtt{efq}\, s$ for some s such that $\vdash_{\mathbf{KP}} s : \bot$, and we use the *i.h.*; the latter case is not possible, since $\Gamma_\neg = \emptyset$. □

Theorem 3.1 (Disjunction property)**.** If $\vdash A \vee B$, then $\vdash A$ or $\vdash B$.

Proof. Assume $\vdash t : A \vee B$ for t in normal form by Theorem B.2. First note that $t \neq \mathtt{efq}\, s$, because otherwise by inversion $\vdash s : \bot$, contradicting consistency. By Lemma B.1 (with $\Gamma_\neg = \emptyset$) t is an injection. Conclude by inversion. □

4 Conclusions and Future Work

Our system provides a meaningful explanation of the admissible rules in terms of normalization of natural deduction proofs. In addition, by simply lifting the condition of having closed proofs on the main premise, we can study intermediate logics characterized by the axioms corresponding to some admissible rules; the study of the Kreisel-Putnam logic exemplifies this approach.

We believe that our presentation is well-suited to continue the study of admissibility in intuitionistic systems, a subject that is currently mostly explored with semantic tools. We devised powerful proofs of normalization for our systems **KP** and **V**, and we will try to extend these results to other similarly obtained systems. We conclude with some remarks on future generalizations.

4.1 The Logic AD

Now that we have shown the potential of our system in analysing the extension of **IPC** with axioms corresponding to admissible rules, we might wonder what could happen when we try to add several of them. We can be even more ambitious: what if we want to add *all* the Visser rules to **IPC**? A theorem by Rozière greatly simplifies our task:

Theorem 4.1 (Rozière [9])**.** All Visser rules are derivable in the logic **AD**, obtained by adding the V_1 axiom schema to **IPC**.

Clearly, since the Visser rules are derivable in **AD** they are also admissible; as we know from Theorem 1.1 this means that they form a basis for all the admissible rules of **AD**, and since they are derivable we obtain:

Corollary 4.1. The logic **AD** is structurally complete.

However, we also know from Iemhoff [5] that **IPC** is the only logic that has the Visser rules as admissible rules and satisfies the disjunction property. This means that **AD** cannot satisfy the disjunction property. This was also proved with different techniques by Rozière, who also showed that **AD** is still weaker than **CPC**. Given these properties, **AD** seems the best candidate to be studied with our technique.

4.2 Arithmetic

Since its inception with Harrop [4], the motivation for studying admissible rules of **IPC** was to understand arithmetical systems. A famous theorem of de Jongh states that the propositional formulas whose arithmetical instances are provable in *intuitionistic arithmetic* (**HA**) are exactly the theorems of **IPC**, and many studies of the admissible rules of **HA** (like Visser [11], Iemhoff and Artemov [1]) originated from it. In particular Visser shows that the propositional admissible rules of **HA** coincide with those of **IPC**, and that Σ^0_1 rules are also related.

Harrop's principle, that we have investigated in this paper, is also known as the propositional Independence of Premise principle. Its first order version:

$$(\neg A \to \exists x.B(x)) \to \exists x.(\neg A \to B(x)) \tag{IP}$$

corresponds to an admissible rule of **HA** that has an important status in the theory of arithmetic, and was given a constructive interpretation for example by Gödel [3] with his well known *Dialectica* interpretation.

We can assign to IP a proof term and two reduction rules that act in the same way as the ones introduced for Harrop's rule: that is, we will distinguish the two cases where there is an explicit proof of the existential in the antecedent, and where an exfalso reasoning has been carried on. We believe that a more advanced study of other admissible rules of **HA** can be carried on similar grounds.

References

[1] Sergei N. Artemov & Rosalie Iemhoff (2004): *From de Jongh's theorem to intuitionistic logic of proofs*. In: *Dick de Jongh's Festschrift*, pp. 1–10. Available at `https://istina.msu.ru/publications/article/19375470/`.

[2] Jean-Yves Girard, Paul Taylor & Yves Lafont (1989): *Proofs and types*. *Cambridge tracts in theoretical computer science* 7, Cambridge University Press, Cambridge. Available at `http://www.paultaylor.eu/stable/prot.pdf`.

[3] Kurt Gödel (1958): *Über eine bisher noch nicht bentzte Erweiterung des finiten Standpunktes*. *Dialectica* 12(3-4), pp. 280–287, doi:10.1111/j.1746-8361.1958.tb01464.x.

[4] Ronald Harrop (1956): *On disjunctions and existential statements in intuitionistic systems of logic*. *Mathematische Annalen* 132(4), pp. 347–361, doi:10.1007/BF01360048.

[5] Rosalie Iemhoff (2001): *A(nother) characterization of intuitionistic propositional logic*. *Annals of Pure and Applied Logic* 113(1), pp. 161–173, doi:10.1016/S0168-0072(01)00056-2.

[6] Rosalie Iemhoff (2001): *On the admissible rules of intuitionistic propositional logic*. *The Journal of Symbolic Logic* 66(1), pp. 281–294, doi:10.2307/2694922.

[7] Rosalie Iemhoff (2005): *Intermediate logics and Visser's rules*. *Notre Dame Journal of Formal Logic* 46(1), pp. 65–81, doi:10.1305/ndjfl/1107220674.

[8] Georg Kreisel & Hilary Putnam (1957): *Eine Unableitbarkeitsbeweismethode für den Intuitionistischen Aussagenkalkl*. *Archiv für mathematische Logik und Grundlagenforschung* 3(3-4), pp. 74–78, doi:10.1007/BF01988049.

[9] Paul Rozière (1993): *Admissible and Derivable Rules in Intuitionistic Logic*. *Mathematical Structures in Computer Science* 3(2), pp. 129–136, doi:10.1017/S0960129500000165.

[10] Morten Heine Sørensen & Pawel Urzyczyn (2006): *Lectures on the Curry-Howard isomorphism*. *Studies in Logic and the Foundations of Mathematics* 149, Elsevier, doi:10.1016/s0049-237x(06)x8001-1.

[11] Albert Visser (2002): *Substitutions of Σ^0_1-sentences: explorations between intuitionistic propositional logic and intuitionistic arithmetic*. *Annals of Pure and Applied Logic* 114(1), pp. 227–271, doi:10.1016/S0168-0072(01)00081-1.

A Theorems on V

First some definitions. We denote with $\vdash_{\mathbf{V}}$ the provability in **V** (but we use $\vdash$ when not ambiguous). We denote with $\Gamma_{\to}$ an *implicative* typing context, *i.e.* of the form $\Gamma_{\to} = \{x_1 : A_1 \to B_1, \ldots, x_n : A_n \to B_n\}$. We say that a term is $\to$*neutral* if it has the form $W\langle x\, s\rangle$ or $W\langle \mathtt{efq}\, s\rangle$.

Lemma A.1 (Classification for **V**)**.** Let $\Gamma_{\to} \vdash_{\mathbf{V}} t : A$ for t in normal form, and t not $\to$neutral:

- *Implication*: if $A = B \to C$, then t is either an abstraction or a variable in $\Gamma_{\to}$;
- *Disjunction*: if $A = B \vee C$, then t is an injection;
- *Conjunction*: if $A = B \wedge C$, then t is a pair;

Proof. By induction on the type derivation of t:

- (ax) t is a variable in $\Gamma_{\to}$. By definition of $\Gamma_{\to}$, the type of t is an implication, and we conclude.
- $(\to_I)$ t is an abstraction, and we conclude.
- $(\to_E)$ and $t = s\,u$ with $\Gamma_{\to} \vdash s : B \to C$. Because t is in normal form, s cannot be an abstraction. By *i.h.*, s is either a variable in $\Gamma_{\to}$ or is $\to$neutral; in both cases t is $\to$neutral.

- ($\vee_I$) t is an injection, and we conclude.
- ($\vee_E$) and $t = \mathtt{case}[s \parallel - \mid -]$ with $\Gamma_\to \vdash s\colon D \vee D'$. Because t is in normal form, s cannot be an injection. By *i.h.* s is $\to$neutral, and therefore t is $\to$neutral.
- ($\wedge_I$) t is a pair, and we conclude.
- ($\wedge_E$) and $t = \mathtt{proj}_i\, s$ with $\Gamma_\to \vdash s\colon D \wedge D'$. Because t is in normal form, s cannot be a pair. By *i.h.* s is $\to$neutral, and therefore t is $\to$neutral.
- (Visser$_n$) not possible. Assume $t = \mathtt{V}_n[\vec{x}.s \parallel - \mid - \parallel -]$ with $\vec{x}\colon (A_i \to B_i)_{i=1\ldots n} \vdash s\colon A_1 \vee A_2$ by inversion, and derive a contradiction. By *i.h.* s is $\to$neutral or an injection, but both cases contradict the hypothesis that t is a normal form.

□

In order to prove normalization, we define an evaluation function $\mathrm{eval}(\cdot)$, mapping each typable term in **V** to its normal form. We first assume a corresponding function for **IPC**:

Definition A.1 ($\mathrm{eval}_{\mathbf{IPC}}(\cdot)$)**.** We call $\mathrm{eval}_{\mathbf{IPC}}(\cdot)$ the function mapping each term typable in **IPC** to its normal form.

Definition A.2 ($\mathrm{eval}(\cdot)$)**.** Let t a term typable in **V**. We define its evaluation $\mathrm{eval}(t)$ by structural induction:

$$
\begin{array}{ll}
\mathrm{eval}(x) & := x \\
\mathrm{eval}(t\,s) & := \mathrm{eval}_{\mathbf{IPC}}(\mathrm{eval}(t)\ \mathrm{eval}(s)) \\
\mathrm{eval}(\lambda x.t) & := \lambda x.\ \mathrm{eval}(t) \\
\mathrm{eval}(\mathtt{efq}\,t) & := \mathtt{efq}\ (\mathrm{eval}(t)) \\
\mathrm{eval}(\langle t,s\rangle) & := \langle \mathrm{eval}(t), \mathrm{eval}(s)\rangle \\
\mathrm{eval}(\mathtt{proj}_i t) & := \mathrm{eval}_{\mathbf{IPC}}(\mathtt{proj}_i\,(\mathrm{eval}(t))) \\
\mathrm{eval}(\mathtt{inj}_i t) & := \mathrm{eval}_{\mathbf{IPC}}(\mathtt{inj}_i\,(\mathrm{eval}(t))) \\
\mathrm{eval}(\mathtt{case}[t \parallel y.s_1 \mid y.s_2]) & := \mathrm{eval}_{\mathbf{IPC}}(\mathtt{case}[\mathrm{eval}(t) \parallel y.\ \mathrm{eval}(s_1) \mid y.\ \mathrm{eval}(s_2)]) \\
\mathrm{eval}(\mathtt{V}_n[\vec{x}.t \parallel y.s_1 \mid y.s_2 \parallel z.\vec{u}]) & := \begin{cases} \mathrm{eval}_{\mathbf{IPC}}(\mathrm{eval}(s_i)\{\lambda\vec{x}.t'/y\}) & \text{if } \mathrm{eval}(t) = \mathtt{inj}_i t' \\ \mathrm{eval}_{\mathbf{IPC}}(\mathrm{eval}(s_1)\{\lambda\vec{x}.\mathtt{efq}\,t'/y\}) & \text{if } \mathrm{eval}(t) = W\langle \mathtt{efq}\,t'\rangle \\ \mathrm{eval}_{\mathbf{IPC}}(\mathrm{eval}(u_j)\{\lambda\vec{x}.t'/z\}) & \text{if } \mathrm{eval}(t) = W\langle x_j t'\rangle \end{cases}
\end{array}
$$

Note: the three cases in the definition of $\mathrm{eval}(\cdot)$ on Visser terms are exhaustive by inspection of the normal forms of type disjunction (Lemma A.1) since it holds by inversion that $\Gamma_\to \vdash t\colon A_1 \vee A_2$ with $\mathrm{dom}(\Gamma_\to) = \vec{x}$.

Lemma A.2 ($\mathrm{eval}(\cdot)$ well-defined)**.** For every **V**-term t s.t. $\Gamma \vdash_{\mathbf{V}} t\colon A$:

1. $\Gamma \vdash_{\mathbf{IPC}} \mathrm{eval}(t)\colon A$,
2. $\mathrm{eval}(t)$ is normal,
3. $t \to_{\mathbf{V}}^* \mathrm{eval}(t)$.

Proof. The three points can be proved mutually, by induction on the type derivation $\Gamma \vdash_{\mathbf{V}} t\colon A$:

1. follows by *i.h.* and by subject reduction for **IPC**;
2. follows by *i.h.* and from the fact that the output of $\mathrm{eval}_{\mathbf{IPC}}(\cdot)$ are only normal forms;
3. follows by *i.h.* and from the fact that **IPC** is a subcalculus of **V**.

□

It easily follows:

Theorem A.1 (Normalization for **V**)**.** **V** enjoys the normalization property.

B Theorems on KP

Theorem B.1 (Subject reduction for **KP**). If $\Gamma \vdash_{\mathbf{KP}} t : A$ and $t \to_{\mathbf{KP}} s$, then $\Gamma \vdash_{\mathbf{KP}} s : A$.

Proof. By the definition of reduction as the closure of $\mapsto_{\mathbf{KP}}$ under evaluation contexts, we just prove the statement when $t \mapsto_{\mathbf{KP}} s$; the general case $t \to_{\mathbf{KP}} s$ follows because substitution preserves types.

The cases of the usual intuitionistic reductions are standard (see for example [10]); we just prove the cases of the reduction rules associated with $\mathtt{hop}$.

For the case of the left injection $\mathtt{hop}[x.\mathtt{inj}_1 t \parallel y.s_1 \mid y.s_2] \mapsto s_1\{\lambda x.t/y\}$, by inversion we have $\Gamma, y : \neg B \to A_1 \vdash s_1 : D$ and $\Gamma, x : \neg B \vdash \mathtt{inj}_1 t : A_1 \vee A_2$ for some A_1, A_2, B, D. Again by inversion $\Gamma, x : \neg B \vdash x : A_1$, and by $\to_I$ we obtain $\Gamma \vdash \lambda x.t : \neg B \to A_1$. By substitutivity we get the desired result $\Gamma \vdash s_1\{\lambda x.t/y\} : D$. The case of the right injection is analogous.

Finally, if $\mathtt{hop}[x.W\langle \mathtt{efq}\, t\rangle \parallel y.s_1 \mid y.s_2] \mapsto s_1\{\lambda x.\mathtt{efq}\, t/y\}$, by inversion we have $\Gamma, y : \neg B \to A_1 \vdash s_1 : D$ and $\Gamma, x : \neg B \vdash W\langle \mathtt{efq}\, t\rangle : A_1 \vee A_2$ for some A_1, A_2, B, D. It is easy to see, by induction on the definition of weak head contexts and by inversion, that $\Gamma, x : \neg B \vdash t : \bot$; by $\bot_E$ we obtain $\Gamma, x : \neg B \vdash \mathtt{efq}\, t : A_1$. By $\to_I$ we obtain $\Gamma \vdash \lambda x.\mathtt{efq}\, t : \neg B \to A_1$, and by substitutivity we get the desired result $\Gamma \vdash s_1\{\lambda x.\mathtt{efq}\, t/y\} : D$. □

We say that a term is $\neg$*neutral* if it has the form $W\langle \mathtt{efq}\, t\rangle$.

Lemma B.1 (Classification for **KP**). Let $\Gamma_\neg \vdash_{\mathbf{KP}} t : A$ for t in (weak head) normal form and t not $\neg$neutral:

- *Implication*: if $A = B \to C$, then t is an abstraction or a variable in $\Gamma_\neg$;
- *Disjunction*: if $A = B \vee C$, then t is an injection;
- *Conjunction*: if $A = B \wedge C$, then t is a pair;
- *Falsity*: if $A = \bot$, then $t = x\,s$ for some s and some $x \in \Gamma_\neg$.

Proof. By induction on the type derivation of t:

- (ax) and t is a variable in $\Gamma_\neg$: by definition of $\Gamma_\neg$, the type of t is an implication, and we conclude.
- ($\to_I$) and t is an abstraction: trivial.
- ($\to_E$) and $t = s\,u$ with $\Gamma_\neg \vdash s : B \to A$. Because t is in normal form, s cannot be an abstraction. By *i.h.*, s is either a variable in $\Gamma_\neg$ or a $\neg$neutral term. In the first case, note that we have that $A = \bot$ and $t = xs$, and the thesis holds; in the second case, t is $\neg$neutral and the thesis holds.
- ($\vee_I$) and t is an injection: trivial.
- ($\vee_E$) and $t = \mathtt{case}[s \parallel - \mid -]$ with $\Gamma_\neg \vdash s : D_1 \vee D_2$. By *i.h.* s is either an injection or $\neg$neutral. The first case is not possible because t is in normal form; in the second case, t is $\neg$neutral as required.
- ($\wedge_I$) and t is a pair: trivial.
- ($\wedge_E$) and $t = \mathtt{proj}_i s$ with $\Gamma_\neg \vdash s : D_1 \wedge D_2$. By *i.h.* s is either a pair or $\neg$neutral, but the first case contradicts the hypothesis that t is in normal form. Therefore s is $\neg$neutral, and also t is $\neg$neutral.
- ($\bot_E$) then t is immediately $\neg$neutral.
- (Harrop) not possible. Assume $t = \mathtt{hop}[x.s \parallel - \mid -]$ with $\Gamma_\neg, x : \neg B \vdash s : D_1 \vee D_2$, and derive a contradiction. By *i.h.* s is an injection or a $\neg$neutral term, but both cases contradict the hypothesis that t is in normal form.

□

B.1 Strong Normalization

In this section, we prove the strong normalization property for **KP** by means of an adapted version of Girard's method of candidates [2].

Definition B.1 (Weak head **KP** contexts)**.**

$$K ::= \Box \mid K\,s \mid \mathtt{proj}_i\,K \mid \mathtt{case}[K \parallel y.s_1 \mid y.s_2] \mid \mathtt{hop}[x.K \parallel y.s_1 \mid y.s_2]$$

Let SN be the set of *strongly normalizing terms* of **KP**. By abuse of notation, we say that a context – be it an **IPC** context W or a **KP** context K – is strongly normalizing if all its "internal" λ-terms are strongly normalizing.

Definition B.2 (Weak head reduction $\to_{\mathrm{SN}}$, $\twoheadrightarrow_{\mathrm{SN}}$)**.** We define $\to_{\mathrm{SN}}$ as the "strongly normalizing" closure of $\mapsto_{\mathbf{KP}}$ (Figure 2) under weak head contexts:

$$\begin{array}{lll}
K\langle(\lambda x.t)\,s\rangle & \to_{\mathrm{SN}} & K\langle t\{s/x\}\rangle \\
K\langle \mathtt{proj}_i\texttt{<}s_1\,,\,s_2\texttt{>}\rangle & \to_{\mathrm{SN}} & K\langle s_i\rangle \\
K\langle \mathtt{case}[\mathtt{inj}_i t \parallel y.s_1 \mid y.s_2]\rangle & \to_{\mathrm{SN}} & K\langle s_i\{t/y\}\rangle \\
K\langle \mathtt{hop}[x.\mathtt{inj}_i t \parallel y.s_1 \mid y.s_2]\rangle & \to_{\mathrm{SN}} & K\langle s_i\{\lambda x.t/y\}\rangle \\
K\langle \mathtt{hop}[x.W\langle \mathtt{efq}\,t\rangle \parallel y.s_1 \mid y.s_2]\rangle & \to_{\mathrm{SN}} & K\langle s_1\{(\lambda x.\mathtt{efq}\,t)/y\}\rangle
\end{array}$$

for every SN contexts W, K and $t, s, s_1, s_2 \in \mathrm{SN}$. As usual, we denote by $\to^*_{\mathrm{SN}}$ the reflexive and transitive closure of $\to_{\mathrm{SN}}$. A term t is a $\to_{\mathrm{SN}}$-normal form (in short, $\to_{\mathrm{SN}}$nf) if $t \not\to_{\mathrm{SN}}$. We say that $t \twoheadrightarrow_{\mathrm{SN}} s$ if $t \to^*_{\mathrm{SN}} s$ and s is a $\to_{\mathrm{SN}}$nf.

By inspection of the reduction rules, one may prove:

Lemma B.2. $\to_{\mathrm{SN}}$ is deterministic.

One of the main properties of reducibility candidates is that they are *backward closed* under reduction:

Definition B.3 (Backward closure $\overleftarrow{\cdot}$)**.** Let T be a set of $\to_{\mathrm{SN}}$nfs. We define its *closure under backward weak head reduction* as the set $\overleftarrow{T} := \{s \mid s \twoheadrightarrow_{\mathrm{SN}} t \in T\}$.

Lemma B.3 (Backward closure of SN)**.** SN is *backward closed* under $\to_{\mathrm{SN}}$.

Proof. Let $t \in \mathrm{SN}$ and $s \to_{\mathrm{SN}} t$; we need show that $s \in \mathrm{SN}$. By cases on the reduction rules of Definition B.2; we only consider the case of *Harrop-inj*, as one can proceed in a similar way for the other reduction rules. Let $s = K\langle \mathtt{hop}[x.\mathtt{inj}_i t' \parallel y.s'_1 \mid y.s'_2]\rangle \to_{\mathrm{SN}} K\langle s'_i\{\lambda x.t'/y\}\rangle = t$, and let us consider a reduction sequence beginning with s. Either the sequence terminates after some internal redutions

$$s \to^* K'\langle \mathtt{hop}[x.\mathtt{inj}_i t'' \parallel y.s''_1 \mid y.s''_2]\rangle$$

which must terminate because all internal terms are SN by definition of $\to_{\mathrm{SN}}$, or eventually we have

$$K'\langle \mathtt{hop}[x.\mathtt{inj}_i t'' \parallel y.s''_1 \mid y.s''_2]\rangle \to K'\langle s''_i\{\lambda x.t''/y\}\rangle.$$

This term is strongly normalizing because it is a reduct of t, and by hypothesis $t \in \mathrm{SN}$. Therefore the reduction sequence must terminate. □

Another key notion are *neutral terms*, that are intuitively $\to_{\mathrm{SN}}$nfs that do not begin with constructors:

Definition B.4 (Neutral terms)**.** $\mathrm{Ne} := \{K\langle x\rangle \mid K \text{ is SN and } x \text{ a variable}\} \cup \{W\langle \mathtt{efq}\, t\rangle \mid W \text{ and } t \text{ are SN}\}$.

Fact B.1. Neutral terms are strongly normalizing $\to_{\mathrm{SN}}$nfs.

We are now ready to define the semantics of formulas:

Definition B.5 (Denotation $[\![\cdot]\!]$)**.**

1. $[\![p]\!] := \mathrm{SN}$ for every p atomic (also $p = \bot$),
2. $[\![A \to B]\!] := \overleftarrow{\{\lambda x.t \mid \forall s \in [\![A]\!], t\{s/x\} \in [\![B]\!]\}} \cup \overleftarrow{\mathrm{Ne}}$,
3. $[\![A_1 \wedge A_2]\!] := \overleftarrow{\{\texttt{<}t_1\texttt{ , }t_2\texttt{>} \mid t_i \in [\![A_i]\!]\}} \cup \overleftarrow{\mathrm{Ne}}$,
4. $[\![A_1 \vee A_2]\!] := \overleftarrow{\{\mathtt{inj}_i t \mid t \in [\![A_i]\!]\}} \cup \overleftarrow{\mathrm{Ne}}$.

In fact, we note that our definition produces candidates of reducibility:

Lemma B.4 (Denotations are candidates)**.** For every A, its denotation:

1. contains only *strongly normalizing* terms: $[\![A]\!] \subseteq \mathrm{SN}$
2. contains all *neutral terms*: $\mathrm{Ne} \subseteq [\![A]\!]$
3. is *backward closed*: if $t \in [\![A]\!]$ and $s \to_{\mathrm{SN}} t$, then $s \in [\![A]\!]$.

Proof. Points 2 and 3 are trivial. Before proving Point 1 we note that as shown in the proof of Lemma B.3, if T contains only strongly normalizing terms, then $\overleftarrow{T}$ does too. We can then prove Point 1 by induction on the structure of types: the case of propositional atoms follows from Definition B.5(1) and Lemma B.3; for the inductive cases, use Fact B.1, the *i.h.* and Lemma B.3. □

We extend the definition of valuation to typing contexts:

Definition B.6. Let Γ be a typing context; we define $[\![\Gamma]\!]$ as the set of substitutions mapping variables in Γ to terms in the denotation of the corresponding type, *i.e.*

$$[\![\Gamma]\!] := \{\sigma \text{ substitution} \mid \mathrm{dom}(\sigma) = \mathrm{dom}(\Gamma) \text{ and } (x \mapsto t) \in \sigma \text{ implies } t \in [\![\Gamma(x)]\!]\}$$

where $\Gamma(x) := A$ when $(x\colon A) \in \Gamma$.

A lemma useful in the proof of Lemma B.6:

Lemma B.5. If $t \to_{\mathrm{SN}} s$ and $t\sigma \in \mathrm{SN}$, then $t\sigma \to_{\mathrm{SN}} s\sigma$.

Proof. First note that if $t = K\langle t'\rangle$ and $t\sigma \in \mathrm{SN}$, then $t\sigma = K'\langle t'\sigma\rangle$ for some SN context K'. Therefore, we assume that $K\langle t'\rangle \to_{\mathrm{SN}} K\langle s'\rangle$ with $t' \mapsto s'$, and we prove that $t'\sigma \mapsto s'\sigma$ by cases on the reduction rules:

- $(\lambda y.s)\,u \mapsto s\{u/y\}$. By renaming, $y \notin \mathrm{fv}(\sigma), \mathrm{dom}(\sigma)$. Then $((\lambda y.s)\,u)\sigma = (\lambda y.s\sigma)\,(u\sigma) \mapsto s\sigma\{u\sigma/y\}$, with $s\{u/y\}\sigma = s\{u/y\}\sigma$. We conclude because $s\sigma\{u\sigma/y\} = s\{u/y\}\sigma$ and $s\sigma, u\sigma \in \mathrm{SN}$ by the hypothesis that $t\sigma \in \mathrm{SN}$.
- $\mathtt{proj}_i\texttt{<}t_1\texttt{ , }t_2\texttt{>} \mapsto t_i$. Then $(\mathtt{proj}_i\texttt{<}t_1\texttt{ , }t_2\texttt{>})\sigma = \mathtt{proj}_i\texttt{<}t_1\sigma\texttt{ , }t_2\sigma\texttt{>} \mapsto t_i\sigma$, and $t_1\sigma, t_2\sigma \in \mathrm{SN}$ by hypothesis.
- $\mathtt{case[inj}_i t \mathtt{\ ||\ } y.s_1 \mathtt{\ |\ } y.s_2\mathtt{]} \mapsto s_i\{t/y\}$. By renaming, $y \notin \mathrm{fv}(\sigma), \mathrm{dom}(\sigma)$. Similar to the case below.

- $\mathtt{hop}[x.\mathtt{inj}_i t \parallel y.s_1 \mid y.s_2] \mapsto s_i\{\lambda x.t/y\}$. By renaming, $x,y \notin \mathrm{fv}(\sigma), \mathrm{dom}(\sigma)$. Then $\mathtt{hop}[x.\mathtt{inj}_i t \parallel y.s_1 \mid y.s_2]\sigma = \mathtt{hop}[x.\mathtt{inj}_i(t\sigma) \parallel y.s_1\sigma \mid y.s_2\sigma] \mapsto s_i\sigma\{\lambda x.t\sigma/y\}$. We conclude because $s_i\sigma\{\lambda x.t\sigma/y\} = (s_i\{\lambda x.t/y\})\sigma$.
- $\mathtt{hop}[x.W\langle \mathtt{efq}\, t\rangle \parallel y.s_1 \mid y.s_2] \mapsto s_1\{\lambda x.\mathtt{efq}\, t/y\}$. By renaming, $x,y \notin \mathrm{fv}(\sigma), \mathrm{dom}(\sigma)$. Then $\mathtt{hop}[x.W\langle \mathtt{efq}\, t\rangle \parallel y.s_1 \mid y.s_2]\sigma = \mathtt{hop}[x.W'\langle \mathtt{efq}\, t\sigma\rangle \parallel y.s_1\sigma \mid y.s_2\sigma]$ for some SN context W'. We have $\mathtt{hop}[x.W'\langle \mathtt{efq}\, t\sigma\rangle \parallel y.s_1\sigma \mid y.s_2\sigma] \mapsto s_1\sigma\{\lambda x.\mathtt{efq}\,(t\sigma)/y\}$, and we conclude because $s_1\sigma\{\lambda x.\mathtt{efq}\,(t\sigma)/y\} = s_1\{\lambda x.\mathtt{efq}\, t/y\}\sigma$.

□

Lemma B.6 (Fundamental lemma)**.** If $\Gamma \vdash t : A$ and $\sigma \in [\![\Gamma]\!]$, then $t\sigma \in [\![A]\!]$.

Proof. By induction on the type derivation. The base case is the axiom, and instantiated variables belong to the corresponding denotations by the definition of $[\![\Gamma]\!]$. Let us now proceed by cases on the rules of inference:

($\to_I$) Assume that for all $\sigma \in [\![\Gamma, x\colon A]\!]$, $t\sigma \in [\![B]\!]$; we need to prove that for all $\sigma \in [\![\Gamma]\!]$, $(\lambda x.t)\sigma \in [\![A \to B]\!]$. Let $\sigma \in [\![\Gamma]\!]$, and by renaming $x \notin \mathrm{dom}(\sigma) \cup \mathrm{fv}(\sigma)$. Then $(\lambda x.t)\sigma = \lambda x.t\sigma$. By Definition B.5(2), $\lambda x.t\sigma \in [\![A \to B]\!]$ iff for all $s \in [\![A]\!]$, $t\sigma\{s/x\} \in [\![B]\!]$. By taking $\sigma' := \sigma \cup \{s/x\}$, this follows from the *i.h.* and from the hypothesis on σ.

($\to_E$) We need to prove that for all $\sigma \in [\![\Gamma]\!]$, $(t\,s)\sigma \in [\![B]\!]$. Note that $(t\,s)\sigma = (t\sigma)(s\sigma)$. By *i.h.* $t\sigma \in [\![A \to B]\!]$, and therefore by Definition B.5(2), either:

- $t\sigma \twoheadrightarrow_{\mathrm{SN}} n \in \mathrm{Ne}$: then $(t\sigma)(s\sigma) \to^*_{\mathrm{SN}} n(s\sigma)$ since $s\sigma \in \mathrm{SN}$ (by *i.h.* and Lemma B.4(1)) Note that $n(s\sigma)$ is neutral, and we conclude by Lemma B.4(2) and Lemma B.4(3).
- $t\sigma \twoheadrightarrow_{\mathrm{SN}} \lambda y.u$: then $(t\sigma)(s\sigma) \to^*_{\mathrm{SN}} (\lambda y.u)\,(s\sigma) \to_{\mathrm{SN}} u\{s\sigma/y\} \in [\![B]\!]$ by Definition B.5(2). Conclude by Lemma B.4(3).

($\bot_I$) By the hypothesis, for every $\sigma \in [\![\Gamma]\!]$, $t\sigma \in [\![\bot]\!]$. We need to prove that $(\mathtt{efq}\, t)\sigma \in [\![A]\!]$. By Lemma B.4(1) $t\sigma \in \mathrm{SN}$, and since $(\mathtt{efq}\, t)\sigma = \mathtt{efq}\,(t\sigma)$, $(\mathtt{efq}\, t)\sigma$ is a neutral term. Conclude by Lemma B.4(2).

($\wedge_I$) Let $\Gamma \vdash t_1 : A_1$ and $\Gamma \vdash t_2 : A_2$: we need to prove that for every $\sigma \in [\![\Gamma]\!]$, $\langle t_1, t_2\rangle\sigma \in [\![A_1 \wedge A_2]\!]$. Since $\langle t, s\rangle\sigma = \langle t\sigma, s\sigma\rangle$, the claim follows from Definition B.5(3) and the *i.h.* $t\sigma \in [\![A]\!]$ and $s\sigma \in [\![B]\!]$.

($\wedge_E$) Let $\Gamma \vdash s : A_1 \wedge A_2$, and by *i.h.* $s\sigma \in [\![A_1 \wedge A_2]\!]$ for every $\sigma \in [\![\Gamma]\!]$. We need to prove that $(\mathtt{proj}_1 s)\sigma \in [\![A_1]\!]$ and $(\mathtt{proj}_2 s)\sigma \in [\![A_2]\!]$ for every $\sigma \in [\![\Gamma]\!]$. There are two cases:

- $s\sigma \twoheadrightarrow_{\mathrm{SN}} n \in \mathrm{Ne}$: then $\mathtt{proj}_i(s\sigma) \twoheadrightarrow_{\mathrm{SN}} \mathtt{proj}_i n$ and we conclude by Lemma B.4(2) and Lemma B.4(3) because that term is neutral.
- $u\sigma \twoheadrightarrow_{\mathrm{SN}} \langle t_1, t_2\rangle$ for some $t_1 \in [\![A_1]\!]$ and $t_2 \in [\![A_2]\!]$: therefore $\mathtt{proj}_i(u\sigma) \to^*_{\mathrm{SN}} \mathtt{proj}_i\langle t_1, t_2\rangle \to_{\mathrm{SN}} t_i \in [\![A_i]\!]$. Conclude by Lemma B.4(3) since $(\mathtt{proj}_i u)\sigma = \mathtt{proj}_i(u\sigma)$.

($\vee_I$) We discuss the case of $\mathtt{inj}_1$; the case of $\mathtt{inj}_2$ is symmetric. Let $\Gamma \vdash t : A$, and by *i.h.* $t\sigma \in [\![A]\!]$ for every $\sigma \in [\![\Gamma]\!]$. We show that also $(\mathtt{inj}_1 t)\sigma \in [\![A \vee B]\!]$ for every $\sigma \in [\![\Gamma]\!]$. Note that $(\mathtt{inj}_1 t)\sigma = \mathtt{inj}_1\,(t\sigma)$, and conclude by *i.h.* and Definition B.5(4).

($\vee_E$) This case is just a simplified version of the following argument for the Harrop rule.

(Harrop) We need to prove that $(\mathtt{hop}[x.t \parallel y.s_1 \mid y.s_2])\sigma \in [\![D]\!]$ for every $\sigma \in [\![\Gamma]\!]$. We first note that $(\mathtt{hop}[x.t \parallel y.s_1 \mid y.s_2])\sigma = \mathtt{hop}[x.t\sigma \parallel y.s_1\sigma \mid y.s_2\sigma]$ (assuming by renaming that x and y do not occur in σ). Let $\sigma' := \sigma \cup \{x/x\}$. $t\sigma = t\sigma'$ and by *i.h.* $t\sigma' \in [\![A_1 \vee A_2]\!]$. There are three cases:

- $t\sigma' \twoheadrightarrow_{\mathrm{SN}} \mathtt{inj}_i\, u_i$ for $u_i \in [\![A_i]\!]$: then also $\mathtt{hop}[x.t\sigma \parallel y.s_1\sigma \mid y.s_2\sigma] \to^*_{\mathrm{SN}} s_i\sigma\{\lambda x.u_i/y\}$. In order to be able to use the *i.h.* we need to show that $\sigma \cup \{\lambda x.u_i/y\} \in [\![\Gamma, y\colon \neg B \to A_i]\!]$, *i.e.* that $\lambda x.u_i \in [\![\neg B \to A_i]\!]$, that by definition holds iff for every $t' \in [\![\neg B]\!]$, $u_i\{t'/x\} \in [\![A_i]\!]$. In order to show the latter, take $\sigma'' := \sigma \cup \{t'/x\}$: then by *i.h.* $t\sigma'' \in [\![A_1 \vee A_2]\!] \subseteq \mathrm{SN}$, and therefore by Lemma B.5 $t\sigma'' = t\sigma'\{t'/x\} \to^*_{\mathrm{SN}} \mathtt{inj}_i\,(u_i\{t'/x\}) \twoheadrightarrow_{\mathrm{SN}} \mathtt{inj}_i\, u_i'$ for $u_i\{t'/x\} \twoheadrightarrow_{\mathrm{SN}} u_i'$. By Definition B.5(4) $u_i' \in [\![A_i]\!]$, but also $u_i\{t'/x\}$ by Lemma B.4(3), and we conclude.
- $t\sigma' \twoheadrightarrow_{\mathrm{SN}} W\langle \mathtt{efq}\, u\rangle \in \mathrm{Ne}$: then also $\mathtt{hop}[x.t\sigma \parallel y.s_1\sigma \mid y.s_2\sigma] \to^*_{\mathrm{SN}} s_1\sigma\{\lambda x.\mathtt{efq}\, u/y\}$. As above, in order to use the *i.h.* and conclude we only need to prove that $(\lambda x.\mathtt{efq}\, u) \in [\![\neg B \to A_1]\!]$. By Definition B.5(2), this is the case if and only if for all $u' \in [\![\neg B]\!]$, $(\mathtt{efq}\, u)\{u'/x\} \in [\![A_1]\!]$. This is proved similarly as the point above, and it follows by Lemma B.5 and the definition of inert terms.
- $t\sigma' \twoheadrightarrow_{\mathrm{SN}} K\langle z\rangle \in \mathrm{Ne}$: we conclude as usual because $\mathtt{hop}[x.K\langle z\rangle \parallel y.s_1\sigma \mid y.s_2\sigma]$ is neutral as well.

□

Theorem B.2 (Strong normalization of **KP**)**.** If $\Gamma \vdash_{\mathbf{KP}} t\colon A$, then t is strongly normalizing.

Proof. By Lemma B.6, $t\sigma \in [\![A]\!]$ for every $\sigma \in [\![\Gamma]\!]$. We now take σ as the *identity substitution*, mapping the variables in Γ to themselves. Note that this is an allowed substitution since variables are neutral terms and therefore are contained in the denotation of every proposition (Lemma B.4(2)). It follows that $t = t\sigma \in [\![A]\!]$, and we conclude because $[\![A]\!]$ contains only SN terms by Lemma B.4(1). □