Two deductive systems for the constructive logic S4, a formal verification

Lourdes del Carmen González-Huesca[1*], Favio E. Miranda-Perea[1†] and P. Selene Linares-Arévalo[1‡]

Departamento de Matemáticas, Facultad de Ciencias UNAM, Circuito Exterior S/N,
Cd. Universitaria 04510, CdMx, México

Abstract

We present a proof of the equivalence between two deductive systems for the constructive modal logic S4. On one side, an axiomatic characterization inspired by Hakli and Negri's system of derivations from assumptions for modal logic K, a Hilbert-style formalism designed to ensure the validity of the deduction theorem. On the other side, the judgmental reconstruction given by Pfenning and Davies by means of a so-called dual natural deduction approach that makes a distinction between valid, true and possible formulas. Both systems and the proof of their equivalence are formally verified using the Coq proof assistant.

1 Introduction

The relevance of modal logic in philosophy and mathematics is well established. Moreover, its importance in computer science has come of age. For instance, the monadic and computational interpretations of modal logic [4, 2] for various type theories are deeply related to concurrent and distributed computations [20, 34]. These applications entail the need for a verification process which nowadays cannot be thought of without the help of a proof assistant.

To be able to carry out serious verification tasks with help of these software programs, we need to provide them with an implementation of deductive methodologies akin to human (mathematical) thinking. This poses a problem in the case of modal reasoning, where the typical deductive systems in the literature are axiomatic or elaborated sequent calculi (see for example [28]). Not to mention tableaux systems [8, chapter 2] which are the basis of several theorem provers for modal logics[1]. Moreover, some known natural deduction presentations of modal logic are sophisticated formalisms that either involve the semantics, like labelled deduction systems ([33]; see also [13] for a comprehensive overview of modal natural deduction systems) or require some clumsy conventions that make them difficult to be implemented in a proof assistant. For example, the use of special subproofs (boxes) and conventions in Fitch-style systems ([3], [9], [10, section 1.6], [17, p. 34]).

In the case of constructive modal logic S4, these problems are mitigated by considering the judgmental reconstruction of this logic proposed by Pfenning and Davies [26]. They use an approach that follows the constructive philosophy of Martin-Löf [22] by means of hypothetical and categorical judgments. S4 is an important logic for its applications in computing, for instance in concurrency and staged computation [4], and also for its relationship with intuitionistic, linear

[*] Supported by DGAPA-UNAM posdoctoral fellowships.

[†] Partially supported by PAPIME UNAM PE102117.

[‡] Partially supported by PAPIME UNAM PE102117.

[1] A non-comprehensive list of theorem provers and other computational tools for modal logics are available at http://www.cs.man.ac.uk/~schmidt/tools/#provers

and lax logic [23]. In this direction, we hope that the here presented mechanization will assist in the development of actual verification case studies, like the formalization of modal lambda calculus in [11] or lax logic in [7], as well as the mechanization of Gödel's interpretation of intuitionistic propositional calculus in S4 [32].

Our specific goal here is to show the equivalence between this system, called dual natural deduction by Kavvos [15] and an axiomatic system in the style of Hakli and Negri [12]. This ensures that the dual system exactly corresponds to the more common axiomatic formalisms for modal logic. To the best of our knowledge the literature lacks of such proof (though, for the case of constructive necessity, this has been settled by Kaavos [15] and by our previous work [6]). We do not pursuit indirect equivalence proofs gained from soundness/completeness results, due to the fact that we are interested in proof-search and translation processes. These objectives are not mentioned here due to lack of space, also we do not include a development involving any formal semantics since it would depart from our goals.

The here exposed results extend our previous work around constructive necessity [6] by adding the $\Diamond$ possibility operator as primitive. Recall that in the constructive setting there is no duality between $\Box$ and $\Diamond$ modal operators. The extension of the axiomatic system is straightforward, for we only need to add the axioms pertinent to $\Diamond$. However, in the case of natural deduction, the system needs to handle not only formulas, but modal judgments ($A\,\mathit{true},\ A\,\mathit{poss}$) stating that a formula can be either true or possible. It is important to remark that these qualifiers, and also that for validity, are defined following the semantic intuition, but without any formal semantics involved. This feature allows to describe modal knowledge syntactically, while still possing some challenges with respect to our mechanization.

The proof approach here taken was gained from a full synergy between pure mathematical paper-and-pencil reasoning and mechanized proof attempts. This path led us to some novel proof techniques. For instance, the admissibility of several inference rules here presented is not proved by induction on the (height of) derivations. Instead a more simple induction on the (length of the) contexts of proved sequents suffices (for instance, see the proof of Theorem 2.3). This succeeds due to the fact that contexts are implemented as an inductive list data structure, not as a set or multiset. Moreover, most of the proofs here presented make heavy use of structural rules, whose particular shape was gained from the interactive verification process. This is an important difference with respect to other deductive system treatments, where the structural rules are either absent or its use is implicit, a feature that cannot be translated to the Coq formal development.

Our exposition begins with the syntax of formulas and contexts for modal logic S4. The axiomatic system is briefly discussed in Section 2 and the natural deduction system is developed in Section 3. The equivalence of these systems is proved in Section 4. To close, we give some final remarks in Section 5. The full Coq development is available at `https://bitbucket.org/luglzhuesca/mlogic-formalverif/src/master/S4` .

1.1 Formulas and contexts

We adopt in this work the characterization of the notion of modal derivability by means of hypothetical judgments (sequents) $\Gamma \vdash A$ where Γ is a finite collection of hypotheses, called the context, and A is a formula. Such a sequent can be read as 'A follows from the collection of hypotheses Γ'. In this brief section we recall the definition of formulas and contexts.

Modal formulas are generated by the following grammar:

$$A, B \quad ::= \quad p_n \mid A \to B \mid \Box A \mid \Diamond A$$

where p_n denotes an element taken from an infinite supply of propositional variables, indexed by a natural number. Observe that implication is the only propositional connective, in particular we do not consider neither negation nor the constant $\bot$. Therefore we will be dealing with the implicational fragment of minimal logic [30] extended with modal operators of necessity and possibility. A particular modal logic is generated by adding suitable axioms to a underlying logic. It is important to remark that the logic here considered is called constructive and differs from the classical and intuitionistic as their logic basis are not the same. Certainly, these logics have more differences to take into account [14, 29, 31], for instance, in the constructive modal logic does not hold the duality axiom $\Diamond A \leftrightarrow \neg\Box\neg A$ nor the formula $\neg\Diamond\bot$ which holds in intuitionistic modal logics.

Contexts are implemented as finite lists of formulas built from the empty list, denoted here by $\cdot$, and a constructor that generates a new list from a given one by adding a new element to its right-end. They are formally defined as follows:

$$\Gamma, \Delta \quad ::= \quad \cdot \mid \Gamma, A$$

Furthermore, the append operation of two contexts Γ and Γ' is denoted with a semicolon $\Gamma;\Gamma'$.

2 Axiomatic system for S4

In contrast to the usual axiomatic deductive systems, the one here presented, originally given by Hakli and Negri in [12] for the classical modal logic K, is specifically designed to derive theorems from hypotheses and not only from axioms or previous theorems. This is the key to being able to validate the deduction theorem, which sometimes is considered invalid for modal logic. The set $\mathcal{A}$ of axioms defining the modal logic $\mathcal{H}_{\mathsf{S4}}$ (a Hilbert-style system for $\mathsf{S4}$) is

$$\begin{array}{ll@{\qquad}ll}
\mathsf{A1} & A \to (B \to A) & \mathsf{A3} & (A \to B \to C) \to (B \to A \to C) \\
\mathsf{A2} & (A \to (A \to B)) \to (A \to B) & \mathsf{A4} & (B \to C) \to ((A \to B) \to (A \to C))
\end{array}$$

$$\begin{array}{ll@{\qquad}ll}
\mathbb{K} & \Box(A \to B) \to (\Box A \to \Box B) & \Diamond\mathbb{K} & \Box(A \to B) \to (\Diamond A \to \Diamond B) \\
\mathbb{T} & \Box A \to A & \Diamond\mathbb{T} & A \to \Diamond A \\
\mathit{4} & \Box A \to \Box\Box A & \Diamond\mathit{4} & \Diamond\Diamond A \to \Diamond A
\end{array}$$

From these axioms we generate a relation of modal derivability $\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A$ by means of the following inductive definition:

$$\dfrac{A \in \Gamma}{\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A}\ (\textsc{Hyp}) \qquad\qquad \dfrac{A \in \mathcal{A}}{\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A}\ (\textsc{Ax})$$

$$\dfrac{\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A \qquad \Gamma' \vdash_{\mathcal{H}_{\mathsf{S4}}} A \to B}{\Gamma';\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} B}\ (\mathrm{MP}) \qquad\qquad \dfrac{\cdot \vdash_{\mathcal{H}_{\mathsf{S4}}} A}{\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} \Box A}\ (\textsc{Nec})$$

Let us observe that the necessitation rule allows to introduce a $\Box$ operator only if the formula to be boxed is a theorem and that, due to the presence of axiom $\Diamond\mathbb{T}$, there is no need for an inference rule involving the $\Diamond$ operator (though see Lemma 2.2 below). Moreover, the *modus ponens* rule (MP) is stated in a multiplicative (independent contexts) style where the context in the conclusion is the union (in our case concatenation) of the different contexts in the premises[2]. The reason to use this approach is that this is the natural way for the establishment of a correspondence of $\mathcal{H}_{\mathsf{S4}}$ with usual axiomatic systems that do not handle hypotheses. This choice departs from the treatment in Kavvos [15], where both axiomatic and natural deduction systems for necessity are additive, and also posses some challenges for the formal verification, as discussed next and in our previous work [6]. In the systems here presented both styles are present. As shown above, the axiomatic rules are multiplicative, whereas the natural deduction rules are additive (see page 6). This issue led to complications on the desired equivalence proof, difficulties that are solved with the definition of suitable structural rules: permutation and contraction in the axiomatic system (Lemma 2.1); weakening and exchange for natural deduction system (Lemma 3.3). The peculiar shape of each of these rules contributes to a WYSIWYG (*What You See Is What You Get*) proof approach (see [5]) in the sense that in the process of checking our proof scripts, the interactive proof session that the reader develops, corresponds straightforward to the proofs in this paper.

2.1 Admissible rules in $\mathcal{H}_{\mathsf{S4}}$

The deduction theorem and other relevant admissible rules in $\mathcal{H}_{\mathsf{S4}}$ are discussed next.

Theorem 2.1 (Deduction)**.** *If* $\Gamma, A \vdash_{\mathcal{H}_{\mathsf{S4}}} B$ *then* $\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A \to B$.

Proof. Induction on $\Gamma, A \vdash_{\mathcal{H}_{\mathsf{S4}}} B$. □

Corollary 2.1 (Cut rule)**.** *The following rule is admissible*

$$\frac{\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A \qquad \Gamma', A \vdash_{\mathcal{H}_{\mathsf{S4}}} B}{\Gamma'; \Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} B}\ (\textsc{Cut})$$

Proof. A direct consequence of the deduction theorem and *modus ponens*. □

The converse implication of the deduction theorem or principle of detachment, is also easily achieved.

Theorem 2.2 (Principle of detachment)**.** *If* $\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A \to B$ *then* $\Gamma, A \vdash_{\mathcal{H}_{\mathsf{S4}}} B$.

Proof. By *modus ponens* of the hypothesis and $A \vdash_{\mathcal{H}_{\mathsf{S4}}} A$. □

Due to the fact that contexts are lists, the deduction theorem allows us to discharge only the last assumption in the context. To being able to discharge any hypothesis we must either use structural rules implicitly or prove a generalization. We choose the second option and spell out the proof which, though quite simple, serves to show the, to the best of our knowledge novel, method of proving admissibility of an inference rule by induction on the context.

Theorem 2.3 (Generalized Deduction Theorem)**.** *The following rule is admissible:*

$$\frac{\Gamma, A; \Gamma' \vdash_{\mathcal{H}_{\mathsf{S4}}} B}{\Gamma; \Gamma' \vdash_{\mathcal{H}_{\mathsf{S4}}} A \to B}\ (\mathrm{GDT})$$

[2] It is more common to use the additive style, which keeps the very same context for both the premises and the conclusion of an inference rule.

Proof. Induction on Γ'. The basis case $\Gamma' = \cdot$ is just the Deduction Theorem 2.1. For the inductive step assume that $\Gamma, A; \Gamma', C \vdash_{\mathcal{H}_{\mathsf{S4}}} B$, which implies $\Gamma, A; \Gamma' \vdash_{\mathcal{H}_{\mathsf{S4}}} C \to B$ by Theorem 2.1. The I.H. yields now $\Gamma; \Gamma' \vdash_{\mathcal{H}_{\mathsf{S4}}} A \to C \to B$. From this by *modus ponens* with an adequate instance of axiom $\mathsf{A3}$ we get $\Gamma; \Gamma' \vdash_{\mathcal{H}_{\mathsf{S4}}} C \to A \to B$. Finally the principle of detachment (Theorem 2.2) allows to conclude $\Gamma; \Gamma', C \vdash_{\mathcal{H}_{\mathsf{S4}}} A \to B$. □

Several further properties of system $\mathcal{H}_{\mathsf{S4}}$ are gained thanks to the availability of the Deduction Theorem and its inverse. We present next some of them that will be needed later to show the equivalence between the axiomatic and natural deduction approaches to $\mathsf{S4}$.

Lemma 2.1 (Structural rules)**.** *The following rules are admissible:*

$$\frac{\Gamma; \Gamma' \vdash_{\mathcal{H}_{\mathsf{S4}}} A}{\Gamma'; \Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A}\ (\textsc{Ctx-Perm}) \qquad\qquad \frac{\Gamma; \Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A}{\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A}\ (\textsc{Ctx-cont})$$

Proof. Induction on Γ in each case. Proposition 2.3 and the detachment principle will be quite useful. □

Next we prove the admissibility of two rules that allow to prove modal formulas, namely a rule for diamond introduction and a generalization of the neccesitation rule when a context is non-empty but consists only of boxed formulas.

Lemma 2.2 (Modal introduction rules)**.** *The following rules are admissible*

$$\frac{\Gamma^{\Box} \vdash_{\mathcal{H}_{\mathsf{S4}}} A}{\Gamma^{\Box}; \Gamma' \vdash_{\mathcal{H}_{\mathsf{S4}}} \Box A}\ (\textsc{GenNec}) \qquad\qquad \frac{\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A}{\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} \Diamond A}\ (\textsc{Dia})$$

Proof. For the first rule, by the (Ctx-Perm) rule it suffices to show that $\Gamma'; \Gamma^{\Box} \vdash_{\mathcal{H}_{\mathsf{S4}}} \Box A$, which is verified by induction on Γ. The second rule is directly derivable from axiom $\Diamond\mathbb{T}$ and *modus ponens.* □

3 Natural deduction for $\mathsf{S4}$

The here discussed formalism for $\mathsf{S4}$, denoted $\mathcal{N}_{\mathsf{S4}}$, is a natural deduction system in sequent form or S-system [13] where propositions are analyzed judgmentally. It corresponds to the formal system for necessity and possibility presented by Pfenning and Davies in [26, Section 5], a work based in the philosophical development of Martin-Löf Type Theory [21]. This formal system makes an essential distinction of three basic judgments to describe knowledge without an explicit use of worlds. The A *true* judgment denotes how to verify A under hypothetical judgments. A *valid* represents, by means of categorical judgments, a proposition which does not depend on true hypotheses or any particular world. Finally, A *poss* represents a possible truth, which implies that A must be the only available true hypothesis in a hypothetical judgment. It is important to remark that the semantic labels in the definition of these judgments are mere intuitive, for there is no formal semantics involved in the following. Instead we could use labels like *global, local* and *unique.* The distinction between valid and true hypotheses is related to the notion of local and global assumptions of Fitting [8, p.177]. but we prefer to keep the terminology of [26]. This approach is also discussed in [12] but it is not a motivation for their axiomatic system with assumptions. In conclusion, the two systems discussed in this work are not obviously related.

Our natural deduction approach handles sequents of the form $\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J$, where the antecedents Δ and Γ are contexts for valid and true hypotheses respectively, and the succedent J is a conclusion judgment, which are judgments of truth or possibility, formally defined as:

$$J \quad ::= \quad A\,\mathit{true} \mid A\,\mathit{poss}$$

Let us observe that contexts contain formulas and not judgments as in the original formulation where, from an strict point of view, there is only one context splitted in two parts, a feature that would be quite complicated to implement in Coq. Instead, our choice simplifies the presentation and implementation of both, contexts and sequents. For instance, there is no need for an explicit judgment of validity (A *valid*). For the contexts are implemented as two disjoint lists making the use of *true* and *valid* labels redundant. This kind of separated contexts is referred to as a dual context notion by Kavvos in [15]. Also, there is no need to explicitly consider neither hypotheses of possibility, as they are modelled by unique true assumptions, nor judgments of validity as conclusions since they are represented by the judgment $\Box A\,\mathit{true}$.

Another difference with the original formulation lies in the fact that, as the authors mention, their system has an explicit propositional reasoning and only an implicit judgment reasoning, saying that the derivability relation is *subject to the inclusion of $A\,true$ in $A\,poss$*. The more convenient way to implement this feature is by an explicit rule called here (TP), which converts a True judgment into a Possibility judgment. Here, the derivability relation is mechanized by an inductive definition, given by the inference rules below, which corresponds to a shallow embedding of derivability. Therefore the explicit statement and use of rule (TP) is mandatory. This rule, which can be considered as an introduction of possibility, is mentioned in [26] as an alternative formulation, less efficient than the current system, including only the definitions for modal operators and the rule (TP) as the introduction of the $A\,\mathit{poss}$ judgment.

System $\mathcal{N}_{\mathsf{S4}}$ is defined by the following inference rules:

$$\frac{}{\Delta|\Gamma, A; \Gamma' \vdash_{\mathcal{N}_{\mathsf{S4}}} A\,\mathit{true}}\ (\textsc{Thyp}) \qquad \frac{}{\Delta, A; \Delta'|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} A\,\mathit{true}}\ (\textsc{Vhyp})$$

$$\frac{\Delta|\Gamma, A \vdash_{\mathcal{N}_{\mathsf{S4}}} B\,\mathit{true}}{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} A \to B\,\mathit{true}}\ (\to\mathrm{I}) \qquad \frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} A \to B\,\mathit{true} \qquad \Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} A\,\mathit{true}}{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} B\,\mathit{true}}\ (\to\mathrm{E})$$

$$\frac{\Delta|\cdot \vdash_{\mathcal{N}_{\mathsf{S4}}} A\,\mathit{true}}{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} \Box A\,\mathit{true}}\ (\Box\mathrm{I}) \qquad \frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} \Box A\,\mathit{true} \qquad \Delta, A|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} C\,\mathit{true}}{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} C\,\mathit{true}}\ (\Box\mathrm{E})$$

$$\frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} \Box A\,\mathit{true} \qquad \Delta, A|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} C\,\mathit{poss}}{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} C\,\mathit{poss}}\ (\Box\text{E-}\textsc{Poss})$$

$$\frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} A\,\mathit{true}}{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} A\,\mathit{poss}}\ (\mathrm{TP}) \qquad \frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} A\,\mathit{poss}}{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} \Diamond A\,\mathit{true}}\ (\Diamond\mathrm{I})$$

$$\frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} \Diamond A\,\mathit{true} \qquad \Delta|A \vdash_{\mathcal{N}_{\mathsf{S4}}} C\,\mathit{poss}}{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} C\,\mathit{poss}}\ (\Diamond\mathrm{E})$$

We have two starting rules corresponding to both types of hypotheses, they are stated in the most general way allowing to infer any formula that belongs to a context, not only the first or the last one. The rule for introduction of necessity ($\Box$ I) exactly captures the definition of validity through a categorical judgment, whilst the rule of necessity elimination ($\Box$ E) behaves as a substitution or cut rule where the formula $\Box A$ is used as lemma A in the valid hypotheses in order to prove C.

The judgment $A\,poss$ is explained with a combination of valid and true judgments by the rules ($\Box$E-Poss), (TP), ($\Diamond$ I) and ($\Diamond$ E). The second elimination rule for the $\Box$ operator is given in order to conclude a local truth as $C\,poss$, this rule takes advantage of a lemma of the form $\Box A\,true$. The introduction and elimination rules for the $\Diamond$ operator are indeed the definition of possibility given in [26].

Let us show next the deduction of axiom $\Diamond\mathbb{K}$, leaving the other axioms of section 2 to the reader (see the corresponding proof-terms in [26, Section 6.2]).

The sequent $\cdot\,|\cdot \vdash_{\mathcal{N}_{\mathsf{S4}}} \Box(A \to B) \to (\Diamond A \to \Diamond B)\ true$ is derivable in $\mathcal{N}_{\mathsf{S4}}$.

1.	$A \to B \mid A \vdash_{\mathcal{N}_{\mathsf{S4}}}$	$A \to B\ true$	(Vhyp)
2.	$A \to B \mid A \vdash_{\mathcal{N}_{\mathsf{S4}}}$	$A\ true$	(Thyp)
3.	$A \to B \mid A \vdash_{\mathcal{N}_{\mathsf{S4}}}$	$B\ true$	($\to$ E) $1, 2$
4.	$A \to B \mid A \vdash_{\mathcal{N}_{\mathsf{S4}}}$	$B\ poss$	(TP) 3
5.	$A \to B \mid \Box(A \to B), \Diamond A \vdash_{\mathcal{N}_{\mathsf{S4}}}$	$\Diamond A\ true$	(Thyp)
6.	$A \to B \mid \Box(A \to B), \Diamond A \vdash_{\mathcal{N}_{\mathsf{S4}}}$	$B\ poss$	($\Diamond$E) 5
7.	$A \to B \mid \Box(A \to B), \Diamond A \vdash_{\mathcal{N}_{\mathsf{S4}}}$	$\Diamond B\ true$	($\Diamond$I) 6
8.	$\cdot \mid \Box(A \to B), \Diamond A \vdash_{\mathcal{N}_{\mathsf{S4}}}$	$\Box(A \to B)\ true$	(Thyp)
9.	$\cdot \mid \Box(A \to B), \Diamond A \vdash_{\mathcal{N}_{\mathsf{S4}}}$	$\Diamond B\ true$	($\Box$E) $7, 8$
10.	$\cdot \mid \Box(A \to B) \vdash_{\mathcal{N}_{\mathsf{S4}}}$	$\Diamond A \to \Diamond B\ true$	($\to$ I) 9
11.	$\cdot \mid \cdot \vdash_{\mathcal{N}_{\mathsf{S4}}}$	$\Box(A \to B) \to (\Diamond A \to \Diamond B)\ true$	($\to$ I) 10

3.1 Admissible rules in $\mathcal{N}_{\mathsf{S4}}$

The next statements are an abridge presentation of the structural rules included in our formalization. In there, the admissible rules here presented (and others like exchange) are similar statements formulated for valid and true contexts combined with true and possible conclusions.

Lemma 3.1 (Weakening)**.** *The following rules are admissible*

$$\frac{\Delta|\Gamma;\Gamma' \vdash_{\mathcal{N}_{\mathsf{S4}}} J}{\Delta|\Gamma, B;\Gamma' \vdash_{\mathcal{N}_{\mathsf{S4}}} J}\ (\textsc{Weak-THyps}) \qquad\qquad \frac{\Delta;\Delta'|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J}{\Delta, B;\Delta'|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J}\ (\textsc{Weak-VHyps})$$

Proof. The rules are proved by structural induction on the given derivation. □

Next we prove that rules $(\to I)$ and $(\Diamond I)$ are invertible.

Lemma 3.2 (Inversion Introduction rules)**.** *The following rules are admissible*

$$\frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} A \to B\ true}{\Delta|\Gamma, A \vdash_{\mathcal{N}_{\mathsf{S4}}} B\ true}\ (\textsc{Det}) \qquad\qquad \frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} \Diamond A\ true}{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} A\ poss}\ (\Diamond\ \textsc{I-Inv})$$

Proof. The rule of detachment (Det) is a direct consequence of weakening and ($\to$ E). The inversion of $\Diamond$-introduction is proved using rules (TP) and ($\Diamond$ E). □

The next lemma presents some generalizations for contexts of the weakening rules of lemma 3.1.

Lemma 3.3 (Structural context rules). *The following rules are admissible*

- *Context Weakening:*

$$\frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J}{\Delta|\Gamma;\Gamma' \vdash_{\mathcal{N}_{\mathsf{S4}}} J}\ (\textsc{TCtx-WeakR}) \qquad \frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J}{\Delta|\Gamma';\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J}\ (\textsc{TCtx-WeakL})$$

$$\frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J}{\Delta;\Delta'|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J}\ (\textsc{VCtx-WeakR}) \qquad \frac{\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J}{\Delta';\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J}\ (\textsc{VCtx-WeakL})$$

Proof. Each weakening rule is proved by induction on the context Γ', respectively Δ'. □

We can now prove a generalization of the implication introduction rule that allows to discharge any true hypotheses.

Lemma 3.4 (Generalized Implication Introduction). *The following rule is admissible:*

$$\frac{\Delta|\Gamma, A;\Gamma' \vdash_{\mathcal{N}_{\mathsf{S4}}} B\ \mathit{true}}{\Delta|\Gamma;\Gamma' \vdash_{\mathcal{N}_{\mathsf{S4}}} A \to B\ \mathit{true}}\ (\textsc{Gen} \to \mathrm{I})$$

Proof. Induction on Γ'. □

3.2 Formula transference between contexts

We discuss next a result not present in [26][3], namely a transfer process between contexts. This is an inference principle that captures the fact that valid formulas are necessary truths, meaning that a formula A belonging to a valid context can be considered as a necessary truth. This is achieved by deleting A from the context of valid assumptions, while adding $\Box A$ to the context of true hypothesis. On the other direction, we can get rid of a boxed formula in the true assumptions context by moving it without the box to the valid assumptions context. Thus converting a boxed hypothesis into a pure propositional one. This transfer process provides an important tool for the actual development of derivations, one that allows to replace a modal reasoning about $\Box$ by a pure propositional one, thus considerably simplifying the actual construction of proofs.

Proposition 3.1 (Valid formulas are necessary truths). *The following is an admissible rule*

$$\frac{\Delta, A\,;\Delta'|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J}{\Delta;\Delta'|\Gamma, \Box A \vdash_{\mathcal{N}_{\mathsf{S4}}} J}\ (\textsc{ValToTrue})$$

Proof. Induction on Δ'. □

We can iterate the application of the above property in such a way that the context of valid formulas becomes empty, this option is not adequate for actual proof construction in $\mathcal{N}_{\mathsf{S4}}$, but

[3] Although one could argue that this result is implicit in the dual context approach coming from exponentials in linear logic, see [1].

plays an important role in the desired equivalence proof of our deductive systems. To formalize this iteration process, let us first give a convenient definition.

Definition 3.1. *Given a context* $\Sigma = [A_0, \dots, A_n]$ *we define the boxed context* $\Sigma^{\Box}$ *as* $\Sigma^{\Box} = [\Box A_0, \dots, \Box A_n]$

Corollary 3.1. *If* $\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J$ *then* $\cdot|\Delta^{\Box}; \Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J$

As another corollary we obtain a rule that allows for the discharge of valid hypotheses.

Corollary 3.2 (Implication introduction for validity)**.** *Let* Δ, Γ *be contexts and* A, B *be propositions. The following rule is admissible:*

$$\frac{\Delta, A; \Delta'|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} B\ \mathit{true}}{\Delta; \Delta'|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} \Box A \to B\ \mathit{true}}\ (\to\mathrm{I\ V{\small AL}})$$

Proof. Induction on Δ'. □

The above rule seems to be important for some special interpretations of the conditional, as in the case of lax logic where the lax implication can be defined as $\Box A \to B$ (see [26, Section 7]). Furthermore, the rule is invertible according to the following

Proposition 3.2 (Detachment for boxed formulas)**.** *The following rule is admissible:*

$$\frac{\Delta; \Delta'|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} \Box A \to B\ \mathit{true}}{\Delta, A; \Delta'|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} B\ \mathit{true}}\ (\Box\ \mathrm{D{\small ET}})$$

Proof. Use $(\to E)$, $(\Box I)$ and weakening. □

This proposition allows to prove the following version of the inverse rule of Proposition 3.1.

Proposition 3.3 (Necessary truths are valid)**.** *Let* Δ, Γ, Γ' *be contexts,* A *be proposition and* J *be a judgment. The following rule is admissible*

$$\frac{\Delta|\Gamma, \Box A\,; \Gamma' \vdash_{\mathcal{N}_{\mathsf{S4}}} J}{\Delta, A|\Gamma; \Gamma' \vdash_{\mathcal{N}_{\mathsf{S4}}} J}\ (\mathrm{T{\small RUE}T{\small O}V{\small AL}})$$

Proof. Induction on Γ'. □

Together propositions 3.1 and 3.3 provide the formula transfer principle between contexts.

4 Equivalence

We come to our main contribution, a proof of the equivalence between the natural deduction system $\mathcal{N}_{\mathsf{S4}}$ and its axiomatic counterpart $\mathcal{H}_{\mathsf{S4}}$.

4.1 From $\mathcal{H}_{\mathsf{S4}}$ to $\mathcal{N}_{\mathsf{S4}}$

The translation of Hilbert-style to dual natural deduction proofs is straightforward. The proof transformation consists mainly in substituting every occurrence of an axiom for its explicit derivation in natural deduction. Moreover, as expected, the translation of a $\mathcal{H}_{\mathsf{S4}}$-sequent will be a $\mathcal{N}_{\mathsf{S4}}$-sequent whose context of valid hypotheses is empty. In our case, we also need weakening structural rules in $\mathcal{N}_{\mathsf{S4}}$ (lemmas 3.1 and 3.3), due to the fact that in $\mathcal{H}_{\mathsf{S4}}$ the (MP) rule is multiplicative whereas the ($\to$ E) rule of $\mathcal{N}_{\mathsf{S4}}$ is additive (context sharing).

Theorem 4.1 (From axiomatic to natural deduction proofs)**.** *If* $\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A$ *then* $\cdot|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} A\, \mathit{true}$*.*

Proof. Induction on $\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} A$. □

A straightforward corollary makes explicit the translation of a $\Diamond$-formula.

Corollary 4.1. *If* $\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} \Diamond A$ *then* $\cdot|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} A\, \mathit{poss}$*.*

4.2 From $\mathcal{N}_{\mathsf{S4}}$ to $\mathcal{H}_{\mathsf{S4}}$

Now we prove the translation of natural deduction proofs to axiomatic derivations. The idea is to follow Corollary 3.1 to empty the validity context, thus getting only a context of true assumptions which can be directly managed in $\mathcal{H}_{\mathsf{S4}}$.

Theorem 4.2 (From natural deduction to axiomatic proofs)**.** *If* $\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J$ *then* $\Delta^{\Box};\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} J^t$ *where* J^t *is defined as* $(A\, \mathit{true})^t = A$ *and* $(A\, \mathit{poss})^t = \Diamond A$*.*

Proof. Induction on $\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} J$. Due to lack of space we only show the case for ($\Diamond$E). Let us assume that $\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} C\, \mathit{poss}$ comes from $\Delta|\Gamma \vdash_{\mathcal{N}_{\mathsf{S4}}} \Diamond A\, \mathit{true}$ and $\Delta|A \vdash_{\mathcal{N}_{\mathsf{S4}}} C\, \mathit{poss}$. Our goal is to show $\Delta^{\Box};\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} \Diamond C$. By the axiom $\Diamond 4$ it suffices to show $\Delta^{\Box};\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} \Diamond\Diamond C$. By using the I.H $\Delta^{\Box};\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} \Diamond A$, and thanks to the rules (MP) and (Ctx-cont), it is enough to show $\Delta^{\Box};\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} \Diamond A \to \Diamond\Diamond C$. But this sequent is consequence of the axiom $\Diamond\mathbb{K}$ and the sequent $\Delta^{\Box};\Gamma \vdash_{\mathcal{H}_{\mathsf{S4}}} \Box(A \to \Diamond C)$, which is derivable from the I.H. $\Delta^{\Box};A \vdash_{\mathcal{H}_{\mathsf{S4}}} \Diamond C$ by the deduction theorem and the rule (GenNec) of general neccesitation. □

5 Closing remarks

In this paper we discussed the equivalence of two formal systems for the modal logic S4, namely the axiomatic system $\mathcal{H}_{\mathsf{S4}}$ inspired by [12] and the natural deduction system $\mathcal{N}_{\mathsf{S4}}$ from [26]. The former a Hilbert-style system incorporating the notion of derivability from assumptions to solve the controversy around the provability of the deduction theorem in modal logic. The latter, a natural deduction formalism in sequent form influenced by Martin-Löf's notions of valid, true and possible propositions inside hypothetical judgments. To the best of our knowledge, this equivalence has not been addresed before in a dedicated manner, although there are works whose goals indirectly force to define deductive systems and their equivalence proofs. For instance the Coq formalization of Litak, et al. [19] or the work of Kobayashi [16] whose methods, employing the sophisticated machinery of category theory and even introducing new concepts like that of $\mathcal{L}$-strong monad, are far from elementary. As showed here, we are interested in proof translations and hence a direct equivalence proof is more suitable to reach this goal. Moreover, a semantic approach to prove equivalence between a dual calculus and an axiomatic system require the definition and development of the particular semantics for the dual calculus which are not available. There are only categorical foundations as given by Kavvos [14].

All the exposed work has been verified using the Coq proof assistant. Two main choices gave guideline to complete this paper and its formal verification. On one hand the implementation of hypotheses collections using a simple list data structure, instead of sticking to sets or multisets, which require more sophisticated data structures that complicate not only the automation but the correspondence with the paper proofs. On the other hand to reconcile a high-level reasoning at the mathematical level, with low-level procedures related to interactive proof-development. These choices originated the proof approach taken here, which allowed to present mathematical arguments involving some uncommon proof advances like the use of induction on contexts to show the admissibility of structural rules instead of the structural induction on derivations which is the preferred proof methodology in the literature. Related developments of interest involve the connections with linear logic [18], the TWELF implementation of lax logic available in `http://twelf.org/wiki/Lax_logic` and some work around the S5 logic with classic [25] and intuitionistic [24] approaches.

A forthcoming line of research consists on the study of alternative rules for manipulate and ease the proofs of possibility judgments. For instance, an analogous rule to (→ I), where the conclusion is a possibility judgment, would provide a way to introduce a hypothesis to such kind of conclusions. Another future research thread of our interest is related to the design of deductive systems adequate for interactive proof-search, along the lines of [27, Chapter 4].

Acknowledgments

We appreciate the valuable feedback of an anonymous referee enhancing the contents of this paper and pointing to related work and formalizations.

References

[1] Andrew G. Barber. Dual intuitionistic linear logic. Technical Report LFCS-96-347, University of Edinburgh, 1996.

[2] Eduardo Bonelli and Federico Feller. The logic of proofs as a foundation for certifying mobile computation. In *Logical Foundations of Computer Science, International Symposium, LFCS 2009, Deerfield Beach, FL, USA, January 3-6, 2009. Proceedings*, pages 76–91, 2009.

[3] Ranald Clouston. Fitch-style modal lambda calculi. *CoRR*, abs/1710.08326, 2017.

[4] Rowan Davies and Frank Pfenning. A modal analysis of staged computation. *J. ACM*, 48(3):555–604, 2001.

[5] Liesbeth De Mol. The proof is in the process: A preamble for a philosophy of computer-assisted mathematics. In *New Directions in the Philosophy of Science*, pages 15–33. 2014.

[6] Lourdes del Carmen González-Huesca, Favio E. Miranda-Perea, and P. Selene Linares-Arévalo. On the equivalence of two characterizations of constructive necessity, a formal verification. Submitted to Journal of Applied Non-Classical Logics, 2019.

[7] Matt Fairtlough and Michael Mendler. Propositional lax logic. *Inf. Comput.*, 137(1):1–33, 1997.

[8] M. Fitting. *Proof Methods for Modal and Intuitionistic Logics*. Synthese Library. Springer Netherlands, 1983.

[9] M. C. Fitting. Modal proof theory. In P. Blackburn, J. van Benthem, and F. Wolter, editors, *Handbook of Modal Logic*, volume 3 of *Studies in Logic and Practical Reasoning*, pages 85–138. Elsevier, Amsterdam, 2007.

[10] James W. Garson. *Modal Logic for Philosophers*. Cambridge University Press, 2006.

[11] Neil Ghani, Valeria de Paiva, and Eike Ritter. Explicit substitutions for constructive necessity. In *Automata, Languages and Programming, 25th International Colloquium, ICALP'98, Aalborg, Denmark, July 13-17, 1998, Proceedings*, pages 743–754, 1998.

[12] Raul Hakli and Sara Negri. Does the deduction theorem fail for modal logic? *Synthese*, 187(3):849–867, 2012.

[13] Andrzej Indrzejczak. *Natural Deduction, Hybrid Systems and Modal Logics*. Springer Publishing Company, Incorporated, 1st edition, 2010.

[14] G. A. Kavvos. The many worlds of modal λ-calculi: I. curry-howard for necessity, possibility and time. *CoRR*, abs/1605.08106, 2016.

[15] G. A. Kavvos. Dual-context calculi for modal logic. In *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017*, pages 1–12, 2017.

[16] Satoshi Kobayashi. Monad as modality. *Theor. Comput. Sci.*, 175(1):29–74, mar 1997.

[17] J.K.J. Konyndyk. *Introductory Modal Logic.* University of Notre Dame Press, 1986.

[18] Olivier Laurent. Preliminary report on the Yalla library. Technical report, Université Claude Bernard Lyon 1, 2018. https://perso.ens-lyon.fr/olivier.laurent/yalla/.

[19] Tadeusz Litak, Miriam Polzer, and Ulrich Rabenstein. Negative translations and normal modality. In *2nd International Conference on Formal Structures for Computation and Deduction, FSCD 2017, September 3-9, 2017, Oxford, UK*, pages 27:1–27:18, 2017.

[20] Pablo López, Frank Pfenning, Jeff Polakow, and Kevin Watkins. Monadic concurrent linear logic programming. In *Proceedings of the 7th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming, July 11-13 2005, Lisbon, Portugal*, pages 35–46, 2005.

[21] P. Martin-Löf and G. Sambin. *Intuitionistic type theory.* Studies in proof theory. Bibliopolis, 1984.

[22] Per Martin-Löf. On the meanings of the logical constants and the justifications of the logical laws. *Nordic J. Philos. Logic*, 1(1):11–60, 1996.

[23] Simone Martini and Andrea Masini. A modal view of linear logic. *The Journal of Symbolic Logic*, 59(3):888–899, 1994.

[24] Agata Murawska. Intuitionistic modal logic is5. Master's thesis, University of Wrocłlaw, 2013.

[25] Tom Murphy VII, Karl Crary, and Robert Harper. Distributed control flow with classical modal logic. In Luke Ong, editor, *Computer Science Logic*, pages 51–69, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[26] Frank Pfenning and Rowan Davies. A judgmental reconstruction of modal logic. *Mathematical Structures in Comp. Sci.*, 11(4):511–540, 2001.

[27] Jan von Plato. *Elements of Logical Reasoning.* Cambridge University Press, 2014.

[28] Francesca Poggiolesi. *Gentzen Calculi for Modal Propositional Logic.* Trends in Logic. Springer Netherlands, 2010.

[29] Alex K. Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic.* PhD thesis, University of Edinburgh, 1994.

[30] Morten Heine Sørensen and Pawel Urzyczyn. *Lectures on the Curry-Howard Isomorphism, Volume 149 (Studies in Logic and the Foundations of Mathematics).* Elsevier Science Inc., New York, NY, USA, 2006.

[31] Martin Sticht. *Proof Search in Multi-Agent Dialogues for Modal Logic.* PhD thesis, University of Bamberg Press, Universitätsbibliothek Bamberg, 2018. doctoralthesis.

[32] A. S. Troelstra. Introductory note to 19s3f. In K. Gödel and S. Feferman, editors, *Kurt Gödel: Collected Works: Volume I: Publications 1929-1936*, Collected Works, pages 296–303. OUP USA, 1986.

[33] Luca Viganò. *Labelled Non-Classical Logics.* Springer Science & Business Media, 2000.

[34] Tom Murphy VII, Karl Crary, Robert Harper, and Frank Pfenning. A symmetric modal lambda calculus for distributed computing. In *19th IEEE Symposium on Logic in Computer Science (LICS 2004), 14-17 July 2004, Turku, Finland, Proceedings*, pages 286–295, 2004.