A Computational Interpretation of Modal Proofs

Simone Martini Andrea Masini *

Abstract

The usual (e.g. Prawitz's) treatment of natural deduction for modal logics involves a complicated rule for the introduction of the necessity, since the naive one does not allow normalization. We propose natural deduction systems for the positive fragments of the modal logics K, K4, KT, and S4, extending previous work by Masini on a two-dimensional generalization of Gentzen's sequents (2-sequents). The modal rules closely match the standard rules for an universal quantifier and different logics are obtained with simple conditions on the elimination rule for $\Box$. We give an explicit term calculus corresponding to proofs in these systems and, after defining a notion of reduction on terms, we prove its confluence and strong normalization.

1. Introduction

The proof theoretical approach has been proved of valuable importance in several computer science areas. The functional programming field, for instance, has received a good momentum from the so-called *Curry-Howard isomorphism*, the observation that typed functional programs can be considered as (and, in fact, are the same thing as) natural deduction proofs of the formulas corresponding to their types. Theories already well developed by their own sake — normalization, confluence, type inference, denotational semantics, category theory, to name just a few of them — could then merge together, suggesting new sound extensions to existing languages and guiding the design of new systems and new implementations. The leading example here is the language Standard ML [MTH90], whose design has been inspired by proof theory from scratch, but we can think also of CAML, the ML dialect developed in Paris [CCM85], whose (efficient) implementation is directly derived from the categorical semantics of natural deduction intuitionistic proofs, or of the several laboratory languages (both for programming and program verification) derived from higher order logic, e.g. [Con86, PHH93].

Also the logic programming field, whose evolution has been mainly driven by model theoretic issues (with the exception of resolution-related matters, of course) has recently discovered that a sound and deep rooting in proof theory can offer a key insight for the design of good, well balanced extensions to the paradigm. The work of Miller *et al.* [MNPS91], relating resolution to the search for suitable "uniform" proofs in extensions of Horn logic, or of Andreoli and Pareschi [AP90], connecting logic programming and linear logic, are paradigmatic of this trend.

The mathematical theory of concurrency, finally, has also drawn off ideas, techniques and systems from proof theory: both the π-calculus of Milner [MPW89], and the concurrent rewriting logic of Meseguer [Mes92] — once again to name just two recent papers — are proof theoretical in spirit and matter.

The situation is very different for the applications of modal logics. The pioneering work in this field is due to Pnueli [Pnu77], whose basic idea (and, in fact, of most of the papers on this topic) was to make the modal quantifier $\Box$ range over computations of concurrent systems. In this way the formula $\Box\sigma$ would assert that the property σ has to be true in each state of each possible computation.

Following this approach, and depending on the kind of observations one allows over a computation, a large variety of modal logics (usually called "temporal logics" in computer science) have been

*Dipartimento di Informatica Università di Pisa Corso Italia, 40 I-56125 Pisa Italy {martini,masini}@di.unipi.it

proposed. It is interesting to observe that all of them are essentially multimodal logics obtained by combining in a suitable way the well known modal systems K, KD, T, S4, S5.

A quick analysis of the literature shows that all these logics have been introduced and studied following an approach à la Hilbert: a logic is characterized by the class of its models, which, in turn, is characterized by a set of axioms. Since any application of a formalism reflects the features of that formalism, it is no wonder that most applications of modal logics are based on their model theory (think, for instance, to the technique of model checking [EH85, MMS92]).

However, if model theory is a rich and developed field, the same is not true for modal proof theory, thus explaining the lack of applications of this kind. Proof theory of modal logics, though largely studied since the fifties, has always been a delicate subject, the main reason being the apparent impossibility to obtain elegant, natural systems for intensional operators (with the excellent exception of intuitionistic logic). For example Segeberg, not earlier than 1984 [BS84], observed that the Gentzen format, which works so well for truth functional and intuitionistic operators, cannot be *a priori* expected to remain valid for modal logics; carrying to the limit this observation one could even assert that "logics with no good proof theory are *innatural*." In such a way we should mark as "innatural" all modal logics (with great delight of a large number of logicians!).

One of the main drawbacks of modal proof theory is well exemplified, in the context of the logics K, KT, and KD, by Scott's sequent rule:

$$\frac{\Gamma \vdash \sigma}{\Box\Gamma \vdash \Box\sigma}\,.$$

This rule, though allowing the proof of a cut elimination theorem, is neither a left nor a right rule, thus destroying the deep symmetries of the sequent calculus. The situation is even worse with the natural deduction formulation of the same logics, where either there are no explicit modal introduction and elimination rules, as in [BS84], or the rule is formulated as

$$\frac{\Box\Gamma \qquad \begin{array}{c}[\Gamma]\\ \vdots\\ \sigma\end{array}}{\Box\sigma}\,\Box K$$

which is neither an introduction nor an elimination rule and in which the same formula(s) appear in the premise twice, one boxed and once unboxed.

The situation is somehow better for S4, with reasonable sequent rules,

$$\frac{\Gamma, \tau \vdash \sigma}{\Gamma, \Box\tau \vdash \sigma}\,\Box \vdash \qquad \frac{\Box\Gamma \vdash \sigma}{\Box\Gamma \vdash \Box\sigma}\,\vdash \Box$$

but, once again, problematic natural deduction. The sequent rules appear strictly related to those for the universal quantifier, and following this analogy Prawitz [Pra65] attempted the definition of a natural deduction system styled after the first order system. This naive approach, however, does not work, and in order to obtain normalization, Prawitz was forced to introduce more elaborated concepts and rules (see Section 4.1.).

In the last few years, however, it has been discovered by several authors that the difficulty was in a too strict interpretation of the "Gentzen format" and that several extensions [Dos85, BM92, GdQ92, Mas92, Mas93] allow a good and "natural" proof theory for modal logics.

We will focus here on the proposal by the second author for the logic KD, whose main idea is a two-dimensional generalization of the notion of sequent. Instead of asserting provability ($\vdash$) between two sequences of formulas, provability is asserted between two-dimensional sequences of formulas.

Developed in [Mas92] as a sequent calculus for classical KD, in [Mas93] the approach is tailored to the intuitionistic framework, for which it is also given an equivalent *natural deduction system*.

The goal of the present paper is to study the computational properties of the system in [Mas93] and of several extensions to other logics, namely the positive fragments of K4, KT, and S4.

To this aim, we introduce first a complete natural deduction system for each of the logics at hand. All the rules of these systems are local (they act only on the conclusions of the deductions they are applied to), no introduction rule has a premise containing the introduced connective (as it is case for rule $\Box K$, for instance), and the modal rules strictly match the standard rules for an universal quantifier, the side conditions on variables becoming a side condition on levels.

One the main features of the approach is its *scalability,* the various logics differring only in one parameter of the elimination rule for $\Box$. This allows both a compact treatment and the study of the "fine structure" of the $\Box$ modality (that is, how several sublogics interact to obtain a larger logic, in this case S4).

By defining a suitable notion of reduction on the terms representing proofs (extending standard β-reduction for λ-terms), we obtain a natural computational interpretation for proofs, which is proved strongly normalizing and confluent.

Finally, this local, two dimensional approach enforces remarkable *global properties* of the resulting deductions. Though this is not the main subject of the paper, in Section 4.1. we will show that all deductions in our system for S4, in fact satisfy Prawitz' global requirements on proofs, thus giving an immediate forgetful translation of our system in Prawitz' one.

2. Systems

Before introducing formally the systems we will deal with, we briefly, and informally recall the natural deduction approach taken in [Mas93]. Let us denote formulas with lowercase greek letters $\alpha, \beta, \sigma, \ldots$, and sequences of formulas with lowercase gothic letters $\mathfrak{S}, \mathfrak{B}, \ldots$, while ε will be the empty sequence. An *intuitionistic 2-sequent* is a two dimensional expression of the form

$$\begin{array}{ccc} \mathfrak{S}_1 & & \varepsilon \\ \mathfrak{S}_2 & & \varepsilon \\ \vdots & \vdash & \vdots \\ \mathfrak{S}_k & & \sigma \end{array} \tag{1}$$

whose intended meaning is the formula

$$\bigwedge \mathfrak{S}_1 \supset \Box(\bigwedge \mathfrak{S}_2 \supset \ldots \Box(\bigwedge \mathfrak{S}_k \supset \sigma)\ldots).$$

Note that the formula σ, the *conclusion* of the deduction, lies at a *level*, k, which is greater than, or equal to, the level of any assumption it depends on (any of the $\mathfrak{S}_j$'s may be empty, of course). The propositional rules act over these two dimensional stuctures in the expected way, just "respecting the levels". The rules for $\supset$, for instance, can be expressed as:

$$\frac{\begin{array}{ccc} \mathfrak{S}_1 & & \varepsilon \\ \mathfrak{S}_2 & & \varepsilon \\ \vdots & \vdash & \vdots \\ \mathfrak{S}_k, \sigma & & \tau \end{array}}{\begin{array}{ccc} \mathfrak{S}_1 & & \varepsilon \\ \mathfrak{S}_2 & & \varepsilon \\ \vdots & \vdash & \vdots \\ \mathfrak{S}_k & & \sigma \supset \tau \end{array}} \supset\mathcal{I} \qquad \frac{\begin{array}{ccccc} \mathfrak{S}_1 & & \varepsilon & & \mathfrak{B}_1 & & \varepsilon \\ \mathfrak{S}_2 & & \varepsilon & & \mathfrak{B}_2 & & \varepsilon \\ \vdots & \vdash & \vdots & & \vdots & \vdash & \vdots \\ \mathfrak{S}_k & & \sigma \supset \tau & & \mathfrak{B}_k & & \sigma \end{array}}{\begin{array}{ccc} \mathfrak{S}_1, \mathfrak{B}_1 & & \varepsilon \\ \mathfrak{S}_2, \mathfrak{B}_2 & & \varepsilon \\ \vdots & \vdash & \vdots \\ \mathfrak{S}_k, \mathfrak{B}_k & & \tau \end{array}} \supset\mathcal{E}$$

Formulas may change their level only by means of modal rules:

$$\frac{\begin{array}{ccc}\mathfrak{S}_1 & & \varepsilon\\ \mathfrak{S}_2 & & \varepsilon\\ \vdots & \vdash & \vdots\\ \mathfrak{S}_k & & \varepsilon\\ \varepsilon & & \sigma\end{array}}{\begin{array}{ccc}\mathfrak{S}_1 & & \varepsilon\\ \mathfrak{S}_2 & & \varepsilon\\ \vdots & \vdash & \vdots\\ \mathfrak{S}_k & & \Box\sigma\end{array}}\ \Box\mathcal{I} \qquad \frac{\begin{array}{ccc}\mathfrak{S}_1 & & \varepsilon\\ \mathfrak{S}_2 & & \varepsilon\\ \vdots & \vdash & \vdots\\ \mathfrak{S}_k & & \Box\sigma\end{array}}{\begin{array}{ccc}\mathfrak{S}_1 & & \varepsilon\\ \mathfrak{S}_2 & & \varepsilon\\ \vdots & \vdash & \vdots\\ \mathfrak{S}_k & & \varepsilon\\ \varepsilon & & \sigma\end{array}}\ \Box\mathcal{E}$$

Thus, the only way to introduce a modality on a formula occurrence σ at level k is that σ is the only formula present at that level. As a result of the rule, the introduced formula is lifted one level up. Vice versa, the elimination rule pushes a formula down one level (but there is no restriction on its premise). The levels thus represent in the calculus a notion of modal dependence: the conclusion σ at level k modally depends on the assumptions at the same level. If there are not any such assumption, than we are allowed to assert the σ is necessary.

As proved in [Mas93], the given rules for $\Box$ characterize the minimal normal modal logic K.[1] In this paper we will extend this approach to a class of modal logics based on K, KT, $\mathsf{K4}$, $\mathsf{S4}$, focusing on the computational aspects of the resulting proofs.

Before going into the details of the systems, we adopt a more compact representation for 2-sequents. Instead of writing two-dimensional judgements, we will denote each formula σ at level k with σ^k and write the judgment (1) as $\Gamma \vdash \sigma^k$, where

$$\Gamma = \begin{array}{c}\mathfrak{S}_1\\ \mathfrak{S}_2\\ \vdots\\ \mathfrak{S}_k\end{array}$$

will be seen as a multiset $\{\tau_1^{i_1}, \ldots, \tau_n^{i_n}\}$. The usefulness of this representation will be especially clear in Section 5. The reader should always bear in mind, however, that the indexes on formulas are only a metatheoretical notation for two dimensional structures.

2.1. Basic definitions

Formally, formulas are built out of *atoms* (ranged over by p); compound formulas are obtained with the connectives: $\Box$ (unary), $\wedge$ and $\supset$ (binary). Any formula of the calculus will be marked with a *level index*, varying in $\mathbb{N}^+$; an indexed formula σ of level i will be written σ^i.

The following definition will introduce a calculus of *terms* and *formulas*, such that to any term M there will correspond a unique indexed formula σ^i, called *its type*; this fact will be denoted with $M : \sigma^i$. For any indexed formula σ^i we assume the existence of a numberable set $\{x_1^i, x_2^i, \ldots\}$ of variables of type σ^i. A *set of assumptions* (called sometimes also a *basis*, or a *context*) is a set $\Gamma = \{x_1^{i_1} : \sigma_1^{i_1}, \ldots, x_n^{i_n} : \sigma_n^{i_n}\}$, where all the variables are different: if $x^k : \sigma^k \in \Gamma$ and $x^h : \tau^h \in \Gamma$, then $\sigma^k = \tau^h$ (and in particular $k = h$). No variable name, hence, can appear in a set of assumptions with two different levels; we will refer to this as to the *level variable convention.* For such a set of assumptions Γ, define $\#\Gamma = \max\{k_j \mid x_k^{k_j} : \sigma_k^{k_j} \in \Gamma\}$; $\#\Gamma = 0$ when Γ is empty.

[1] More precisely, [Mas93] introduces a system for the minimal deontic normal modal logic KD, that in absence of negation and $\Diamond$ is equivalent to K.

Moreover, $\Gamma^{<i} = \{x^k : \sigma^k \in \Gamma \mid k < i\}$; the set $\Gamma^{\geq i}$ is defined analogously. Finally, for $n \in \mathbb{Z}$, $\Gamma_{(n)} = \{x^{k+n} : \sigma^{k+n} \mid x^k : \sigma^k \in \Gamma\}$.

DEFINITION 2.1. [Calculus λ^ℓ] *Terms* and *derivations* are inductively defined by the following rules.

$$x^k : \sigma^k$$

$$\frac{\begin{array}{cc}\Gamma & \Delta \\ \vdots & \vdots \\ M : \sigma^k & N : \tau^k\end{array}}{\langle M, N\rangle^k : \sigma \wedge \tau^k}\wedge\mathcal{I} \qquad \frac{\begin{array}{c}\Gamma \\ \vdots \\ M : \sigma \wedge \tau^k\end{array}}{(\mathsf{fst}\, M)^k : \sigma^k}\wedge\mathcal{E}_l \qquad \frac{\begin{array}{c}\Gamma \\ \vdots \\ M : \sigma \wedge \tau^k\end{array}}{(\mathsf{snd}\, M)^k : \tau^k}\wedge\mathcal{E}_r$$

$$\frac{\begin{array}{c}\Gamma \quad [x^k : \sigma^k] \\ \vdots \\ M : \tau^k\end{array}}{(\lambda x^k{:}\sigma^k.M)^k : \sigma \supset \tau^k}\supset\mathcal{I} \qquad \frac{\begin{array}{cc}\Gamma & \Delta \\ \vdots & \vdots \\ M : \sigma \supset \tau^k & N : \sigma^k\end{array}}{(MN)^k : \sigma^k}\supset\mathcal{E}$$

While we will always attach a level to a formula, in the exposition we will be more liberal for terms, writing both $M : \sigma^k$ and $M^k : \sigma^k$, since no confusion may arise in this way.

If S is one of the systems introduced below, we write $\Gamma \vdash_S M^i : \sigma^i$ when in S there is a derivation:

$$\begin{array}{c}\Gamma \\ \vdots \\ M^i : \sigma^i\end{array}$$

$\Gamma \vdash_S \sigma^i$ holds when there is a term M^i such that $\Gamma \vdash_S M^i : \sigma^i$.

2.2. SYSTEM $\lambda^\ell K$

The typed λ-calculus $\lambda^\ell K$ is obtained by adding to λ^ℓ the two rules already discussed in the introduction of this section:

$$\frac{\begin{array}{c}\Gamma \\ \vdots \\ M^j : \sigma^j\end{array}}{\mathsf{gen}(M^j)^{j-1} : \Box\sigma^{j-1}}\Box\mathcal{I}\quad {\scriptstyle \mathrm{j}>\#\Gamma} \qquad \frac{\begin{array}{c}\Gamma \\ \vdots \\ M^j : \Box\sigma^j\end{array}}{\mathsf{ungen}(M^j)^{j+1} : \sigma^{j+1}}\Box\mathcal{E}$$

The informal meaning of these rules is thus the following.

- $\Box\mathcal{I}$ If, from the hypotheses in Γ, we derive that σ holds at knowledge level j, and nothing else holds at any level greater than or equal to j, then $\Box\sigma$ has to hold at level $j-1$.
- $\Box\mathcal{E}$ If, from the hypothesis in Γ, we derive that $\Box\sigma$ holds true at knowledge level j, then σ has to be true at the next level.

Such an interpretation corresponds to the semantical property relative to the minimal normal modal logic K: System K is complete with respect to the set of Kripke frames whose accessibility relation is "irreflexive", "asymmetric" and "intransitive."

The characteristic axiom of K, $\Box(\alpha \supset \beta) \supset (\Box\alpha \supset \Box\beta)$, is derived in $\lambda^\ell K$ in the following way.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{x^1 : \Box\alpha^1}{\mathsf{ungen}(x^1)^2 : \alpha^2}\Box\mathcal{E} \qquad \dfrac{y^1 : \Box(\alpha \supset \beta)^1}{\mathsf{ungen}(y^1)^2 : \alpha \supset \beta^2}\Box\mathcal{E}}{(\mathsf{ungen}(y^1)^2\mathsf{ungen}(x^1)^2)^2 : \beta^2}\supset\mathcal{E}}{\mathsf{gen}((\mathsf{ungen}(y^1)^2\mathsf{ungen}(x^1)^2)^2)^1 : \Box\beta^1}\Box\mathcal{I}}{\lambda x^1 : \Box\alpha^1.\mathsf{gen}((\mathsf{ungen}(y^1)^2\mathsf{ungen}(x^1)^2)^2)^1 : \Box\alpha \supset \Box\beta^1}\supset\mathcal{I}}{\lambda y^1 : \Box(\alpha \supset \beta)^1.\lambda x^1 : \Box\alpha^1.\mathsf{gen}((\mathsf{ungen}(y^1)^2\mathsf{ungen}(x^1)^2)^2)^1 : \Box(\alpha \supset \beta) \supset (\Box\alpha \supset \Box\beta)^1}\supset\mathcal{I}$$

2.3. System $\lambda^\ell KT$

The typed λ-calculus $\lambda^\ell KT$ is obtained from $\lambda^\ell K$ by extending the elimination rule for $\Box$.

$$\dfrac{\begin{array}{c}\Gamma\\ \vdots\\ M^j : \Box\sigma^j\end{array}}{\mathsf{ungen}(M^j)^k : \sigma^k}\Box\mathcal{E}\quad {\scriptstyle \mathrm{k}\in\{\mathrm{j},\mathrm{j}+1\}}$$

The informal meaning of such a rule is thus:

> If, from the hypothesis in Γ, we derive that $\Box\sigma$ holds at knowledge level j, then σ has to hold at the next $(j+1)$ and at the current (j) level.

We have a correspondence with the semantical property of the Hilbert type formulation of KT: System KT is complete with respect to the set of Kripke frames where the accessibility relation is "reflexive", "asymmetric" and "intransitive."

By using the above rule we can prove the characteristic axiom of KT, $\Box\alpha \supset \alpha$.

$$\dfrac{\dfrac{x^1 : \Box\alpha^1}{\mathsf{ungen}(x^1)^1 : \alpha^1}\Box\mathcal{E}}{(\lambda x^1 : \Box\alpha^1.\mathsf{ungen}(x^1)^1)^1 : \Box\alpha \supset \alpha^1}\supset\mathcal{I}$$

2.4. System $\lambda^\ell K4$

The typed λ-calculus $\lambda^\ell K4$ is obtained from $\lambda^\ell K$ by extending the elimination rule for $\Box$.

$$\dfrac{\begin{array}{c}\Gamma\\ \vdots\\ M^j : \Box\sigma^j\end{array}}{\mathsf{ungen}(M^j)^k : \sigma^k}\Box\mathcal{E}\quad {\scriptstyle \mathrm{k}>\mathrm{j}}$$

The informal meaning of such a rule is:

> If, from the hypotheses in Γ, we derive that $\Box\sigma$ holds at knowledge level j, then σ has to hold at any level greater than j.

We have a correspondence with the following semantical property of the Hilbert type formulation of $\mathsf{K4}$: System KT is complete with respect to the set of frames with the accessibility relation "irreflexive", "asymmetric," and "transitive."

The characteristic $\mathsf{K4}$ axiom, $\Box\alpha \supset \Box\Box\alpha$, is proved in the following way.

$$\dfrac{\dfrac{\dfrac{\dfrac{x^1 : \Box\alpha^1}{\mathsf{ungen}(x^1)^3 : \alpha^3}\,\Box\mathcal{E}}{\mathsf{gen}(\mathsf{ungen}(x^1)^3)^2 : \Box\alpha^2}\,\Box\mathcal{I}}{\mathsf{gen}(\mathsf{gen}(\mathsf{ungen}(x^1)^3)^2)^1 : \Box\Box\alpha^1}\,\Box\mathcal{I}}{(\lambda x^1 : \Box\alpha^1.\mathsf{gen}(\mathsf{gen}(\mathsf{ungen}(x^1)^3)^2)^1)^1 : \Box\alpha \supset \Box\Box\alpha^1}\,\supset\mathcal{I}$$

2.5. System $\lambda^\ell S4$

The typed λ-calculus $\lambda^\ell S4$ is obtained from $\lambda^\ell K$ by allowing both the $\lambda^\ell KT$ and the $\lambda^\ell K4$ $\Box$ elimination rules.

$$\dfrac{\begin{array}{c}\Gamma\\ \vdots\\ M^j : \Box\sigma^j\end{array}}{\mathsf{ungen}(M^j)^k : \sigma^k}\,\Box\mathcal{E}\quad {\scriptstyle \mathrm{k}\geq\mathrm{j}}$$

The informal meaning of such a rule is:

> If, from the hypotheses in Γ, we derive that $\Box\sigma$ holds at knowledge level j, then σ has to hold at each level greater than or equal to j.

We have a correspondence with the following semantical property of the Hilbert type formulation of $\mathsf{S4}$: System $\mathsf{S4}$ is complete with respect to the set of Kripke frames whose accessibility relation is "reflexive", "asymmetric," and "transitive."

Since the characteristic axioms of $\mathsf{S4}$ are those of K, KT, and $\mathsf{K4}$, they can be proved in $\lambda^\ell S4$.

2.6. Implicitly typed λ-calculi

The implicitly typed λ-calculi $\lambda^* K$, $\lambda^* KT$, $\lambda^* K4$, and $\lambda^* S4$ are obtained from the previously defined calculi, by erasing from terms the level and type decorations. We loose a 1-to-1 correspondence between proofs and terms, but we gain in readability. The proof terms corresponding to the characteristic axioms of the various logic in the implicit form are the following.

$\vdash_{\lambda^* K} \lambda y.\lambda x.\mathsf{gen}(\mathsf{ungen}(y)\mathsf{ungen}(x)) : \Box(\alpha \supset \beta) \supset (\Box\alpha \supset \Box\beta)^1$

$\vdash_{\lambda^* KT} \lambda x.\mathsf{ungen}(x) : \Box\alpha \supset \alpha^1$

$\vdash_{\lambda^* K4} \lambda x.\mathsf{gen}(\mathsf{gen}(\mathsf{ungen}(x))) : \Box\alpha \supset \Box\Box\alpha^1$

3. Hilbert style systems, a comparison

In this section we show that provability in the calculi $\lambda^\ell K$, $\lambda^\ell KT$, $\lambda^\ell K4$, and $\lambda^\ell S4$ is equivalent to provability in the positive fragment of the Hilbert style modal logics K, KT, $\mathsf{K4}$, and $\mathsf{S4}$. Let L be the positive fragment of one of the logics in $\{\mathsf{K}, \mathsf{KT}, \mathsf{K4}, \mathsf{S4}\}$.

For the purpose of this section, we omit the term labelling for the derivations in the calculus; moreover, if $\Gamma = \{\sigma_1^i, \ldots, \sigma_n^i\}$, then $\Gamma^\flat = \{\sigma_1, \ldots, \sigma_n\}$.

Theorem 3.1.

$$\vdash_L \sigma \quad \Longleftrightarrow \quad \vdash_{\lambda^\ell L} \sigma^1$$

The proof of this fact breaks down into the following lemmas.

LEMMA 3.2. $\vdash_L \sigma \implies \vdash_{\lambda^\ell L} \sigma^1$.

Proof. By induction on the lenght of the derivation. Propositional axioms and modus ponens are trivial. The proof in $\lambda^\ell L$ of the modal axioms of L has been given in the previous section. For the inference rule (Gen), suppose we proved $\vdash_L \sigma$. By induction hypothesis we have $\vdash_{\lambda^\ell L} \sigma^1$. Replacing now any index level k in this deduction with $k+1$, we obtain a deduction of $\vdash_{\lambda^\ell L} \sigma^2$. An application of $\Box\mathcal{I}$ gives $\vdash_{\lambda^\ell L} \Box\sigma^1$. ∎

The following "translation function" corresponds to the intended meaning of our judgments.

DEFINITION 3.3.

- $\mathfrak{T}[\Gamma \vdash \alpha^1] = \bigwedge \Gamma^\flat \supset \alpha$
- $\mathfrak{T}[\Gamma \vdash \alpha^{j+1}] = \bigwedge(\Gamma^{<2})^\flat \supset \Box(\mathfrak{T}[\Gamma^{\geq 2}{}_{(-1)} \vdash \alpha^j])$

where, $\bigwedge \varnothing = \top$ (any tautology).

LEMMA 3.4. $\Gamma \vdash_{\lambda^\ell L} \alpha^j \implies \vdash_L \mathfrak{T}[\Gamma \vdash \alpha^j]$.

Proof. By trivial, and long, induction on the deduction $\Gamma \vdash_{\lambda^\ell L} \alpha^j$. ∎

4. INTERMEZZO

4.1. ON THE GEOMETRY OF PROOFS

One of the most interesting properties of the system we have proposed (or better of the level machinery), is the geometry it enforces on its deductions. In particular, we show in this section that all (not necessary normal) deductions involving a $\Box\mathcal{I}$ have a very remarkable global structure.

Before showing the technical fact we have in mind, however, we recall a different natural deduction system for S4, namely the "third version" of the calculus discussed in Prawitz' classical monograph [Pra65, Chapter VI, pag. 79]. The propositional rules of that system can be obtained from those of Definition 2.1 by simply erasing the level indexes (thus obtaining the usual rules for intuitionistic propositional logic). As for the rules for $\Box$, the elimination is the same as ours with the omission of levels, while the introduction rule (which we will call $\Box\mathcal{I}_\mathcal{P}$) is rather elaborate, in order to ensure normalization and the subformula property. An application of $\Box\mathcal{I}_\mathcal{P}$ has the form:

$$\dfrac{\begin{array}{ccc}\mathcal{D}_1 & & \mathcal{D}_n \\ [\Box\tau_1 & \dots & \Box\tau_n]\end{array}}{\begin{array}{c}\mathcal{D} \\ \sigma \\ \hline \Box\sigma\end{array}\ \Box\mathcal{I}_\mathcal{P}}$$

where $\Box\tau_1, \dots, \Box\tau_n$ are all the open assumptions of $\mathcal{D}$, and no open assumption in the deductions $\mathcal{D}_i$ (of conclusion τ_i) is bound in $\mathcal{D}$.[2] In other words, an application of $\Box\mathcal{I}_\mathcal{P}$ is obtained by taking a deduction

$$\begin{array}{ccc}\Box\tau_1 & \dots & \Box\tau_n \\ & \mathcal{D} & \\ & \sigma & \end{array}$$

[2]Prawitz' original definition is formulated via the concept of *essentially modal formula*. It is not difficult to see that our formulation of $\Box\mathcal{I}_\mathcal{P}$, though not equivalent (it allows less deductions), it is still complete for the $\wedge, \supset, \Box$ fragment.

where *all* open assumptions (if any) are boxed, and plugging into these assumptions arbitrary derivations with the right conclusion. Rule $\Box\mathcal{I}_{\mathcal{P}}$ is far from being "natural": it allows normalization, but at the price of a globally stated constraint on its application.

Coming back to our system, we can show that all applications of $\Box\mathcal{I}$, in fact, comply with Prawitz' requirement. In order to give a clearer picture of the involved deductions we will dispense from terms.

THEOREM 4.1. *Let $\mathcal{E}$ be a deduction of $\Gamma \vdash_{\lambda^\ell S4} \sigma^k$, with $k > \#\Gamma$. Then $\mathcal{E}$ has the form*

$$\begin{array}{ccc} \Gamma_1 & & \Gamma_n \\ \mathcal{D}_1 & & \mathcal{D}_n \\ [\Box\tau_1^{h_1} & \dots & \Box\tau_n^{h_n}] \\ & \mathcal{D} & \\ & \sigma^k & \end{array}$$

where: (i) any Γ_j is non empty; (ii) the union of the Γ_j's is Γ; (iii) any $\mathcal{D}_j$ is a deduction of $\Gamma_j \vdash_{\lambda^\ell S4} \Box\tau_j^{h_j}$; (iv) $\mathcal{D}$ is a deduction of $\Box\tau_1^{h_1}, \dots, \Box\tau_n^{h_n} \vdash_{\lambda^\ell S4} \sigma^k$; (v) for any j, $h_j < k$.

Proof. If Γ is empty, then the statement is vacuous ($n = 0$ and $\mathcal{D} = \mathcal{E}$). Otherwise, the following informal algorithm will produce the required data.

Let r be any path in $\mathcal{E}$ from the conclusion σ^k to an occurrence of an open assumption $\rho \in \Gamma$. In r there must be an application of $\Box\mathcal{E}$, since $k > \#\Gamma$ and $\Box\mathcal{E}$ is the only rule allowing its conclusion to be at a higher level of its premise. Pick the first application (starting from the conclusion up) of $\Box\mathcal{E}$ in which the level h of the premise (say, $\Box\tau^h$) is strictly less than k. We choose this $\Box\tau^h$ as $\tau_1^{h_1}$; $\mathcal{D}_1$ is the subtree of $\mathcal{E}$ rooted at $\Box\tau^h$; Γ_1 is the set of all open assumptions of the deduction $\mathcal{D}_1$ with conclusion $\Box\tau^h$. Clearly $\rho \in \Gamma_1$, thus establishing (i) and (iii) for $j = 1$; in order to eventually establish (iv), we have to guarantee that no assumption in Γ_1 can be discharged below $\Box\tau^h$. However, this is obvious, because any formula appearing in the path r below $\Box\tau^h$ have a level $l > h$ (by construction), while $\#\Gamma_1 \leq h$, by Proposition 5.1, thus forbidding the application of a $\supset\mathcal{E}$ at level l below $\Box\tau^h$.

The previous procedure can be repeated until there are no more occurrences of assumptions in Γ not already allocated to some Γ_i.

When the algorithm terminates, (ii) is obvious, and (iv) follows by construction. ∎

Writing $\vdash_{\mathcal{P}}$ for provability in Prawitz' system and denoting with $(\quad)^\flat$ the obvious function stripping the level indexes out of a formula (deduction, etc.), the following is straightforward.

COROLLARY 4.2. *If $\mathcal{D}$ is a deduction of $\Gamma \vdash_{\lambda^\ell S4} \sigma^k$, then $\mathcal{D}^\flat$ is a deduction of $\Gamma^\flat \vdash_{\mathcal{P}} \sigma$.*

Not any proof in $\vdash_{\mathcal{P}}$ can be decorated with levels to become a proof in our system, as the following deduction shows:

$$\dfrac{\Box\sigma}{\Box\Box\sigma}\,\Box\mathcal{I}_{\mathcal{P}}$$

Proofs in our system, however, are still enough for completeness and, moreover, seem to have a more direct interpretation as travelling in a Kripke model (cfr. [BM92]).

Many consequences can be drawn from Corollary 4.2. Since any reduction step in our system becomes also a reduction step in $\vdash_{\mathcal{P}}$ under the $(\quad)^\flat$ translation, we immediately obtain normalization for $\lambda^\ell S4$ from the normalization theorem for $\vdash_{\mathcal{P}}$. We will give a different proof of *strong normalization* for $\lambda^\ell S4$, in Section 6.2..

Moreover, by adding to the usual clauses that, for any k, σ^k has to considered a subformula of σ^h, we also obtain the following *subformula property.*

THEOREM 4.3 (Subformula principle) *Any formula occurring in a normal deduction of* $\Gamma \vdash_{\lambda^\ell S4} \sigma^k$ *is a subformula of* σ^k *or of some formula in* Γ.

Proof. (Sketch) It is enough to prove the theorem for $\vdash_{\mathcal{P}}$, which can be obtained in the same way as the corresponding result for intuitionistic logic [Pra65, Theorem 2, pag. 53; cfr pag. 80]. ■

Starting from a purely structural extension of the syntax (the levels) and adopting only local rules (in particular, $\Box\mathcal{I}$ as opposed to $\Box\mathcal{I}_{\mathcal{P}}$) we have recovered the global, elaborated constraint on the *geometry* of the deductions that other systems are forced to require from the beginning.

4.2. A PROOF THEORETICAL REQUEST... FULFILLED

One of the principal features of a good modal proof theory is its capability to suit a class of different modal logics without changing the way modal connectives are manipulated (e.g. introduced and eliminated). The differentiation between logics is instead delegated to the way (general) formulas are manipulated.

A clear discussion on this topics (in the case of modal systems) may be found in recent work of Wansing [Wan93] and Došen [Dos85]. This point of view (that [Wan93] calls *Došen principle*, but that should be traced back to Gentzen, for the differentiation of intuitionistic from classical logic) may be stated as:

> The rules for the logical operations are never changed: all changes are made in the structural rules. [Dos85]

At first look our calculi violate this principle: different systems are obtained with different elimination rules.

One could attempt a "weak" defense, arguing that all the proposed elimination rules are equal in "spirit", since they differ only in level decorations. But this would miss the point. Indeed, we totally agree with Došen principle and we claim that our approach does not violate it... when observed in the right context. The distinction between logical and structural rules, in fact, is only relevant in *sequent* calculi, and it is thus there that the challenge posed by Došen principle has to be attacked. The natural deduction system $\lambda^\ell K$ has an associated *2-sequent* calculus (see [Mas93]), whose left and right $\Box$ introduction rules are the following:

$$\frac{\begin{array}{cc}\mathfrak{S}_1 & \varepsilon\\ \mathfrak{S}_2 & \varepsilon\\ \vdots & \vdots\\ \mathfrak{S}_{k-1} & \varepsilon\\ \mathfrak{S}_k,\sigma & \tau\end{array}}{\begin{array}{cc}\mathfrak{S}_1 & \varepsilon\\ \mathfrak{S}_2 & \varepsilon\\ \vdots & \vdots\\ \mathfrak{S}_{k-1},\Box\sigma & \varepsilon\\ \mathfrak{S}_k & \tau\end{array}}\,\Box\vdash \qquad \frac{\begin{array}{cc}\mathfrak{S}_1 & \varepsilon\\ \mathfrak{S}_2 & \varepsilon\\ \vdots & \vdots\\ \mathfrak{S}_k & \varepsilon\\ \varepsilon & \sigma\end{array}}{\begin{array}{cc}\mathfrak{S}_1 & \varepsilon\\ \mathfrak{S}_2 & \varepsilon\\ \vdots & \vdots\\ \mathfrak{S}_k & \Box\sigma\end{array}}\,\vdash\Box$$

Sequent calculi for KT and $\mathsf{K4}$ are now obtained by adding the *structural rules* (on levels) $\vdash{\uparrow}_{(KT)}$ and $\vdash{\downarrow}_{(T4)}$, respectively:

$$\dfrac{\begin{array}{ccc}\mathfrak{S}_1 & & \varepsilon\\ \mathfrak{S}_2 & & \varepsilon\\ \vdots & \vdash & \vdots\\ \mathfrak{S}_k & & \varepsilon\\ \varepsilon & & \sigma\end{array}}{\begin{array}{ccc}\mathfrak{S}_1 & & \varepsilon\\ \mathfrak{S}_2 & & \varepsilon\\ \vdots & \vdash & \vdots\\ \mathfrak{S}_k & & \sigma\end{array}}\vdash\!\uparrow_{(KT)} \qquad \dfrac{\begin{array}{ccc}\mathfrak{S}_1 & & \varepsilon\\ \mathfrak{S}_2 & & \varepsilon\\ \vdots & \vdash & \vdots\\ \mathfrak{S}_k & & \varepsilon\\ \varepsilon & & \sigma\end{array}}{\begin{array}{ccc}\mathfrak{S}_1 & & \varepsilon\\ \mathfrak{S}_2 & & \varepsilon\\ \vdots & \vdash & \vdots\\ \mathfrak{S}_k & & \varepsilon\\ \varepsilon^n & & \varepsilon^n\\ \varepsilon & & \sigma\end{array}}\vdash\!\downarrow_{(K4)}$$

where $n \geq 1$ and

$$\varepsilon^n = \left.\begin{array}{c}\varepsilon\\ \vdots\\ \varepsilon\end{array}\right\} n \text{ times}$$

The calculus for S4 is obtained by adding to the basic logical rules both $\vdash\!\uparrow_{(KT)}$ and $\vdash\!\downarrow_{(T4)}$. Thus, in a sequent setting, the four systems *are* obtained by means of structural rules.

The structural rules of sequent calculi, on the other hand, should not be explicit in the corresponding natural deduction formulation. Intuitionistic contractions and weakenings, for instance, are realized by the convention on the discharging (meta-) operation. This is why our calculi do not contain rules like

$$\dfrac{\begin{array}{c}\Gamma\\ \vdots\\ \sigma^r\end{array}}{\sigma^j}$$

Following the traditional natural deduction approach, such rules have been embedded into the (logical) $\Box\mathcal{E}$ rules.

5. Working with $\lambda^\ell S4$ proofs

In this section $\vdash$ will stand for $\vdash_{\lambda^\ell S4}$, whose rules are recalled in Figure 1.

Proposition 5.1. *Let* $\Gamma \vdash M^i : \sigma^i$. *Then* $i \geq \#\Gamma$.

Proof. Inspection of the rules. ∎

Definition 5.2. A derivation $\Gamma \vdash M^i : \sigma^i$ is *concluded* if $i = 1$ and $\#\Gamma \leq 1$.

Theorem 5.3. *Any non concluded derivation can be extended to a concluded one.*

Proof. Given a non concluded $\Gamma \vdash \sigma^k$, first replace any $\sigma^h \in \Gamma$ with:

$$\dfrac{\Box\sigma^1}{\sigma^h}\,\Box\mathcal{E}$$

At this point apply $k-1$ times the rule $\Box\mathcal{I}$ to the conclusion, obtaining a formula of level 1. ∎

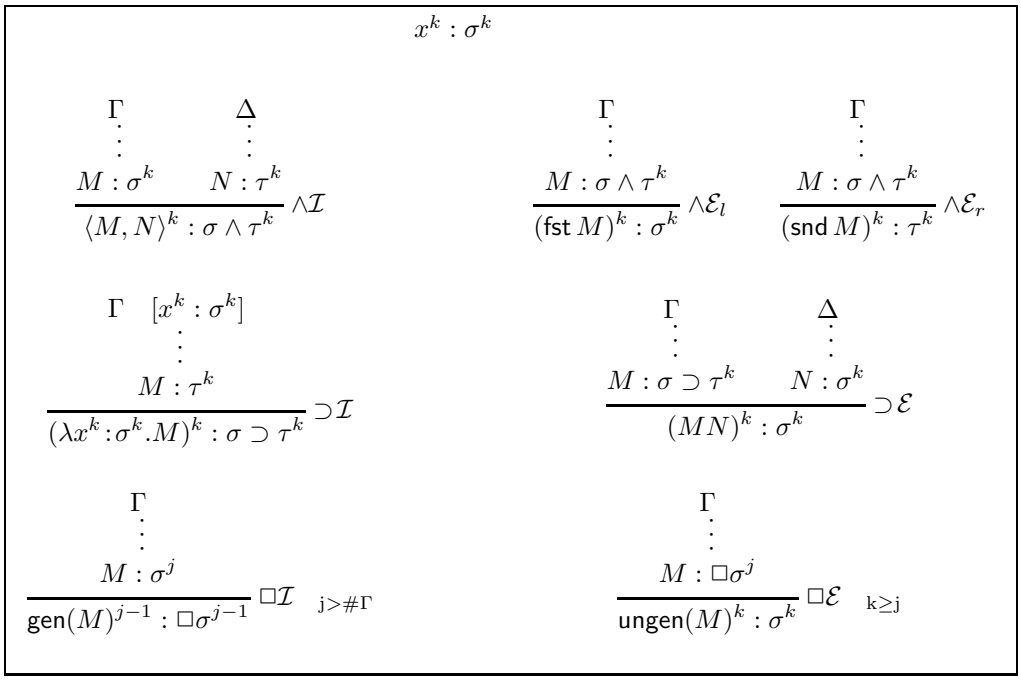


Figure 1: Rules for $\lambda^\ell S4$

The following technical lemmas aim to show, given a deduction for $\Gamma \vdash \sigma^k$, how to obtain a deduction for the same conclusion at a different level, possibly changing also some of the levels in Γ. We will see in Section 6. that this operation is essential for the computational interpretation of proofs.

At first sight the operations on proof trees given in this section may appear heavy and difficult to grasp. Notice, however, that the problem we tackle is essentially the same as the one arising in the first order natural deduction system NJ, when, given a deduction for $\Gamma \vdash \sigma(x)$ and a term t, we want to obtain a deduction for $\Gamma' \vdash \sigma(t)$. Many texts say, in this case, that all it is needed is the uniform substitution of t for x in the proof tree. A careful analysis of the process involved, however, shows that care must be taken in performing this operation; in particular, it is needed a strong discipline in the use of variables. A very clear account of the issues involved is given in [TvD88, Volume II, Ch. 10]. Levels in $\lambda^\ell S4$ play a very similar role to variables of NJ; the following lemmas can then be seen as expressing concepts like "renaming," "term substitution" and their properties.

LEMMA 5.4. *Let* $k > 0$. $\Gamma \vdash \alpha^j \quad \Longrightarrow \quad \forall i \leq j \quad \Gamma^{<i}, \Gamma^{\geq i}{}_{(+k)} \vdash \alpha^{j+k}$

Proof.

- $\alpha^j \vdash \alpha^j \Rightarrow \alpha^j \in \Gamma^{\geq i}{}_{(+k)}$ then $\alpha^{j+k} \vdash \alpha^{j+k}$
- if $\dfrac{\begin{array}{c}\Gamma, \alpha^j \\ \vdots \\ \beta^j\end{array}}{\alpha \supset \beta^j}$ then $\mathit{I.H.}\left\{\dfrac{\begin{array}{c}\Gamma^{<i}, \Gamma^{\geq i}{}_{(+k)}, \alpha^{j+k} \\ \vdots \\ \beta^{j+k}\end{array}}{\alpha \supset \beta^{j+k}}\right.$
- if $\dfrac{\begin{array}{c}\Gamma \\ \vdots \\ \alpha^j\end{array}}{\Box\alpha^{j-1}}$ then $\mathit{I.H.}\left\{\dfrac{\begin{array}{c}\Gamma^{<i}, \Gamma^{\geq i}{}_{(+k)} \\ \vdots \\ \alpha^{j+k}\end{array}}{\Box\alpha^{j-1+k}}\right.$

- if $\dfrac{\begin{array}{c}\Gamma\\ \vdots\\ \Box\alpha^j\end{array}}{\alpha^r}$ we have two subcases:

  $(i \leq j)$ in this case we have:

  $$I.H. \left\{ \begin{array}{c} \Gamma^{<i}, \Gamma^{\geq i}{}_{(+k)} \\ \vdots \\ \Box\alpha^{j+k} \end{array} \right. \Rightarrow \frac{\Box\alpha^{j+k}}{\alpha^{r+k}}$$

  $(j < i \leq r)$ in this case, without applying induction hypothesis and noting that $\Gamma^{\geq i} = \varnothing$ by Proposition 5.1, we have:

  $$\dfrac{\begin{array}{c}\Gamma^{<i}, \Gamma^{\geq i}{}_{(+k)}\\ \vdots\\ \Box\alpha^j\end{array}}{\alpha^{r+k}}$$

■

LEMMA 5.5. *Let* $j \leq 2$. $\Gamma \vdash \alpha^j \implies \forall i\, (2 \leq i \leq j)\ \Gamma^{<i}, \Gamma^{\geq i}{}_{(-1)} \vdash \alpha^{j-1}$

Proof.

- $\alpha^j \vdash \alpha^j \Rightarrow \alpha^{j-1} \in \Gamma^{\geq i}{}_{(-1)}$ then $\alpha^{j-1} \vdash \alpha^{j-1}$
- if $\dfrac{\begin{array}{c}\Gamma, \alpha^j\\ \vdots\\ \beta^j\end{array}}{\alpha \supset \beta^j}$ then $I.H. \left\{ \begin{array}{c} \Gamma^{<i}, \Gamma^{\geq i}{}_{(-1)}, \alpha^{j-1} \\ \vdots \\ \beta^{j-1} \end{array} \right. \Rightarrow \dfrac{\beta^{j-1}}{\alpha \supset \beta^{j-1}}$
- if $\dfrac{\begin{array}{c}\Gamma\\ \vdots\\ \alpha^j\end{array}}{\Box\alpha^{j-1}}$ then $I.H. \left\{ \begin{array}{c} \Gamma^{<i}, \Gamma^{\geq i}{}_{(-1)} \\ \vdots \\ \alpha^{j-1} \end{array} \right. \Rightarrow \dfrac{\alpha^{j-1}}{\Box\alpha^{j-2}}$
- if $\dfrac{\begin{array}{c}\Gamma\\ \vdots\\ \Box\alpha^j\end{array}}{\alpha^r}$ we have two subcases:

  $(j \geq 2, i \leq j)$ in this case we have:

  $$I.H. \left\{ \begin{array}{c} \Gamma^{<i}, \Gamma^{\geq i}{}_{(-1)} \\ \vdots \\ \Box\alpha^{j-1} \end{array} \right. \Rightarrow \frac{\Box\alpha^{j-1}}{\alpha^{r-1}}$$

  $(j < i \leq r)$ in this case, without applying induction hypothesis and noting that $\Gamma^{\geq i} = \varnothing$ by Proposition 5.1, we have:

$$\dfrac{\begin{array}{c}\Gamma^{<i}, \Gamma^{\geq i}{}_{(+k)} \\ \vdots \\ \Box\alpha^{j}\end{array}}{\alpha^{r-1}}$$

■

The operations on deductions given in the proof of the two previous lemmas is explicitated on proof terms by the following definition.

Definition 5.6. [Level substitution]
Let $\Gamma \vdash M : \sigma^v$ and $i \geq 1$; let $n \in \{-1\} \cup \mathbb{N}$ if $v \geq 2$, and $n \in \mathbb{N}$ otherwise. We inductively define the level substitution $[n]_i M$ (read: increment by n any levels greater than or equal to i).
If $v < i$:

$$[n]_i M^v = M^v$$

If $v \geq i$:

$$[n]_i x^v = x^{v+n}$$
$$[n]_i \langle M, N\rangle^v = \langle [n]_i M, [n]_i N\rangle^{v+n}$$
$$[n]_i (\mathsf{fst}\, M)^v = (\mathsf{fst}\, [n]_i M)^{v+n}$$
$$[n]_i (\mathsf{snd}\, M)^v = (\mathsf{snd}\, [n]_i M)^{v+n}$$
$$[n]_i (\lambda x^v : \sigma^v . M)^v = (\lambda x^{v+n} : \sigma^{v+n} . [n]_i M)^{v+n}$$
$$[n]_i (MN)^v = ([n]_i M\, [n]_i N)^{v+n}$$
$$[n]_i \mathsf{gen}(M)^v = \mathsf{gen}([n]_i M)^{v+n}$$
$$[n]_i \mathsf{ungen}(M)^v = \mathsf{ungen}([n]_i M)^{v+n}$$

Whenever we write a level substitution $[n]_i M$, we assume that all the constraints of the definition are satisfied (in particular those on n). Note that $[0]_i M^v = M^v$.

Lemmas 5.4 and 5.5 can then be reformulated as follows.

Lemma 5.7. $\Gamma \vdash M : \alpha^j \quad \Longrightarrow \quad \forall i \leq j, \quad \Gamma^{<i}, \Gamma^{\geq i}{}_{(+k)} \vdash [+k]_i M : \alpha^{j+k}$

Lemma 5.8. *Let $j \geq 2$, then:*
$\Gamma \vdash M : \alpha^j \quad \Longrightarrow \quad \forall i, 2 \leq i \leq j, \quad \Gamma^{<i}, \Gamma^{\geq i}{}_{(-1)} \vdash [-1]_i M : \alpha^{j-1}$

We can picture the effect of the level substitution on proof trees as follows. It is not difficult to extend Theorem 4.1 to the following more general fact.

Theorem 5.9. *Let $\mathcal{E}$ be a deduction of $\Gamma \vdash \sigma^k$, and let $i \leq k$. Then $\mathcal{E}$ has the form*

$$\dfrac{\begin{array}{cccc}\Gamma_1^{<i} & & \Gamma_n^{<i} & \\ \mathcal{D}_1 & & \mathcal{D}_n & \\ [\Box\tau_1^{h_1} & \ldots & \Box\tau_n^{h_n}] & \Gamma^{\geq i}\end{array}}{\begin{array}{c}\mathcal{D} \\ \sigma^k\end{array}}$$

where: (i) any $\Gamma_j^{<i}$ is non empty; (ii) the union of the $\Gamma_j^{<i}$'s is $\Gamma^{<i}$; (iii) any $\mathcal{D}_j$ is a deduction of $\Gamma_j^{<i} \vdash \Box\tau_j^{h_j}$; (iv) $\mathcal{D}$ is a deduction of $\Box\tau_1^{h_1}, \ldots, \Box\tau_n^{h_n}, \Gamma^{\geq i} \vdash \sigma^k$; (v) for any j, $h_j < i$.

Proof. A simple variant of the proof of Theorem 4.1, or, for the reader preferring recursion to iteration, by a routine induction on the lenght of $\mathcal{E}$, similarly to Lemmas 5.4 and 5.5. ■

In the same hypotheses of the theorem, now, the deduction $[m]_i\mathcal{E}$ is the following

$$\dfrac{\begin{array}{cccc}\Gamma_1^{<i} & & \Gamma_n^{<i} & \\ \mathcal{D}_1 & & \mathcal{D}_n & \\ [\Box\tau_1^{h_1} & \dots & \Box\tau_n^{h_n}] & \Gamma^{\geq i}{}_{(m)}\end{array}}{\dfrac{[m]_i\mathcal{D}}{\sigma^k}}$$

where *all* formulas appearing in $\mathcal{D}$ are affected by the level modification, while all the $\mathcal{D}_j$'s deductions are left unchanged.

Next lemma shows how level substitution interact with term substitution.

LEMMA 5.10. $([n]_iM)[[n]_iN/x^{k+n}] = [n]_i(M[N/x^k])$

Proof. Just note that if $x^k \in FV(M)$ then any subterm of M containing x^k has a level $h \geq k$. If $x^k \notin FV(M)$ then the variable-level-convention ensures the thesis. ∎

We show, next, a property of nested level substitutions.

LEMMA 5.11 (Level substitution lemma) *Let $k \geq 1$, $n \geq -1$, and $j \geq 0$.*

(i) If $i \leq k-1$, then for any $l \geq k$, $[n]_i[j-1]_kM^l = [j-1]_{k+n}[n]_iM^l$.

(ii) If $k-1 < i \leq k-1+j$, then for any $l \geq k$, $[n]_i[j-1]_kM^l = [j-1+n]_kM^l$.

Proof. By induction on M^l. The base case and all the propositional cases are straigthforward. We give only the modal cases.
(i)

$M^l = \mathsf{ungen}(N^v)^l$: $[j-1]_{k+n}[n]_i\mathsf{ungen}(N^v)^l = \mathsf{ungen}([j-1]_{k+n}[n]_iN^v)^{l+n+j-1}$, and
$[n]_i[j-1]_k\mathsf{ungen}(N^v)^l = \mathsf{ungen}([n]_i[j-1]_kN^v)^{l+n+j-1}$.
If $v \geq k$, we apply the induction hypothesis.
If $i \leq v < k$, $[j-1]_{k+n}[n]_iN^v = [n]_iN^v = [n]_i[j-1]_kN^v$.
If $v < i \leq k-1$, $[j-1]_{k+n}[n]_iN^v = N^v = [n]_i[j-1]_kN^v$.

$M^l = \mathsf{gen}(N^{l+1})^l$: $[j-1]_{k+n}[n]_i\mathsf{gen}(N^{l+1})^l = \mathsf{gen}([j-1]_{k+n}[n]_iN^{l+1})^{l+n+j-1}$, and
$[n]_i[j-1]_k\mathsf{gen}(N^{l+1})^l = \mathsf{gen}([n]_i[j-1]_kN^{l+1})^{l+n+j-1}$.
Conclude by induction hypothesis.

(ii)

$M^l = \mathsf{ungen}(N^v)^l$: $[j-1+n]_k\mathsf{ungen}(N^v)^l = \mathsf{ungen}([j-1+n]_kN^v)^{l+j-1+n}$, and
$[n]_i[j-1]_k\mathsf{ungen}(N^v)^l = \mathsf{ungen}([n]_i[j-1]_kN^v)^{l+j-1+n}$.
If $v \geq k$, conclude by the induction hypothesis.
If $v < k$, $[j-1+n]_kN^v = N^v = [n]_i[j-1]_kN^v$.

$M^l = \mathsf{gen}(N^{l+1})^l$: $[j-1+n]_k\mathsf{gen}(N^{l+1})^l = \mathsf{gen}([j-1+n]_kN^{l+1})^{l+j-1+n}$, and
$[n]_i[j-1]_k\mathsf{gen}N^{l+1})^l = \mathsf{gen}([n]_i[j-1]_kN^{l+1})^{l+j-1+n}$.
Conclude by the induction hypothesis.

∎

6. Computations

In the previous section a class of modal typed λ-calculi has been introduced. It is now necessary to study their computational behavior, by introducing suitable notions of reduction extending the usual typed β-reduction and corresponding to the process of proof normalization. We will be able to show that this reduction is *confluent* (or Church-Rosser) and *strongly normalizing* (or nötherian).

Definition 6.1. [Contraction]

$$((\lambda x^j{:}\sigma^j.M^j)^j N^j)^j \rhd [N^j/x^j]M^j$$

$$(\mathsf{fst}\,\langle M^j, N^j\rangle^j)^j \rhd M^j$$

$$(\mathsf{snd}\,\langle M^j, N^j\rangle^j)^j \rhd N^j$$

$$\mathsf{ungen}(\mathsf{gen}(M^k)^{k-1})^{k-1+j} \rhd [j-1]_k M^k \text{ (for } j \in \mathbb{N}).$$

The compatible closure of $\rhd$ (or *one-step reduction*) is denoted with $\to$; its transitive closure is $\overset{+}{\to}$, while $\twoheadrightarrow$ (the *reduction relation*) is the transitive and reflexive closure.

The following theorem expresses the correctness of Definition 6.1 with respect to types.

Theorem 6.2. *If $\Gamma \vdash M^j : \sigma^j$ and $M^j \twoheadrightarrow N^j$, then $\Gamma \vdash N^j : \sigma^j$.*

Proof. The only non standard case is when the reduction is a modal contraction. From $M = \mathsf{ungen}(\mathsf{gen}(P^k)^{k-1})^{k-1+j}$ we have $\Gamma \vdash P^k : \Box\sigma^k$ and $k > \#\Gamma$. The level substitution in $[j-1]_k P^k$, then, does not affect the free variables of P and Lemmas 5.7 and 5.8 give the thesis. ∎

Reduction and level substitution match well: the former is preserved by the latter, as the following results will show.

Lemma 6.3. *If $M^h \rhd N^h$, then for any $i \le h$ and any n, $[n]_i M^h \rhd [n]_i N^h$.*

Proof. By cases on the definition of contraction. We give only the modal case. Suppose that, for $j \in \mathbb{N}$,

$$\mathsf{ungen}(\mathsf{gen}(M^k)^{k-1})^{k-1+j} \rhd [j-1]_k M^k$$

and we have to prove, for any $i \le k-1+j$, that

$$[n]_i\mathsf{ungen}(\mathsf{gen}(M^k)^{k-1})^{k-1+j} \rhd [n]_i[j-1]_k M^k.$$

We distinguish two cases. If $i \le k-1$:

$$\begin{array}{rcl} [n]_i\mathsf{ungen}(\mathsf{gen}(M^k)^{k-1})^{k-1+j} & = & \mathsf{ungen}(\mathsf{gen}([n]_i M^k)^{k-1+n})^{k-1+j+n} \\ & \rhd & [j-1]_{k+n}[n]_i M^k \\ & = & [n]_i[j-1]_k M^k \quad \text{by Lemma 5.11(i)} \end{array}$$

Otherwise, when $i > k-1$:

$$\begin{array}{rcl} [n]_i\mathsf{ungen}(\mathsf{gen}(M^k)^{k-1})^{k-1+j} & = & \mathsf{ungen}(\mathsf{gen}(M^k)^{k-1})^{k-1+j+n} \\ & \rhd & [j-1+n]_k M^k \\ & = & [n]_i[j-1]_k M^k \quad \text{by Lemma 5.11(ii)} \end{array}$$

∎

LEMMA 6.4. *If $M^h \to N^h$ then for any $i \leq h$ and any n, $[n]_i M^h \to [n]_i N^h$.*

Proof. By induction on the definition of the relation $\to$. If $M^h \rhd N^h$, use Proposition 6.3. The inductive steps are all straightforward, but the modal cases.

Let $\mathsf{ungen}(M^v)^k) \to \mathsf{ungen}(N^v)^k$, with $M^v \to N^v$, and let $i \leq k$. We have to prove that $[n]_i\mathsf{ungen}(M^v)^k) \to [n]_i\mathsf{ungen}(N^v)^k$, that is $\mathsf{ungen}([n]_i M^v)^{k+n} \to \mathsf{ungen}([n]_i N^v)^{k+n}$. If $i \leq v$, apply the induction hypotesis; otherwise $[n]_i M^v = M^v$, $[n]_i N^v = N^v$ and conclude.

Let $\mathsf{gen}(M^{k+1})^k \to \mathsf{gen}(N^{k+1})^k$, with $M^{k+1} \to N^{k+1}$, and $i \leq k$. We have to prove that $[n]_i\mathsf{gen}(M^{k+1})^k) \to [n]_i\mathsf{gen}(N^{k+1})^k$, that is $\mathsf{gen}([n]_i M^{k+1})^{k+n} \to \mathsf{gen}([n]_i N^{k+1})^{k+n}$. Conclude applying the induction hypothesis. ∎

THEOREM 6.5. *If $M^h \twoheadrightarrow N^h$, then for any $i \leq h$ and any n, $[n]_i M^h \twoheadrightarrow [n]_i N^h$.*

Proof. By induction on the lenght of the reduction, using lemma 6.4. ∎

6.1. CONFLUENCE

We prove the Church-Rosser property for $\twoheadrightarrow$, using Tait's technique as formulated in [Gir87] or [Bar84], here adapted to modal terms. We define first a new auxiliary notion of reduction ($\rightrightarrows$), corresponding to the (possible) parallel contraction of several non overlapping redexes; note that $\rightrightarrows$ is not transitive. Then, $\rightrightarrows$ is shown to respect both term and level substitution; from this we prove that " $\rightrightarrows$ satisfy the diamond property," Lemma 6.9. Since $\twoheadrightarrow$ is obviously the transitive and reflexive closure of $\rightrightarrows$, we have a standard proof that $\twoheadrightarrow$ is Church-Rosser.

In the following proofs we will give only the main (modal) cases. For the others, which are standard, the reader is referred to the literature.

DEFINITION 6.6. The *one-step parallel reduction* is defined by the following clauses.

i. $M : \alpha^k \rightrightarrows M : \alpha^k$;

ii. If $M : \alpha^k \rightrightarrows M' : \alpha^k$ and $N : \beta^k \rightrightarrows N' : \beta^k$, then $\langle M, N\rangle^k : \alpha \wedge \beta^k \rightrightarrows \langle M', N'\rangle^k : \alpha \wedge \beta^k$;

iii. If $M : \beta^k \rightrightarrows M' : \beta^k$, then $(\lambda x^k{:}\alpha^k.M)^k : \alpha \supset \beta^k \rightrightarrows (\lambda x^k{:}\alpha^k.M')^k : \alpha \supset \beta^k$;

iv. If $M : \alpha^k \rightrightarrows M' : \alpha^k$, then $\mathsf{gen}(M)^{k-1} : \Box\alpha^{k-1} \rightrightarrows \mathsf{gen}(M')^{k-1} : \Box\alpha^{k-1}$;

v. If $M : \alpha \wedge \beta^k \rightrightarrows M' : \alpha \wedge \beta^k$, then $(\mathsf{fst}\, M)^k : \alpha^k \rightrightarrows (\mathsf{fst}\, M')^k : \alpha^k$ and $(\mathsf{fst}\, M)^k : \alpha^k \rightrightarrows (\mathsf{fst}\, M')^k : \alpha^k$;

vi. If $M : \alpha^k \rightrightarrows M' : \alpha^k$ and $N : \alpha \supset \beta^k \rightrightarrows N' : \alpha \supset \beta^k$, then $(NM)^k : \beta^k \rightrightarrows (N'M')^k : \beta^k$;

vii. If $M : \Box\alpha^k \rightrightarrows M' : \Box\alpha^k$, then $\mathsf{ungen}(M)^w : \alpha^w \rightrightarrows \mathsf{ungen}(M')^w : \alpha^w$;

viii. If $M : \alpha^k \rightrightarrows M' : \alpha^k$ and $N : \beta^k \rightrightarrows N' : \beta^k$, then $(\mathsf{fst}\, \langle M, N\rangle^k)^k : \alpha^k \rightrightarrows M' : \alpha^k$ and $(\mathsf{snd}\, \langle M, N\rangle^k)^k : \beta^k \rightrightarrows N' : \beta^k$;

ix. If $M : \beta^k \rightrightarrows M' : \beta^k$ and $N : \alpha^k \rightrightarrows N' : \alpha^k$, then $((\lambda x^k{:}\alpha^k.M)^k N^k)^k : \beta^k \rightrightarrows M'[N'/x^k] : \beta^k$;

x. If $M : \alpha^k \rightrightarrows M' : \alpha^k$, then $\mathsf{ungen}(\mathsf{gen}(M)^{k-1})^{k-1+j} : \alpha^{k-1+j} \rightrightarrows [j-1]_k M' : \alpha^{k-1+j}$.

LEMMA 6.7. *If* $N : \alpha^k \rightrightarrows N' : \alpha^k$, $M : \beta^h \rightrightarrows M' : \beta^h$, *and* $x^k : \alpha^k$, *then*

$$M[N/x^k] : \beta^h \rightrightarrows M'[N'/x^k] : \beta^h.$$

Proof. By induction on the lenght of the derivation of $M : \beta^h \rightrightarrows M' : \beta^h$.

Base case: $M = M'$. This case is established by a structural induction on M.

Induction step: by cases on the last clause used to derive $M : \beta^h \rightrightarrows M' : \beta^h$. We give some cases, labelled by the clause used.

(iv) $\mathsf{gen}(M)^h : \Box\alpha^h \rightrightarrows \mathsf{gen}(M')^h : \Box\alpha^h$, where $M : \alpha^{h+1} \rightrightarrows M' : \alpha^{h+1}$. By induction hypothesis, $M[N/x^k] : \alpha^{h+1} \rightrightarrows M'[N'/x^k] : \alpha^{h+1}$, from which the thesis, since $\mathsf{gen}(M)^h[N/x^k] = \mathsf{gen}(M[N/x^k])^h : \Box\alpha^h$ and similarly for M'.

(vii) similarly to the previous case.

(x) $\mathsf{ungen}(\mathsf{gen}(M)^{h-1})^{h-1+j} : \alpha^{h-1+j} \rightrightarrows [j-1]_h M' : \alpha^{h-1+j}$, where $M : \alpha^h \rightrightarrows M' : \alpha^h$. The thesis is now given by the following diagram:

$$\begin{array}{ccc} \mathsf{ungen}(\mathsf{gen}(M)^{h-1})^{h-1+j}[N/x^k] : \alpha^{h-1+j} & \overset{?}{\rightrightarrows} & ([j-1]_h M')[N'/x^k] : \alpha^{h-1+j} \\ \| & & \| \quad (*) \\ \mathsf{ungen}(\mathsf{gen}(M)^{h-1}[N/x^k])^{h-1+j} & \rightrightarrows & [j-1]_h(M'[N'/x^k]) : \alpha^{h-1+j} \end{array}$$

where the $\rightrightarrows$ in the bottom row is given by induction hypothesis and clause (x), while equality (*) holds as either x^k does not occur in M, or $k < h$. ∎

LEMMA 6.8. *If* $M : \alpha^k \rightrightarrows M' : \alpha^k$, *then for any* i *and any* n

$$[n]_i M : \alpha^{k+n} \rightrightarrows [n]_i M' : \alpha^{k+n}$$

Proof. If $i > k$ the statement is trivial; otherwise we proceed by induction on the lenght of the derivation of $M : \alpha^k \rightrightarrows M' : \alpha^k$.

Basis: If $M = M'$ the thesis is trivial.

Induction step: we give only some typical cases, labelled by the last clause used.

(iii) $M = (\lambda x^k : \alpha^k.N)^k : \alpha \supset \beta^k$, $M' = (\lambda x^k : \alpha^k.N')^k : \alpha \supset \beta^k$, with $N : \beta^k \rightrightarrows N' : \beta^k$. By induction hypotesis $[n]_i N : \beta^{k+n} \rightrightarrows [n]_i N' : \beta^{k+n}$; now conclude by clause (iii) and definition of level substitution.

(iv) As the previous case.

(vii) $M = \mathsf{ungen}(N^{k-j})^k : \alpha^k$ and $M' = \mathsf{ungen}(N'^{k-j})^k : \alpha^k$,
with $N^{k-j} : \beta^{k-j} \rightrightarrows N'^{k-j} : \beta^{k-j}$.
The thesis is given by the following diagram:

$$\begin{array}{ccc} [n]_i\mathsf{ungen}(N^{k-j})^k : \alpha^{k+n} & \overset{?}{\rightrightarrows} & [n]_i\mathsf{ungen}(N'^{k-j})^k : \alpha^{k+n} \\ \| & & \| \\ \mathsf{ungen}([n]_i N^{k-j})^{k+n} : \alpha^{k+n} & \overset{\text{by IH}}{\rightrightarrows} & \mathsf{ungen}([n]_i N'^{k-j})^{k+n} : \alpha^{k+n} \end{array}$$

(ix) $M = ((\lambda x^k : \alpha^k.N)^k P^k)^k : \beta^k$ and $M' = N'^k[P'^k/x^k] : \beta^k$,
with $N : \beta^k \rightrightarrows N' : \beta^k$ and $P^k : \alpha^k \rightrightarrows P'^k : \alpha^k$. The thesis is given by the following diagram:

$$\begin{array}{ccc} [n]_i((\lambda x^k{:}\alpha^k.N)^k P^k)^k : \beta^{k+n} & \overset{?}{\rightrightarrows} & [n]_i(N'^k[P'^k/x^k]) : \beta^{k+n} \\ \| & & \| \quad (*) \\ ((\lambda x^{k+n}{:}\alpha^{k+n}.[n]_i N)^{k+n}([n]_i P^k))^{k+n} : \beta^{k+n} & \overset{\text{by IH}}{\rightrightarrows} & ([n]_i N')^k[[n]_i P'^k/x^{k+n}] : \beta^{k+n} \end{array}$$

where (*) is Lemma 5.10 and the $\rightrightarrows$ in the bottom row follows by induction hypothesis and clause ix.

(x) $M = \mathsf{ungen}(\mathsf{gen}(N^{k-j+1})^{k-j})^k : \alpha^k$ and $M' = [j-1]_{k-j+1}N'^{k-j+1} : \alpha^k$, with $N^{k-j+1} : \alpha^{k-j+1} \rightrightarrows N'^{k-j+1} : \alpha^{k-j+1}$, which by IH implies that

$$[n]_i N^{k-j+1} : [n]_i\alpha^{k-j+1} \rightrightarrows [n]_i N'^{k-j+1} : [n]_i\alpha^{k-j+1} \tag{2}$$

We have two cases. If $i \leq k-j$ the thesis is given by the following diagram:

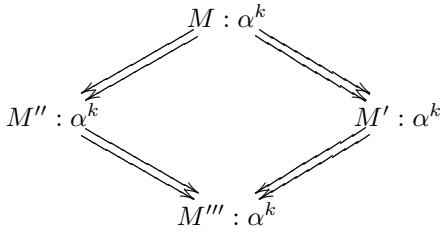
$$\begin{array}{ccc} [n]_i\mathsf{ungen}(\mathsf{gen}(N^{k-j+1})^{k-j})^k : \alpha^{k+n} & \overset{?}{\rightrightarrows} & [n]_i[j-1]_{k-j+1}N'^{k-j+1} : \alpha^{k+n} \\ \| & & \| \quad (*) \\ \mathsf{ungen}(\mathsf{gen}([n]_i N^{k-j+1})^{k-j+n})^{k+n} : \alpha^{k+n} & \overset{(**)}{\rightrightarrows} & [j-1]_{k-j+1+n}[n]_i N'^{k-j+1} : \alpha^{k+n} \end{array}$$

where (*) is Lemma 5.11(i), and (**) follows by (2) and clause x. If $i > k-j$ the following diagram establishes the thesis:

$$\begin{array}{ccc} [n]_i\mathsf{ungen}(\mathsf{gen}(N^{k-j+1})^{k-j})^k : \alpha^{k+n} & \overset{?}{\rightrightarrows} & [n]_i[j-1]_{k-j+1}N'^{k-j+1} : \alpha^{k+n} \\ \| & & \| \quad (*) \\ \mathsf{ungen}(\mathsf{gen}(N^{k-j+1})^{k-j})^{k+n} : \alpha^{k+n} & \overset{(**)}{\rightrightarrows} & [j-1+n]_{k-j+1}N'^{k-j+1} : \alpha^{k+n} \end{array}$$

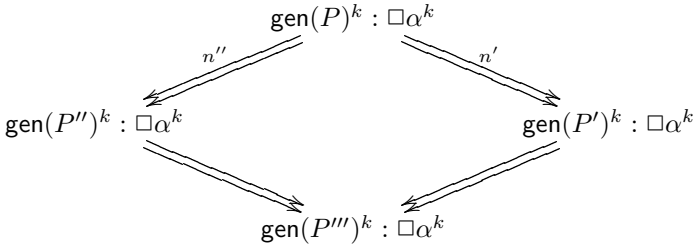
where (*) is Lemma 5.11(ii), and (**) follows by 2 and clause x. ∎

Lemma 6.9 (Diamond Property) *Suppose $M : \alpha^k \rightrightarrows M' : \alpha^k$ and $M : \alpha^k \rightrightarrows M'' : \alpha^k$. Then we can find a term $M''' : \alpha^k$ such that*

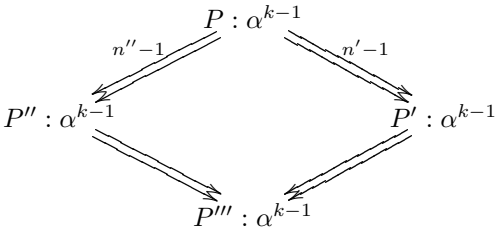


Proof. Let n' and n'' be the lenght of the derivations r' of $M : \alpha^k \rightrightarrows M' : \alpha^k$ and r'' of $M : \alpha^k \rightrightarrows M'' : \alpha^k$. The thesis is extablished by induction on $n' + n''$. We give only the modal cases. We write $M : \alpha^k \overset{n}{\rightrightarrows} M' : \alpha^k$ to denote that $M : \alpha^k \rightrightarrows M' : \alpha^k$ is established with a deduction of lenght n.

- Both r' and r'' end with clause (iv).

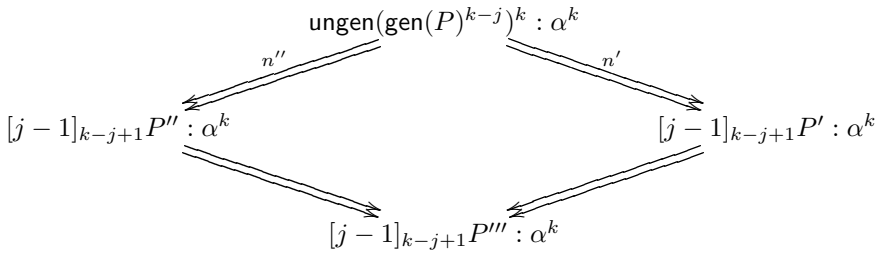


where

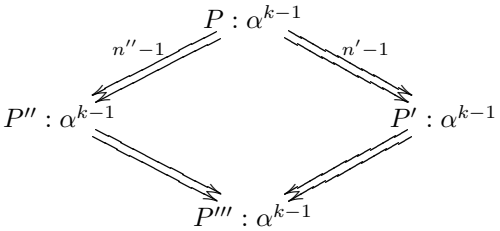


is obtained by I.H.

- Both r' and r'' end with clause (vii). As the previous case.
- Both r' and r'' end with clause (x).



Where

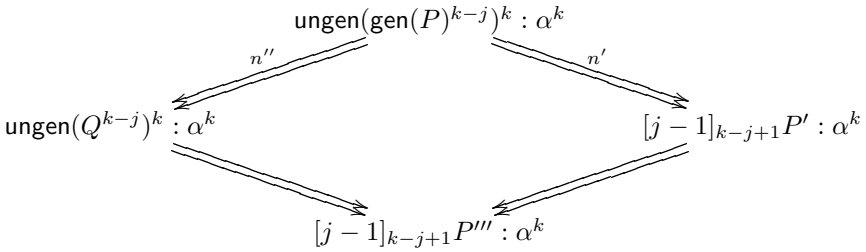


is obtained by I.H. and

$$[j-1]_{k-j+1}P' : \alpha^k \;\rightrightarrows\; [j-1]_{k-j+1}P''' : \alpha^k \leftleftarrows [j-1]_{k-j+1}P'' : \alpha^k$$

holds by Lemma 6.8.

- Last clause of r' is (x) and last clause of r'' is (vii).



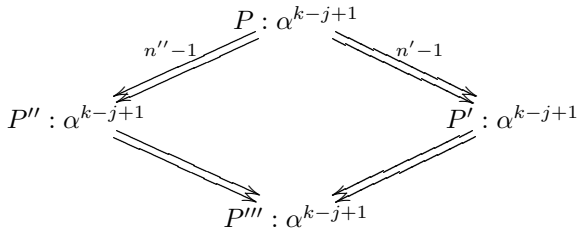
where

$$\mathsf{gen}(P)^{k-j} : \Box\alpha^{k-j} \overset{n''-1}{\rightrightarrows} Q^{k-j} : \Box\alpha^{k-j}$$

Observe now that $Q^{k-j} = \mathsf{gen}(P'')^{k-j}$, with

$$P : \alpha^{k-j+1} \overset{<n''}{\rightrightarrows} P'' : \alpha^{k-j+1}$$

since no clause for $\rightrightarrows$ may remove a toplevel gen. By induction hypothesis we obtain



Lemma 6.8 allows to conclude. ∎

THEOREM 6.10 (Church-Rosser) *The $\twoheadrightarrow$ relation is confluent.*

Proof. $M \twoheadrightarrow N$ iff $M = M_0 \rightrightarrows \ldots \rightrightarrows M_n = N$ with $n \geq 0$. The usual Church-Rosser diamond can now be closed by using the previous lemma. ∎

6.2. STRONG NORMALIZATION

We reduce the problem of strong normalization for $\lambda^\ell S4$ to the strong normalization for the system of next definition.

DEFINITION 6.11. [Calculus $\lambda S4$] *Terms* and *derivations* are inductively defined by the following rules.

$$x : \sigma^k$$

$$\frac{\begin{array}{cc}\Gamma & \Delta \\ \vdots & \vdots \\ M : \sigma^k & N : \tau^k\end{array}}{\langle M, N\rangle : \sigma \wedge \tau^k}\wedge\mathcal{I} \qquad \frac{\begin{array}{c}\Gamma \\ \vdots \\ M : \sigma \wedge \tau^k\end{array}}{(\mathsf{fst}\, M) : \sigma^k}\wedge\mathcal{E}_l \qquad \frac{\begin{array}{c}\Gamma \\ \vdots \\ M : \sigma \wedge \tau^k\end{array}}{(\mathsf{snd}\, M) : \tau^k}\wedge\mathcal{E}_r$$

$$\frac{\begin{array}{c}\Gamma \quad [x:\sigma^k] \\ \vdots \\ M:\tau^k\end{array}}{\lambda x.M:\sigma\supset\tau^k}\supset\mathcal{I} \qquad \frac{\begin{array}{cc}\Gamma & \Delta \\ \vdots & \vdots \\ M:\sigma\supset\tau^k & N:\sigma^k\end{array}}{MN:\sigma^k}\supset\mathcal{E}$$

$$\frac{\begin{array}{c}\Gamma \\ \vdots \\ M:\sigma^j\end{array}}{M:\Box\sigma^{j-1}}\Box\mathcal{I}\ {\scriptstyle \mathrm{j}>\#\Gamma} \qquad \frac{\begin{array}{c}\Gamma \\ \vdots \\ M:\Box\sigma^j\end{array}}{M:\sigma^k}\Box\mathcal{E}\ {\scriptstyle \mathrm{k}\geq\mathrm{j}}$$

Derivations in $\lambda^\ell S4$ can be obviously translated into $\lambda S4$, by forgetting the type and level decoration as well as all the gen, ungen constructors. Writing M° for the term obtained in this way, the following is straightforward.

PROPOSITION 6.12. $\Gamma \vdash_{\lambda^\ell S4} M:\sigma^k \iff \Gamma^\circ \vdash_{\lambda S4} M^\circ:\sigma^k$

Let λ be the intuitionistic lambda calculus with implication and conjunction. The types of $\lambda S4$ can be interpreted into the types of λ by means of the following translation.

$$\begin{array}{rcl}(p^k)^* & = & p \\ (\alpha\supset\beta^k)^* & = & (\alpha^k)^*\supset(\beta^k)^* \\ (\alpha\wedge\beta^k)^* & = & (\alpha^k)^*\wedge(\beta^k)^* \\ (\Box\alpha^k)^* & = & (\alpha^{k+1})^*\end{array}$$

PROPOSITION 6.13. $\Gamma \vdash_{\lambda S4} M:\sigma^k \Longrightarrow \Gamma^* \vdash_\lambda M:\sigma^*$

Proof. Induction on the derivation, the modal rules becoming vacuous steps in λ. ∎

It is well known (e.g. [Bar92]) that λ enjoys strong normalization. It is now easy to obtain as a corollary the same result for $\lambda^\ell S4$.

THEOREM 6.14. *$\lambda^\ell S4$ enjoys strong normalization.*

Proof. Let $\Gamma \vdash_{\lambda^\ell S4} M:\sigma^k$ and suppose there is an infinite reduction sequence starting from M. Observe now that this sequence cannot be composed (from some point on) only of modal contractions, since a modal contraction strictly decreases the number of nodes of the proof tree. Hence the reduction sequence contains an infinite number of propositional reductions (that is, contractions of non modal redexes). But this is impossibile, because these propositional reductions would also be reductions of M°, which is typeable in λ, by the previous propositions, while λ enjoys strong normalization. ∎

6.3. Computations in subsystems of $\lambda^\ell S4$

While all the results of the previous sections are stated for the stronger system $\lambda^\ell S4$, a careful inspection of the proofs shows that all the statements which apply to a given system still hold.

THEOREM 6.15. *Let $\lambda^\ell L$ one of $\lambda^\ell K$, $\lambda^\ell KT$, $\lambda^\ell K4$, or $\lambda^\ell S4$.*
(i) Reduction in $\lambda^\ell L$ is confluent.
(ii) Reduction in $\lambda^\ell L$ enjoys strong normalization.

7. Related work

In this brief section we relate our proposal to some of the recent work on natural deduction for modal logics. This is not the place for a detailed proof theoretical analysis of the different systems and, for this reason, we will discuss only those systems allowing a computational interpretation of proofs, the exception being the work presented next, which we take into account for its similarity with our system. For more detailed analysis of the proof theory of modal logic, we refer to [Min92] and [Wan93].

7.1. The "constructive" system of Benevides and Maibaum

Benevides and Maibaum [BM92], starting from a semantical intuition on Hintikka systems, propose a set of natural deduction rules for the $\Box$-based systems essentially analogous to our proposal. However, their semantical insight seems to hinder a full mastering of the level machinery. They introduce in their system redundant rules for the interaction between $\Box$ and the propositional connectives (see the rules R_2 of their Section 3.2.2), which are derivable in the rest of the system. From a proof theoretical point of view these rules are hardly justified, since they do not obey to the tenet: "For each connective, (only) one introduction and (only) one elimination". For this reason, it seems impossible to relate these systems to any clean sequent calculus for the same logics (see, *contra*, our Section 4.2.)

They prove the equivalence of their systems to the classical Hilbert style formulations. However, no notion of normalization of proofs is introduced. It is our belief that any study of the constructive content of a logical system cannot dispense from the study of proof normalization. If one does not tackle normalization, why not using the simple, naive approaches outlined in the Introduction?

7.2. The intuitionistic calculus of Bierman, Meré and de Paiva

In [BMdP92] is presented an approach to the $\Box$ modality essentially based on a variation of Prawitz proposal. The problematic $\Box\mathcal{I}$ rule has the form

$$\frac{\begin{array}{ccccc}\Gamma_1 & & \Gamma_n & & [x_1 : \Box\sigma_1, \ldots, x_n : \Box\sigma_n] \\ \vdots & & \vdots & & \vdots \\ M_1 : \Box\sigma_1 & \ldots & M_n : \Box\sigma_n & & N : \tau\end{array}}{\mathsf{box}\ N\ \mathsf{with}\ M_1, \ldots, M_n\ \mathsf{for}\ x_1, \ldots, x_n : \Box\tau}\ \Box\mathcal{I}$$

For this system, the authors introduce several reduction rules corresponding to a categorical model and show its equivalence with the standard sequent calculus for S4.

It is clear that this system has some advantages over Prawitz', since the rule $\Box\mathcal{I}$ is not as global as $\Box\mathcal{I}_{\mathcal{P}}$ (see Section 4.1.) and allow a clearer reduction step. However, the approach seems specifically designed for S4, since it is not clear how the rule would scale to the normal subsystems of S4. Moreover, many of the critiques of the Introduction still apply to the proposed rule. In particular, a good introduction rule should construct its conclusion from *all* its premises and possibly some assumptions, a requirement clearly violated by the proposed $\Box\mathcal{I}$.

7.3. The labelled natural deduction of Gabbay and de Queiroz

A completely different approach is the one proposed by Gabbay and de Queiroz in a sequel of papers, e.g. [GdQ92, GdQ91], as an attempt to give a general theory of natural deduction extending the Curry-Howard isomorphism to a large class of logics (classical, linear, relevant, modal). As for modalities,

> it offers a *deductive* (as opposed to *model theoretic*) account of the connections between modal logics and its propositional counterparts when world-variables are introduced in the functional calculus of the labels (i.e. when a little of the semantics is *brought to the syntax,* so to speak). [GdQ91]

The calculus is a kind of second order system, where second order objects, which syntactically are only variables, correspond to possible worlds. The basic rules for introduction and elimination of $\Box$ are:

$$\frac{\begin{array}{c}\Gamma\ [\mathbb{W} : \mathcal{U}] \\ \vdots \\ M : \sigma\end{array}}{\Lambda\mathbb{W}.M : \Box\sigma}\ \Box\mathcal{I} \qquad \frac{\begin{array}{cc}\Gamma & \Delta \\ \vdots & \vdots \\ M : \Box\sigma & \mathbb{T} : \mathcal{U}\end{array}}{\mathcal{EXTR}(M, \mathbb{T}) : \sigma(\mathbb{T})}\ \Box\mathcal{E}$$

where $\mathcal{U}$ stands for an intended collection of "worlds."

There is an certain analogy between our levels and the world-variables, which is especially clear in the case of the logic K. Moving to stronger logics, however, obscures this analogy. The characteristic axiom of KT, for instance, is not provable *as is* in their system; they can only prove its modal closure, $\Box(\Box\sigma \supset \sigma)$ (it seems they would need a kind of second order constants to prove $\Box\sigma \supset \sigma$). In the case of $\mathsf{K4}$, the proofs of the characteristic axioms are remarkably different in the two systems; while their proof consists of just a $\Box\mathcal{I}$ rule, in our case we have a $\Box\mathcal{E}$ followed by two $\Box\mathcal{I}$.

References

[AP90] Jean-Marc Andreoli and Remo Pareschi. Logic programming with sequent systems: a linear logic approach. In *Proc. of Workshop on Extensions of Logic Programming*, Lecture Notes in Artificial Intelligence. Springer-Verlag, 1990.

[Bar84] Henk Barendregt. *The Lambda Calculus: its Syntax and Semantics*. Studies in Logic and the Foundations of Mathematics. North-Holland, 1984. Revised Edition.

[Bar92] Henk Barendregt. Lambda calculus with types. In S. Abramsky, D.M. Gabbay, and T.S.E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume II Background: Computational Structures, pages 118–310. Oxford University Press, 1992.

[BM92] M.R.F. Benevides and T.S.E. Maibaum. A constructive presentation for the modal connective of necessity ($\Box$). *Journal of Logic and Computation*, 2:31–50, 1992.

[BMdP92] Gavin Bierman, Claudia Meré, and Valeria de Paiva. Intuitionistic necessity revisited. In *Logic at Work: Applied Logic Conference*, 1992.

[BS84] R. Bull and K. Segeberg. Basic modal logic. In D. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic*, volume II, pages 1–88. Reidel, 1984.

[CCM85] G. Cousineau, P.-L. Curien, and M. Mauny. The categorical abstract machine. In *ACM Conference on Functional Programming and Computer Architecture, Nancy, France*, 1985.

[Con86] Robert Constable. *Implementing Mathematics with the Nuprl Proof Development System*. Prentice-Hall, 1986.

[Dos85] Kosta Dosen. Sequent-systems for modal logic. *Journal of Symbolic Logic*, 50:149–168, 1985.

[EH85] E. A. Emerson and J. Y. Halpern. Decision procedures and expressiveness in the temporal logic of branching time. *Journal of Computer and System Science*, 30:1–24, 1985.

[GdQ91] Dov M. Gabbay and Ruy J.G.B. de Queiroz. Labelled natural deduction. Imperial College, Preliminary Draft, 1991.

[GdQ92] Dov M. Gabbay and Ruy J.G.B. de Queiroz. Extending the curry-howard interpretation to linear, relevant and other resource logics. *Journal of Symbolic Logic*, 57:1319–1365, 1992.

[Gir87] Jean-Yves Girard. *Proof Theory and Logical Complexity*. Bibliopolis, 1987.

[Mas92] Andrea Masini. 2-sequent calculus: A proof theory of modalities. *Annals of Pure and Applied Logic*, 58:229–246, 1992.

[Mas93] Andrea Masini. 2-sequent calculus: Intuitionism and natural deduction. *Journal of Logic and Computation*, 3:1–31, 1993. to appear.

[Mes92] José Meseguer. Conditional rewriting logic as a unified model of concurrency. *Theoretical Computer Science*, 96:73–155, 1992.

[Min92] Grigori Mints. *Selected Papers in Proof Theory*. Bibliopolis, 1992.

[MMS92] Andrea Masini and Andrea Maggiolo-Schettini. TTL: A formalism to describe local and global properties of distributed systems. *Theoretical Informatics and Applications*, 2:115–149, 1992.

[MNPS91] Dale Miller, Gopalan Nadathur, Frank Pfenning, and Andre Scedrov. Uniform proofs as a foundation for logic programming. *Annals of Pure and Applied Logic*, 51:125–157, 1991.

[MPW89] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, I and II. Technical Report ECS-LFCS-89-85&86, University of Edinburgh, Dpt. of Computer Science, 1989.

[MTH90] Robin Milner, Mads Tofte, and Robert Harper. *The Definition of Standard ML*. The MIT Press, 1990.

[PHH93] Gordon Plotkin, Furio Honsell, and Robert Harper. A framework for defining logics. *Journal of the ACM*, 40(1):143–184, 1993.

[Pnu77] Amir Pnueli. The temporal logic of concurrent programs. In *Proc. of ACM Symposium on Foundations of Computer Science*, pages 45–57. IEEE, 1977.

[Pra65] Dag Prawitz. *Natural Deduction*. Acta Universitatis Stockholmiensis, Stockholm Studies in Philosophy 3. Almqvist & Wiksell, Stockholm, 1965.

[TvD88] Anne Troelstra and Dirk van Dalen. *Constructivism in Mathematics*, volume II. North-Holland, 1988.

[Wan93] H. Wansing. Sequent calculi for normal modal propositional logic. *Journal of Logic and Computation*, 1993. to appear.