On the Complexity of the Disjunction Property in Intuitionistic and Modal Logics

MAURO FERRARI and CAMILLO FIORENTINI
Università degli Studi di Milano
and
GUIDO FIORINO
Università degli Studi di Milano-Bicocca

In this article we study the complexity of disjunction property for intuitionistic logic, the modal logics **S4**, **S4.1**, Grzegorczyk logic, Gödel-Löb logic, and the intuitionistic counterpart of the modal logic **K**. For **S4** we even prove the feasible interpolation theorem and we provide a lower bound for the length of proofs. The techniques we use do not require proving structural properties of the calculi in hand, such as the cut-elimination theorem or the normalization theorem. This is a key point of our approach, since it allows us to treat logics for which only Hilbert-style characterizations are known.

Categories and Subject Descriptors: F.4.1 [**Mathematical Logic and Formal Languages**]: Mathematical Logic—*Modal logic; proof theory*; F.2.2 [**Analysis of Algorithms and Problem Complexity**]: Nonnumerical Algorithms and Problems—*Complexity of proof procedures*

General Terms: Theory, Algorithms

Additional Key Words and Phrases: Intuitionistic logic, modal logic, proof-length, feasible interpolation

1. INTRODUCTION

In the last years there has been a growing interest in studying the complexity of logical proofs. So far, the main issues have been concerned with the length of classical propositional proofs, a problem related to the $NP \neq coNP$ question [Buss 1999; Krajíček 1995; Pudlák 1999]. Recently, some studies [Buss and Mints 1999; Buss and Pudlák 2001; Ferrari et al. 2002] have also been devoted to the *complexity* of some properties of intuitionistic logic, in particular the

Authors' current addresses: M. Ferrari, DICOM, Università degli Studi dell'Insubria, Via Mazzini 5, 21100 Varese, Italy; email: mauro.ferrari@uninsubria.it; C.Fiorentini, Dipartimento di Scienze dell'Informazione, Università degli Studi di Milano, Via Comelico 39/41, 20135 Milan, Italy; email: fiorentini@dsi.unimi,it; G. Fiorino, Dipartimento di Metodi Quantitativi, Università degli Studi di Milano-Bicocca, Via P. dell'Ateneo Nuovo 1, 20126 Milan, Italy; email: guido.fiorino@unimib.it

disjunction property ($A \vee B \in$ **Int** implies $A \in$ **Int** or $B \in$ **Int**). In Buss and Mints [1999] and Buss and Pudlák [2001], it was proved that Intuitionistic Logic enjoys *the feasible disjunction property*: there exist a calculus **C** for **Int** and an algorithm $\mathcal{A}$ such that, given a proof π of **C** of the formula $A \vee B$, $\mathcal{A}$ provides either a proof of A or a proof of B in polynomial time in the size of π. In Buss and Mints [1999] the result was proved for **C** as a natural deduction calculus, while in Buss and Pudlák [2001] it was proved for **C** as a sequent calculus. In both cases the result essentially depends on structural properties of the proofs of the calculus in hand; indeed, in Buss and Mints [1999] it relied on a restricted version of the normalization theorem, whereas in Buss and Pudlák [2001] it was based on a particular form of the cut-elimination theorem. This prevents the possibility of applying these techniques to other logics, in particular to logics for which only Hilbert-style characterizations are known.

In this article we prove the feasible disjunction property for intuitionistic logic using a different technique based on a suitable *extraction calculus*, namely, a calculus that, processing the information implicitly contained in the proof of $A \vee B$, solves the disjunction property. In our approach there is a sharp separation between the calculus **C** in which the proof of $A \vee B$ is built, and the extraction calculus that solves the disjunction property. This makes our proof of the feasible disjunction property essentially independent of structural properties of **C**. This has some advantages: first of all, it allows us to get the result without proving cut-elimination or normalization; second, it allows us to extend the proof to calculi with "weak structural properties" such as Hilbert-style calculi, and hence to treat also logics for which only Hilbert-style characterizations are known. This framework has already been applied in Ferrari et al. [2002] to study the complexity of the disjunction property and the explicit definability property (the predicate counterpart of disjunction property) of some predicate intermediate logics.

Here, after having discussed the paradigmatic case of intuitionistic logic, we study the case of modal logics and intuitionistic modal logics. We recall that in the case of intuitionistic modal logics the disjunction property is defined as for intuitionistic logic. For a modal logic **L** deciding the disjunction property means to find out which between A and B is provable in **L** given a proof of $\Box A \vee \Box B$. In more detail, we study the case of the modal logics **S4**, **S4.1**, Grzegorczyk logic and Gödel-Löb logic [Chagrov and Zakharyaschev 1997] and the case of the intuitionistic modal logic **IK** (the result can be easily extended to the intuitionistic counterpart of other modal logics). The schema of the proof of the feasible disjunction theorem is the same for all these logics, even if we use different kinds of calculi. For **S4**, **S4.1** and Grzegorczyk logic we use a natural deduction calculus; in the case of Gödel-Löb logic and **IK** we use Hilbert-style calculi.

For **S4** we prove the feasible disjunction theorem also in presence of a particular class of assumptions (*modal Harrop assumptions*) and we get, as a corollary, the *feasible interpolation theorem*. As a remarkable consequence, along the lines of Buss and Pudlák [2001], we get a lower bound on the length of the proofs of **S4**.

2. EXTRACTION CALCULI

In this article we deal with different (propositional) languages. Given a language $\mathcal{L}$, a *sequent* is any expression of the form $\Gamma \vdash A$, where $A \in \mathcal{L}$ and Γ is a finite subset of $\mathcal{L}$; when Γ is empty we simply write $\vdash A$.

Here, we introduce the extraction calculus to decide the disjunction property for some logics. Although in this article we apply the extraction calculus to natural deduction proofs and Hilbert-style proofs, in its general formulation it can be applied to a great variety of calculi. For this reason the definition of extraction calculus is based on an abstract notion of proof and calculus which enables a uniform treatment of the subject (for a complete discussion we refer the reader to Ferrari and Fiorentini [2003] and Ferrari et al. [2003]).

A *proof* over the language $\mathcal{L}$ is any finite object π such that

(1) the (finite) set of formulas of $\mathcal{L}$ occurring in π is uniquely determined and nonempty;
(2) π proves a sequent $\Gamma \vdash A$, where Γ (possibly empty) is the set of *assumptions* of π, while A is the *consequence* of π.

The notation $\pi : \Gamma \vdash A$ means that $\Gamma \vdash A$ is the sequent proved by π. The *size* $\|\pi\|$ *of a proof* π is the number of symbols occurring in π, where a symbol is either a propositional variable or a logical constant. Given a finite set of proofs Π, the *size of* Π is $\|\Pi\| = \sum_{\pi \in \Pi} \|\pi\|$.

A *calculus* over $\mathcal{L}$ is a pair $(\mathbf{C}, [\cdot])$, where $\mathbf{C}$ is a recursive set of proofs over $\mathcal{L}$ and $[\cdot]$ is a recursive map associating with every proof of the calculus the set of its subproofs. We require $[\cdot]$ to satisfy the following natural conditions: $\pi \in [\pi]$ and, for every $\pi' \in [\pi]$, $[\pi'] \subseteq [\pi]$. We remark that any usual single conclusion inference system is a calculus according to our definition. With an abuse of notation we often identify a calculus $(\mathbf{C}, [\cdot])$ with the set $\mathbf{C}$ of its proofs.

Given $\Pi \subseteq \mathbf{C}$, $\mathrm{Seq}(\Pi) = \{\Gamma \vdash A \mid \text{there exists } \pi \in \Pi \text{ such that } \pi : \Gamma \vdash A \in \Pi\}$ is the set of the *sequents proved in* Π and $[\Pi] = \{\pi' \mid \text{there exists } \pi \in \Pi \text{ such that } \pi' \in [\pi]\}$ is the *closure under subproofs* of Π in the calculus $\mathbf{C}$.

An *inference rule* R is a relation between sequents of the kind

$$\frac{\Gamma_1 \vdash A_1 \ldots \Gamma_n \vdash A_n}{\Delta \vdash B}\,\mathrm{R},$$

where $\Gamma_1 \vdash A_1, \ldots, \Gamma_n \vdash A_n$ are the *premises* of the rule while $\Delta \vdash B$ is the *consequence*. An inference rule R is an *extraction rule*[1] *(e-rule) for* $\mathbf{C}$ iff

— R is an *admissible rule in* $\mathbf{C}$, that is $\{\Gamma_1 \vdash A_1, \ldots, \Gamma_n \vdash A_n\} \subseteq \mathrm{Seq}(\mathbf{C})$ implies $\Delta \vdash B \in \mathrm{Seq}(\mathbf{C})$;
— R can be *polynomially simulated in* $\mathbf{C}$; that is, there exists a polynomial time algorithm in the size of the input proofs that, given $\pi_1 : \Gamma_1 \vdash A_1, \ldots, \pi_n : \Gamma_n \vdash A_n$ of $\mathbf{C}$, builds a proof $\pi : \Delta \vdash B$ of $\mathbf{C}$.

[1]This definition is different from the one of Ferrari and Fiorentini [2003] and Ferrari et al. [2003] where the authors were interested in the logical complexity of extraction calculi instead of their computational complexity.

Let $\mathcal{R}$ be a recursive set of e-rules for $\mathbf{C}$ and let Π be a recursive set of proofs of $\mathbf{C}$; the closure of Seq([Π]) with respect to $\mathcal{R}$ gives rise to a calculus we call *extraction calculus*.

Definition 2.1 (*Extraction Calculus*). Given a recursive set $\mathcal{R}$ of e-rules for $\mathbf{C}$ and a recursive set $\Pi \subseteq \mathbf{C}$, the *extraction calculus for* Π, denoted by $\mathbb{ED}(\mathcal{R}, [\Pi])$, is defined as follows:

(1) If $\Gamma \vdash A \in \mathrm{Seq}([\Pi])$, then

$$\tau \equiv \frac{}{\Gamma \vdash A}$$

is a proof-tree of $\mathbb{ED}(\mathcal{R}, [\Pi])$ and τ proves $\Gamma \vdash A$.

(2) If $\tau_1 : \Gamma_1 \vdash A_1, \ldots, \tau_n : \Gamma_n \vdash A_n$ are proof-trees of $\mathbb{ED}(\mathcal{R}, [\Pi])$ and

$$\frac{\Gamma_1 \vdash A_1, \ldots, \Gamma_n \vdash A_n}{\Delta \vdash B}\,\mathrm{R}$$

is an e-rule of $\mathcal{R}$, then the proof-tree

$$\tau \equiv \frac{\tau_1 : \Gamma_1 \vdash A_1 \ \ldots \ \tau_n : \Gamma_n \vdash A_n}{\Delta \vdash B}\,\mathrm{R}$$

belongs to $\mathbb{ED}(\mathcal{R}, [\Pi])$ and τ proves $\Delta \vdash B$.

When Π consists of a single proof π, we simply denote the extraction calculus with $\mathbb{ED}(\mathcal{R}, [\pi])$.

In the sequel we show that, taking very "simple" e-rules, we obtain extraction calculi which allow us to solve (DP) in polynomial time. For instance, let $\mathcal{ND}_{\mathbf{Int}}$ be the natural deduction calculus for intuitionistic logic and let SLD be the following inference rule formalizing SLD-resolution:

$$\frac{\vdash A_1 \quad \ldots \quad \vdash A_n \quad A_1, \ldots, A_n \vdash B}{\vdash B}\,\mathrm{SLD},$$

where $A_1, \ldots, A_n, B$ are arbitrary formulas. It is easy to check that SLD is an e-rule for $\mathcal{ND}_{\mathbf{Int}}$. The proof of the *feasible disjunction property* for intuitionistic logic proceeds along the following lines. Let $\pi :\vdash A \vee B$ be a proof of $\mathcal{ND}_{\mathbf{Int}}$ and let us consider the extraction calculus $\mathbb{ED}(\mathrm{SLD}, [\pi])$.

—First, we show that $\mathbb{ED}(\mathrm{SLD}, [\pi])$ contains either a proof of $\vdash A$ or a proof of $\vdash B$ (to this aim we introduce a notion of *evaluation* of a formula in a calculus).

—Second, we exhibit a polynomial time strategy to generate all the proofs of $\mathbb{ED}(\mathrm{SLD}, [\pi])$. By the definition of e-rule, we get a polynomial time algorithm to construct either a proof $\pi_A :\vdash A$ or a proof $\pi_B :\vdash B$ of the calculus $\mathcal{ND}_{\mathbf{Int}}$.

For modal logics and intuitionistic modal logics the proof follows the same schema changing the involved e-rules and the notion of evaluation.

We remark that in the following, when SLD is applied, the rightmost sequent is an axiom of the extraction calculus. Hereafter we write

$$\overline{A_1, \ldots, A_n \vdash B}$$

to emphasize that $A_1, \ldots, A_n \vdash B$ is an axiom of the extraction calculus in hand.

To conclude this section, we notice that extraction calculi have been introduced in Ferrari and Fiorentini [2003] and Ferrari et al. [2003] to define a class

Table I. The Natural Deduction Calculus $\mathcal{ND}_{\mathbf{Int}}$ for Intuitionistic Logic

$$\frac{}{A \vdash A}\,\mathrm{Id} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash A}\,\bot_{\mathrm{Int}}$$

$$\frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \wedge B}\,\mathrm{I}\wedge \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,\mathrm{E}\wedge \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,\mathrm{E}\wedge$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,\mathrm{I}\vee \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,\mathrm{I}\vee \qquad \frac{\Gamma \vdash A \vee B \; \Delta, A \vdash C \; \Theta, B \vdash C}{\Gamma, \Delta, \Theta \vdash C}\,\mathrm{E}\vee$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\,\mathrm{I}\to \qquad \frac{\Gamma \vdash A \quad \Delta \vdash A \to B}{\Gamma, \Delta \vdash B}\,\mathrm{E}\to$$

of systems for which the disjunction property and the explicit definability property (given a proof of $\exists x A(x)$, find out a term t such that $A(t)$ is provable) can be decided using only information contained in a proof of $A \vee B$, respectively of $\exists x A(x)$. Extraction calculi have also been applied in the framework of program synthesis from formal proofs; see Avellone et al. [2001]; Ferrari et al. [1999].

3. PROPOSITIONAL INTUITIONISTIC LOGIC

In this section we study the case of propositional intuitionistic logic **Int**. Here we consider the language $\mathcal{L}$ of (propositional) *formulas* built up in the usual way starting from a denumerable set of propositional variables and the logical constants $\bot$, $\wedge$, $\vee$, and $\to$. We denote with $\mathcal{ND}_{\mathbf{Int}}$ the natural deduction calculus of Table I (see, e.g., Troelstra and Schwichtenberg [1996]). A proof π of $\mathcal{ND}_{\mathbf{Int}}$ is a tree of sequents built using the rules of Table I. The sequent proved by π is the lowest sequent of π; the notions of subproof of π and depth(π) are defined in the obvious way.

It is well known that **Int** meets the disjunction property (DP), that is, $A \vee B \in$ **Int** implies $A \in$ **Int** or $B \in$ **Int**. In Buss and Mints [1999] and Buss and Pudlák [2001] it was proved that (DP) can be decided in polynomial time in the size of a proof of $A \vee B$. Here we show an analogous result obtained with a different technique. In particular, given a proof $\pi :\vdash A \vee B$ of $\mathcal{ND}_{\mathbf{Int}}$, we exhibit an algorithm to construct a proof of $\vdash A$ or a proof of $\vdash B$ in the calculus $\mathcal{ND}_{\mathbf{Int}}$ in polynomial time in the size of π, using the extraction calculus $\mathbb{ID}(\mathrm{SLD}, [\pi])$.

To study the deductive power of $\mathbb{ID}(\mathrm{SLD}, [\pi])$, we introduce the following notion of evaluation:

Definition 3.1 (*Evaluation*). Given a set of proofs Π of a calculus **C** and a formula A, A is *evaluated* in Π (in symbols $\Pi \rhd A$) iff the following conditions hold:

(i) There exists a proof $\pi :\vdash A \in \Pi$.
(ii) One of the following inductive conditions holds:
  (a) A is a propositional variable;
  (b) $A \equiv B \wedge C$ and $\Pi \rhd B$ and $\Pi \rhd C$;

(c) $A \equiv B \vee C$ and either $\Pi \rhd B$ or $\Pi \rhd C$;
(d) $A \equiv B \to C$ and, if $\Pi \rhd B$, then $\Pi \rhd C$.

A set Γ of formulas is evaluated in Π, and we write $\Pi \rhd \Gamma$, if $\Pi \rhd A$ holds for every $A \in \Gamma$.

To show that either A or B is provable in $\mathbb{ID}(\text{SLD}, [\pi])$, it suffices to prove that $\mathbb{ID}(\text{SLD}, [\pi]) \rhd A \vee B$. The key point is the following lemma:

LEMMA 3.2. *Let Π be a recursive set of proofs of $\mathcal{ND}_{\mathbf{Int}}$. For every $\pi : \Gamma \vdash A$ belonging to $[\Pi]$, if $\mathbb{ID}(\text{SLD}, [\Pi]) \rhd \Gamma$ then $\mathbb{ID}(\text{SLD}, [\Pi]) \rhd A$.*

PROOF. Let us assume that $\Gamma = \{B_1, \ldots, B_n\}$ is evaluated in $\mathbb{ID}(\text{SLD}, [\Pi])$. By definition there exist in $\mathbb{ID}(\text{SLD}, [\Pi])$ the proofs $\tau_1 :\vdash B_1, \ldots, \tau_n :\vdash B_n$. Moreover, since $\Gamma \vdash A \in \text{Seq}([\Pi])$, then $\Gamma \vdash A$ is an axiom of $\mathbb{ID}(\text{SLD}, [\Pi])$; hence the proof

$$\frac{\tau_1 :\vdash B_1, \ldots, \tau_n :\vdash B_n \qquad \overline{\Gamma \vdash A}}{\vdash A}\text{SLD}$$

belongs to $\mathbb{ID}(\text{SLD}, [\Pi])$ (this is the only point requiring the use of SLD). This proves point (i) of Definition 3.1; to prove point (ii) we proceed by induction on $\text{depth}(\pi)$.

If $\text{depth}(\pi) = 0$, the only rule applied in π is an assumption introduction Id; hence $\Gamma = \{A\}$ and the assertion trivially holds. Let us suppose that $\text{depth}(\pi) = h + 1$. The proof goes on by cases according to the last rule applied in π; here we only discuss some representative cases.

Disjunction elimination:

$$\pi : \Gamma \vdash A \equiv \frac{\pi_0 : \Gamma_0 \vdash B_1 \vee B_2 \quad \pi_1 : \Gamma_1, B_1 \vdash A \quad \pi_2 : \Gamma_2, B_2 \vdash A}{\Gamma_0, \Gamma_1, \Gamma_2 \vdash A}\text{E}\vee.$$

Since $\mathbb{ID}(\text{SLD}, [\Pi]) \rhd \Gamma_0$, π_0 belongs to $[\Pi]$ and $\text{depth}(\pi_0) \leq h$, we get, by induction hypothesis, that $\mathbb{ID}(\text{SLD}, [\Pi]) \rhd B_1 \vee B_2$. Thus, there exists $i \in \{1, 2\}$ such that $\mathbb{ID}(\text{SLD}, [\Pi]) \rhd B_i$ and, since $\pi_i : \Gamma_i, B_i \vdash A$ belongs to $[\Pi]$, by induction hypothesis we have $\mathbb{ID}(\text{SLD}, [\Pi]) \rhd A$.

Implication introduction:

$$\pi : \Gamma \vdash A \equiv \frac{\pi' : \Gamma, B \vdash C}{\Gamma \vdash B \to C}\text{I}\to.$$

Let us assume that $\mathbb{ID}(\text{SLD}, [\Pi]) \rhd B$; since $\mathbb{ID}(\text{SLD}, [\Pi]) \rhd \Gamma$, π' belongs to $[\Pi]$ and $\text{depth}(\pi') \leq h$, by induction hypothesis we get $\mathbb{ID}(\text{SLD}, [\Pi]) \rhd C$. □

By the above lemma it follows that we can use the extraction calculus to solve (DP). Indeed, let $\pi :\vdash A \vee B$ be a proof of $\mathcal{ND}_{\mathbf{Int}}$. Since the empty set of formulas is trivially evaluated in $\mathbb{ID}(\text{SLD}, [\pi])$, by Lemma 3.2 we deduce that $\mathbb{ID}(\text{SLD}, [\pi]) \rhd A \vee B$. Hence, $\mathbb{ID}(\text{SLD}, [\pi]) \rhd A$ or $\mathbb{ID}(\text{SLD}, [\pi]) \rhd B$ and, by point (i) of Definition 3.1, at least one between the sequents $\vdash A$ and $\vdash B$ is provable in $\mathbb{ID}(\text{SLD}, [\pi])$. Thus:

THEOREM 3.3. *If $\pi :\vdash A \vee B$ is a proof of $\mathcal{ND}_{\mathbf{Int}}$, then either $\vdash A$ or $\vdash B$ is provable in $\mathbb{ID}(\text{SLD}, [\pi])$.*

One can prove that the calculus $\mathbb{ID}(\text{SLD}, [\pi])$ has the disjunction property, that is, for every $\vdash A \vee B$ provable in $\mathbb{ID}(\text{SLD}, [\pi])$, either $\vdash A$ or $\vdash B$ is provable in $\mathbb{ID}(\text{SLD}, [\pi])$ (see, e.g., Ferrari et al. [2003]).

To study the complexity of the disjunction property, we need to investigate the complexity of the extraction calculus. To this aim we define a strategy to generate all the proofs of the extraction calculus in polynomial time. Let SEQ be the set of all the sequents over $\mathcal{L}$; given a finite set of sequents Σ, the map $E_\Sigma : 2^{\text{SEQ}} \to 2^{\text{SEQ}}$ is defined as follows:

$$E_\Sigma(\Delta) = \{ \vdash A \mid B_1, \ldots, B_n \vdash A \in \Sigma \text{ and } \{\vdash B_1, \ldots, \vdash B_n\} \subseteq \Delta\}.$$

It is easy to check that E_Σ is a monotone and continuous operator on the complete partial order $\langle 2^{\text{SEQ}}, \subseteq \rangle$. Hence, by the Knaster-Tarsky theorem, E_Σ has the least fixpoint E_Σ^∞ and, by the Kleene theorem, $E_\Sigma^\infty = \bigcup_{k\in\omega} E_\Sigma^k$, where

$$\begin{aligned} E_\Sigma^0 &= \emptyset, \\ E_\Sigma^{k+1} &= E_\Sigma(E_\Sigma^k). \end{aligned}$$

Given a finite set of proofs Π of $\mathcal{ND}_{\mathbf{Int}}$, let $\Sigma = \text{Seq}([\Pi])$; it is immediate to check that $\vdash A$ is provable in $\mathbb{ID}(\text{SLD}, [\Pi])$ iff $\vdash A \in E_\Sigma^\infty$. Thus, we can generate proofs of $\mathbb{ID}(\text{SLD}, [\Pi])$ by repeatedly applying E_Σ. In the next theorem we show that this can be performed in polynomial time.

THEOREM 3.4. *Let Π be a finite set of proofs of $\mathcal{ND}_{\mathbf{Int}}$.*

(i) *There exists a polynomial time algorithm in $\|\Pi\|$ that, given Π, generates a proof $\tau_A : \vdash A$ of the calculus $\mathbb{ID}(\text{SLD}, [\Pi])$ for every sequent $\vdash A$ provable in $\mathbb{ID}(\text{SLD}, [\Pi])$.*

(ii) *There exists a polynomial time algorithm in $\|\Pi\|$ that, given Π, generates a proof $\pi_A : \vdash A$ of the calculus $\mathcal{ND}_{\mathbf{Int}}$ for every sequent $\vdash A$ provable in $\mathbb{ID}(\text{SLD}, [\Pi])$.*

PROOF

(i) We have to generate the sequence of E_Σ^k, with $\Sigma = \text{Seq}([\Pi])$, and, at each step k, a proof $\tau_A : \vdash A$ for every $\vdash A$ of E_Σ^k not already proved. At iteration $k+1$ we have to consider any sequent $B_1, \ldots, B_m \vdash A$ of Σ such that proofs $\tau_1 : \vdash B_1, \ldots, \tau_m : \vdash B_m$ have been already generated but no proof of $\vdash A$ has been built; we construct the proof $\tau_A : \vdash A$ by applying SLD. Note that the axioms of Σ of the form $\Gamma \vdash A$ will not be used in successive iterations; therefore, if $n = |\text{Seq}([\Pi])|$ we have that $E_\Sigma^n = E_\Sigma^\infty$. We can conclude that the algorithm works in time polynomial in $\|\Pi\|$.

(ii) Immediately follows from point (i) and the definition of e-rule. □

To summarize, given a proof $\pi : \vdash A \vee B$ of $\mathcal{ND}_{\mathbf{Int}}$, by Theorem 3.3 either $\vdash A$ or $\vdash B$ is provable in $\mathbb{ID}(\text{SLD}, [\pi])$; hence, by the previous theorem, a proof of $\vdash A$ or a proof of $\vdash B$ of $\mathcal{ND}_{\mathbf{Int}}$ can be constructed in polynomial time in the size of π. Therefore:

THEOREM 3.5. **Int** *has the feasible disjunction property.*

We point out that our technique does not require any manipulation of the proofs. We only use the fact that the proofs of the natural deduction calculus preserve evaluation of formulas (Lemma 3.2). This is not a peculiar feature of natural deduction calculi, but it also holds for other deductive systems for **Int** such as the sequent calculus of Buss and Pudlák [2001]. Thus the results of our article can be restated also for different calculi (possibly with different e-rules). We also notice that the result of Buss and Pudlák [2001] was based on an implicit extraction calculus using the e-rules cut and weakening. In this sense our result is an improvement of the one of Buss and Pudlák [2001], since SLD provides a better search strategy. On the other hand, our algorithm is essentially equivalent to the one exhibited in Buss and Mints [1999].

It is well known that the disjunction property does not hold in general under assumptions. On the other hand, it holds for sequents of the form $\Gamma \vdash A \vee B$ where Γ is a set of *Harrop formulas*, that is, formulas of the kind

$$H \ ::= \ p \mid \bot \mid H \wedge H \mid A \to H,$$

where p is a propositional variable and A is any formula. To treat the case of Harrop formulas, beside the e-rule SLD we need the e-rules RE$_\wedge$ (*restricted and elimination*) and RMP (*restricted modus ponens*)

$$\frac{\vdash H_1 \wedge H_2}{\vdash H_i}\text{RE}_\wedge \quad \text{with } i \in \{1,2\}, \qquad \frac{\vdash A \quad \vdash A \to H}{\vdash H}\text{RMP},$$

where H, H_1, and H_2 are Harrop formulas and A is any formula. As proved in Ferrari et al. [2002] (see also the discussion about *modal Harrop formulas* in Section 4.2), the feasible disjunction property also holds in presence of Harrop assumptions. That is:

THEOREM 3.6. *There exists a polynomial time algorithm that given a proof $\pi : \Gamma \vdash A \vee B$ of $\mathcal{ND}_{\mathbf{Int}}$, with Γ a set of Harrop formulas, constructs a proof $\pi_A : \Gamma \vdash A$ or a proof $\pi_B : \Gamma \vdash B$ of the calculus $\mathcal{ND}_{\mathbf{Int}}$.*

As proved in Buss and Pudlák [2001], the above theorem leads to the *feasible interpolation theorem* for intuitionistic logic:

THEOREM 3.7. *Given a proof $\pi : p_1 \vee \neg p_1, \ldots, p_n \vee \neg p_n \vdash B_0 \vee B_1$ of $\mathcal{ND}_{\mathbf{Int}}$, it is possible to construct a circuit $\mathcal{C}(\overline{p})$ whose size is polynomial in $\|\pi\|$ such that, for every $\overline{a} \in \{0,1\}^n$, if $\mathcal{C}(\overline{a}) = i$, then the formula $\tilde{B}_i$ obtained by substituting p_j with $\bot$ if $a_j = 0$ and p_j with $\bot \to \bot$ if $a_j = 1$, is a classical tautology.*

As a consequence, provided that $NP \cap coNP \not\subseteq P/poly$, there exist intuitionistic proofs whose size cannot be bounded by a polynomial in the size of the proved formula (see Buss and Pudlák [2001] or the analogous discussion for **S4** in Section 4.2).

4. MODAL LOGICS

In this section we focus on the disjunction property in some modal logics. Here we consider the language $\mathcal{L}_\Box$ built up on a denumerable set of propositional variables, the logical constants $\bot$, $\wedge$, $\vee$, $\to$ and the modal operator $\Box$; $\neg A$ is an abbreviation for $A \to \bot$. In the case of a modal logic **L**, the disjunction property

Table II. Natural Deduction Rules for **S4**

$$\frac{\Gamma \vdash \Box A}{\Gamma \vdash A}\,\mathrm{E}\Box \qquad \frac{\Box B_1, \ldots, \Box B_m \vdash A}{\Box B_1, \ldots, \Box B_m \vdash \Box A}\,\mathrm{I}\Box$$

(DP) is formulated as follows: if $\Box A \vee \Box B \in \mathbf{L}$ then either A or B belongs to $\mathbf{L}$. $\mathbf{L}$ has the *feasible disjunction property* iff there exist a calculus $\mathbf{C}$ for $\mathbf{L}$ and an algorithm $\mathcal{A}$ such that, given a proof $\pi : \vdash \Box A \vee \Box B$, $\mathcal{A}$ constructs either a proof $\pi_A : \vdash A$ or a proof $\pi_B : \vdash B$ in polynomial time in $\|\pi\|$.

Here we prove the feasible disjunction property for **S4**, **S4.1**, Grzegorczyk logic, and Gödel-Löb logic. In the case of **S4**, **S4.1**, and Grzegorczyk logic, we prove the result using a natural deduction calculus; for Gödel-Löb logic we exploit a Hilbert-style calculus. The calculi are defined by extending the natural deduction calculus $\mathcal{ND}_{\mathbf{Cl}}$ for classical logic, which is obtained by adding to the calculus $\mathcal{ND}_{\mathbf{Int}}$ of Table I the rule

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\,\bot_{\mathbf{Cl}}.$$

4.1 **S4** Logic

S4 is the modal logic obtained by adding to classical logic the axiom-schemata

$$\begin{aligned}(K) &\equiv \Box(p \to q) \to (\Box p \to \Box q),\\ (T) &\equiv \Box p \to p,\\ (4) &\equiv \Box p \to \Box\Box p.\end{aligned}$$

The natural deduction calculus $\mathcal{ND}_{\mathbf{S4}}$ for **S4** is obtained by adding to $\mathcal{ND}_{\mathbf{Cl}}$ the rules of Table II (see, e.g., Prawitz [1965]).

To prove the feasible disjunction property, we argue as in Section 3. Here we consider the rule

$$\frac{\vdash A_1 \quad \ldots \quad \vdash A_n \qquad \overline{\Box A_1, \ldots, \Box A_n \vdash B}}{\vdash B}\,\mathrm{SLD}\Box.$$

It is easy to check that SLD$\Box$ is an e-rule for $\mathcal{ND}_{\mathbf{S4}}$. We recall that **S4** does not enjoy the intuitionistic disjunction property due the presence of $\bot_{\mathbf{Cl}}$; thus we cannot prove the main lemma using the evaluation for **Int**. To treat **S4** we introduce a new notion of evaluation, which differs from the previous one because provability is only required for boxed formulas. We remark that the evaluation for **Int** does not work for **S4**; otherwise it would follow that **S4** has the intuitionistic disjunction property.

Definition 4.1 (**S4**-*Evaluation*). Given a set of proofs Π of a calculus $\mathbf{C}$ and a formula A, A is **S4**-*evaluated* in Π (in symbols $\Pi \rhd_{\mathbf{S4}} A$) iff one of the following inductive conditions holds:

(1) A is a propositional variable;
(2) $A \equiv B \wedge C$ and $\Pi \rhd_{\mathbf{S4}} B$ and $\Pi \rhd_{\mathbf{S4}} C$;
(3) $A \equiv B \vee C$ and either $\Pi \rhd_{\mathbf{S4}} B$ or $\Pi \rhd_{\mathbf{S4}} C$;
(4) $A \equiv B \to C$ and, if $\Pi \rhd_{\mathbf{S4}} B$ then $\Pi \rhd_{\mathbf{S4}} C$;
(5) $A \equiv \Box B$ and $\Pi \rhd_{\mathbf{S4}} B$ and there exists a proof $\tau : \vdash B \in \Pi$.

We remark that, since $\bot$ is not **S4**-evaluated in Π, $\Pi \rhd_{\mathbf{S4}} \neg A$ iff $\Pi \rhd_{\mathbf{S4}} A$ does not hold; this classical interpretation of $\neg$ is essential to treat the case of $\bot_{\mathbf{Cl}}$ in the following lemma. Given a set of formulas Γ, $\Pi \rhd_{\mathbf{S4}} \Gamma$ iff $\Pi \rhd_{\mathbf{S4}} A$ for every $A \in \Gamma$. The main step consists in proving that proofs of $\mathcal{ND}_{\mathbf{S4}}$ preserve **S4**-evaluation.

LEMMA 4.2. *Let Π be a recursive set of proofs of $\mathcal{ND}_{\mathbf{S4}}$. For every $\pi : \Gamma \vdash A$ belonging to $[\Pi]$, if $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} \Gamma$ then $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} A$.*

PROOF. The proof proceeds as in Lemma 3.2 by induction on the depth of π. The base case and the inductive cases corresponding to the rules for $\wedge, \vee, \rightarrow$ and the case of E$\Box$-rule easily follow from the definition of **S4**-evaluation (there is no need to apply e-rules). It remains to prove the cases of $\bot_{\mathbf{Cl}}$-rule and I$\Box$-rule.

$\bot_{\mathbf{Cl}}$*-rule*:

$$\pi : \Gamma \vdash A \equiv \frac{\pi' : \Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\bot_{\mathbf{Cl}}.$$

Let us assume that all the formulas in Γ are **S4**-evaluated in $\mathbb{ID}(\text{SLD}_\Box, [\Pi])$. If $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} \neg A$, by the induction hypothesis on π' it follows that $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} \bot$, against the definition of **S4**-evaluation. This implies that $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} \neg A$ does not hold; hence $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} A$.

I$\Box$*-rule*:

$$\pi : \Gamma \vdash A \equiv \frac{\pi' : \Box B_1, \ldots, \Box B_n \vdash C}{\Box B_1, \ldots, \Box B_n \vdash \Box C}\text{I}\Box.$$

If $\Box B_1, \ldots, \Box B_n$ are **S4**-evaluated in $\mathbb{ID}(\text{SLD}_\Box, [\Pi])$, there exist proofs $\tau_1 : \vdash B_1, \ldots, \tau_n : \vdash B_n$ in $\mathbb{ID}(\text{SLD}_\Box, [\Pi])$. Moreover, since the sequent $\Box B_1, \ldots, \Box B_n \vdash C$ belongs to Seq($[\Pi]$), the proof

$$\frac{\tau_1 : \vdash B_1, \ldots, \tau_n : \vdash B_n \qquad \overline{\Box B_1 \ldots \Box B_n \vdash C}}{\vdash C}\text{SLD}_\Box$$

belongs to $\mathbb{ID}(\text{SLD}_\Box, [\Pi])$. Finally, by induction hypothesis on π', C is **S4**-evaluated in $\mathbb{ID}(\text{SLD}_\Box, [\Pi])$; hence $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} \Box C$. □

Since the empty set of assumptions is trivially **S4**-evaluated, by the previous lemma and by the definition of **S4**-evaluation, we immediately get

THEOREM 4.3. *If $\pi : \vdash \Box A \vee \Box B$ is a proof of $\mathcal{ND}_{\mathbf{S4}}$, then either $\vdash A$ or $\vdash B$ is provable in $\mathbb{ID}(\text{SLD}_\Box, [\pi])$.*

Thus, we can exploit the extraction calculus to solve (DP) for **S4**. Now we study the complexity of the extraction calculus. Let SEQ be the set of all the sequents over $\mathcal{L}_\Box$ and let $E_\Sigma : 2^{\text{SEQ}} \rightarrow 2^{\text{SEQ}}$ be the map defined as follows:

$$E_\Sigma(\Delta) = \{\vdash B \mid \Box A_1, \ldots, \Box A_m \vdash B \in \Sigma \text{ and } \{\vdash A_1, \ldots, \vdash A_m\} \subseteq \Delta\}.$$

E_Σ is a monotone and continuous operator on the complete partial order $\langle 2^{\text{SEQ}}, \subseteq\rangle$; hence E_Σ has the least fixpoint E_Σ^∞. Given a finite set of proofs Π of $\mathcal{ND}_{\mathbf{S4}}$, let $\Sigma = \text{Seq}([\Pi])$; it is immediate to check that $\vdash A$ is provable in

$\mathbb{ID}(\text{SLD}_\Box, [\Pi])$ iff $\vdash A \in E^\infty_\Sigma$. We can proceed as in Theorem 3.4 and prove the following:

THEOREM 4.4. *Let Π be a finite set of proofs of $\mathcal{ND}_{\mathbf{S4}}$.*

(i) *There exists a polynomial time algorithm in $\|\Pi\|$ that, given Π, generates a proof $\tau_A : \vdash A$ of the calculus $\mathbb{ID}(\text{SLD}_\Box, [\Pi])$ for every sequent $\vdash A$ provable in $\mathbb{ID}(\text{SLD}_\Box, [\Pi])$.*

(ii) *There exists a polynomial time algorithm in $\|\Pi\|$ that, given Π, generates a proof $\pi_A : \vdash A$ of the calculus $\mathcal{ND}_{\mathbf{S4}}$ for every sequent $\vdash A$ provable in $\mathbb{ID}(\text{SLD}_\Box, [\Pi])$.*

Combining Theorems 4.3 and 4.4, we get the following:

THEOREM 4.5. **S4** *has the feasible disjunction property.*

4.2 **S4** with Assumptions

Here we investigate the disjunction property for proofs of $\mathcal{ND}_{\mathbf{S4}}$ with assumptions. We introduce a class of formulas we call *modal Harrop formulas*, which behave as Harrop formulas in intuitionistic logic. Formally, a modal Harrop formula is any formula H of the kind

$$H \ ::= \ p \mid \bot \mid H \wedge H \mid \Box A \rightarrow H \mid \Box H,$$

where p is a propositional variable and A is any formula. Note that by translating Harrop formulas according to the $^\circ$ modal embedding of Troelstra and Schwichtenberg [1996], we obtain modal Harrop formulas.

For technical reasons, instead of considering natural deduction proofs with modal Harrop formulas as open assumptions, we introduce Harrop formulas as axioms of the calculus. Given a recursive set $\mathbf{H}$ of modal Harrop formulas, we denote with $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$ the natural deduction calculus obtained by adding the axiom-rule

$$\frac{}{\vdash H}\,\text{H}\in\mathbf{H}$$

to $\mathcal{ND}_{\mathbf{S4}}$. We remark that, given a set $\mathbf{H} = \{H_1, \ldots, H_n\}$ of modal Harrop formulas, there exists a trivial one-to-one translation between proofs $\pi : H_1, \ldots, H_n \vdash A$ of $\mathcal{ND}_{\mathbf{S4}}$ and proofs $\pi' : \vdash A$ of $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$.

We extend the extraction calculus of the previous section with the rules $\text{RME}_\wedge$ (*restricted modal $\wedge$ elimination*), RMMP (*restricted modal modus ponens*), and $\text{RE}_\Box$ (*restricted $\Box$ elimination*)

$$\frac{\vdash H_1 \wedge H_2}{\vdash H_i}\,\text{RME}_\wedge \text{ with } i \in \{1,2\}, \qquad \frac{\vdash A \quad \vdash \Box A \rightarrow H}{\vdash H}\,\text{RMMP}, \qquad \frac{\vdash \Box H}{\vdash H}\,\text{RE}_\Box,$$

where H, H_1, and H_2 are modal Harrop formulas and A is any formula. It is immediate to check that $\text{RME}_\wedge$, RMMP and $\text{RE}_\Box$ are e-rules for $\mathcal{ND}_{\mathbf{S4}}$.

Given a recursive set of proofs Π of $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$, we denote with $\mathbb{ID}_{\mathbf{S4}^+}([\Pi])$ the extraction calculus $\mathbb{ID}(\{\text{SLD}_\Box, \text{RME}_\wedge, \text{RMMP}, \text{RE}_\Box\}, [\Pi])$. First we have to show that the modal Harrop axioms added to $\mathcal{ND}_{\mathbf{Int}}$ are actually **S4**-evaluated in $\mathbb{ID}_{\mathbf{S4}^+}([\Pi])$. This is a consequence of the following lemma.

LEMMA 4.6. *Let* $\mathbf{H}$ *be a recursive set of modal Harrop formulas, let* Π *be a recursive set of proofs of* $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$ *and let us suppose that* $\vdash \bot$ *is not provable in* $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$. *For every modal Harrop formula* H, *if* $\vdash H$ *is provable in* $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$, *then* $\mathbb{D}_{\mathbf{S4}^+}([\Pi]) \rhd_{\mathbf{S4}} H$.

PROOF. Let $\vdash H$ be provable in $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$; we prove that H is **S4**-evaluated by induction on the structure of H. By hypothesis $H \not\equiv \bot$. If H is a propositional variable, the assertion immediately follows. If $H \equiv H_1 \wedge H_2$ the assertion follows by the closure of $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$ with respect to the e-rule $\text{RME}_\wedge$ and by the induction hypothesis. The case $H \equiv \Box K$ is similar and requires the e-rule $\text{RE}_\Box$. Let $H \equiv \Box A \to K$ and suppose that $\mathbb{D}_{\mathbf{S4}^+}([\Pi]) \rhd_{\mathbf{S4}} \Box A$. By definition, $\vdash A$ is provable in $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$. By applying the e-rule RMMP, it follows that $\vdash K$ is provable in $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$. Since K is a modal Harrop formula, by induction hypothesis we get $\mathbb{D}_{\mathbf{S4}^+}([\Pi]) \rhd_{\mathbf{S4}} K$. □

We can prove the main lemma about **S4**-evaluation.

LEMMA 4.7. *Let* $\mathbf{H}$ *be a recursive set of modal Harrop formulas, let* Π *be a recursive set of proofs of* $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$, *and let us suppose that* $\vdash \bot$ *is not provable in* $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$. *For every proof* $\pi : \Gamma \vdash A$ *belonging to* $[\Pi]$, *if* $\mathbb{D}_{\mathbf{S4}^+}([\Pi]) \rhd_{\mathbf{S4}} \Gamma$ *then* $\mathbb{D}_{\mathbf{S4}^+}([\Pi]) \rhd_{\mathbf{S4}} A$.

PROOF. The proof is similar to the one given for Lemma 4.2. We only have to consider the case in which π consists of an axiom-rule. In this case $\Gamma = \emptyset$ and A is a modal Harrop formula; since $\vdash A \in \text{Seq}([\Pi])$, then $\vdash A$ is provable in $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$, and, by Lemma 4.6, $\mathbb{D}_{\mathbf{S4}^+}([\Pi]) \rhd_{\mathbf{S4}} A$. □

By the previous lemma and by the definition of **S4**-evaluation we get

THEOREM 4.8. *Let* $\mathbf{H}$ *be a recursive set of modal Harrop formulas, let* $\pi : \vdash \Box A \vee \Box B$ *be a proof of* $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$, *and let us suppose that* $\vdash \bot$ *is not provable in* $\mathbb{D}_{\mathbf{S4}^+}([\pi])$. *Then either* $\vdash A$ *or* $\vdash B$ *is provable in* $\mathbb{D}_{\mathbf{S4}^+}([\pi])$.

To study the complexity of the extraction calculus, we need to extend the map E_Σ of the previous section to consider the new e-rules. Given a finite set of sequents Σ, $E_\Sigma : 2^{\text{SEQ}} \to 2^{\text{SEQ}}$ is defined as follows:

$$
\begin{aligned}
E_\Sigma(\Delta) = {} & \{\vdash A \mid \Box B_1, \ldots, \Box B_n \vdash A \in \Sigma \text{ and } \{\vdash B_1, \ldots, \vdash B_n\} \subseteq \Delta\} \\
& \bigcup \{\vdash H_1 \mid H_1 \wedge H_2 \text{ is a modal Harrop formula and } \vdash H_1 \wedge H_2 \in \Delta\} \\
& \bigcup \{\vdash H_2 \mid H_1 \wedge H_2 \text{ is a modal Harrop formula and } \vdash H_1 \wedge H_2 \in \Delta\} \\
& \bigcup \{\vdash H \mid \Box A \to H \text{ is a modal Harrop formula and} \\
& \quad \{\vdash \Box A \to H, \vdash A\} \subseteq \Delta\} \\
& \bigcup \{\vdash H \mid \Box H \text{ is a modal Harrop formula and } \vdash \Box H \in \Delta\}.
\end{aligned}
$$

E_Σ has the least fixpoint E_Σ^∞. Given a finite set of proofs Π of $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$, let $\Sigma = \text{Seq}([\Pi])$; it is immediate to check that $\vdash A$ is provable in $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$ iff $\vdash A \in E_\Sigma^\infty$.

THEOREM 4.9. *Let* $\mathbf{H}$ *be a finite set of modal Harrop formulas and let* Π *be a finite set of proofs of* $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$.

(i) *There exists a polynomial time algorithm in* $\|\Pi\|$ *that, given* Π*, generates a proof* $\tau_A : \vdash A$ *of the calculus* $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$ *for every sequent* $\vdash A$ *provable in* $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$.

(ii) *There exists a polynomial time algorithm in* $\|\Pi\|$ *that, given* Π*, generates a proof* $\pi_A : \vdash A$ *of the calculus* $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$ *for every sequent* $\vdash A$ *provable in* $\mathbb{D}_{\mathbf{S4}^+}([\Pi])$.

PROOF. The proof of point (i) is similar to the one given for Theorem 3.4. We only remark that to get the fixpoint we need a $O(n^2)$ iterations with $n = \|\Pi\|$. Indeed, since the application of the e-rules RME$_\wedge$, RMMP, and RE$_\Box$ decomposes some formulas, we can do at most n iterations without applying SLD$_\Box$. Moreover, since $|\mathrm{Seq}([\Pi])| \leq n$, SLD$_\Box$ can be applied in at most n iterations. Point (ii) immediately follows from point (i) and the definition of e-rule. □

Let $\pi : \vdash \Box A \vee \Box B$ be a proof of $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$. To decide (DP) in polynomial time, we exploit the calculus $\mathbb{D}_{\mathbf{S4}^+}([\pi])$. By Theorem 4.8, we know that either $\vdash \bot$ or $\vdash A$ or $\vdash B$ is provable in $\mathbb{D}_{\mathbf{S4}^+}([\pi])$. By Theorem 4.9 we can generate in polynomial time either a proof $\pi_1 : \vdash \bot$ or a proof $\pi_2 : \vdash A$ or a proof $\pi_3 : \vdash B$ of $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$. Note that in the first case $\mathbf{H}$ is **S4**-inconsistent and from π_1 we can construct a proof $\pi : \vdash A$ (or a proof $\pi : \vdash B$) of $\mathcal{ND}_{\mathbf{S4}}(\mathbf{H})$ simply by applying the rule $\bot_{\mathbf{Int}}$ to π_1. Hence, we get the feasible disjunction property in presence of modal Harrop assumptions.

THEOREM 4.10. *There exists a polynomial time algorithm that, given a proof* $\pi : \Gamma \vdash \Box A \vee \Box B$ *of* $\mathcal{ND}_{\mathbf{S4}}$ *with* Γ *a set of modal Harrop formulas, constructs a proof* $\pi_A : \Gamma \vdash A$ *or a proof* $\pi_B : \Gamma \vdash B$ *of the calculus* $\mathcal{ND}_{\mathbf{S4}}$.

As a consequence of the above theorem, arguing as in Buss and Pudlák [2001], one can prove the following version of the *feasible interpolation theorem* for **S4**:

COROLLARY 4.11. *Given a proof* $\pi : \Box p_1 \vee \Box\neg\Box p_1, \ldots, \Box p_n \vee \Box\neg\Box p_n \vdash \Box B_0 \vee \Box B_1$ *of* $\mathcal{ND}_{\mathbf{S4}}$*, it is possible to construct a circuit* $\mathcal{C}(\overline{p})$ *whose size is polynomial in* $\|\pi\|$ *such that, for every* $\overline{a} \in \{0,1\}^n$*, if* $\mathcal{C}(\overline{a}) = i$*, then the formula* $\tilde{B}_i$ *obtained by substituting* p_j *with* $\bot$ *if* $a_j = 0$ *and* p_j *with* $\bot \to \bot$ *if* $a_j = 1$*, belongs to* **S4**.

This yields the following result about the size of proofs of $\mathcal{ND}_{\mathbf{S4}}$:

THEOREM 4.12. *If* $NP \cap coNP \not\subseteq P/poly$*, then the size of shortest proofs of* $\mathcal{ND}_{\mathbf{S4}}$ *cannot be bounded by a polynomial in the size of the proved formulas.*

PROOF. Let X be a set in $NP \cap coNP$. For every $n \geq 1$, there are formulas $A^n(\overline{p}, \overline{q})$ and $B^n(\overline{p}, \overline{r})$, with $\overline{p} = p_1, \ldots, p_n$, such that the size of $A^n(\overline{p}, \overline{q})$ and $B^n(\overline{p}, \overline{r})$ is bounded by some polynomial in n. Moreover:

$$X \cap \{0,1\}^n = \{\overline{a} \in \{0,1\}^n : \exists \overline{q} A^n(\overline{a}, \overline{q}) \text{ is satisfiable}\},$$

$$X^c \cap \{0,1\}^n = \{\overline{a} \in \{0,1\}^n : \exists \overline{r} B^n(\overline{a}, \overline{r}) \text{ is satisfiable}\}.$$

This implies that the formulas $\neg A^n(\overline{p}, \overline{q}) \vee \neg B^n(\overline{p}, \overline{r})$ $(n \geq 1)$ are classical tautologies, and hence the sequents

$$p_1 \vee \neg p_1, \ldots, p_n \vee \neg p_n \vdash \neg A^n(\overline{p}, \overline{q}) \vee \neg B^n(\overline{p}, \overline{r})$$

are provable in **Int** (see Buss and Pudlák [2001]; Pudlák [1999]). Using the $^\circ$ modal embedding of Troelstra and Schwichtenberg [1996], we get that, for every $n \geq 1$, there exists in $\mathcal{ND}_{\mathbf{S4}}$ a proof

$$\pi_n : \Box(\Box p_1 \vee \Box\neg\Box p_1), \ldots, \Box(\Box p_n \vee \Box\neg\Box p_n) \vdash \Box(\neg A^n(\overline{p}, \overline{q}))^\circ \vee \Box(\neg B^n(\overline{p}, \overline{r}))^\circ.$$

Since $\Box(\Box A \vee \Box B) \leftrightarrow (\Box A \vee \Box B)$ holds in **S4**, we get a proof

$$\pi'_n : \Box p_1 \vee \Box\neg\Box p_1, \ldots, \Box p_n \vee \Box\neg\Box p_n \vdash \Box(\neg A^n(\overline{p}, \overline{q}))^\circ \vee \Box(\neg B^n(\overline{p}, \overline{r}))^\circ.$$

Let us assume that all the proofs π'_n have polynomial size in the proved formulas. Then, the circuit $\mathcal{C}_n$ associated with π'_n by Corollary 4.11 has polynomial size in n. Moreover, since for every formula C not containing $\Box$, $C^\circ \in \mathbf{S4}$ implies $C \in \mathbf{Cl}$, we can use $\mathcal{C}_n$ to decide the membership to $X \cap \{0,1\}^n$. This means that $X \in P/pol\, y$. □

4.3 Grzegorczyk Logic

Grzegorczyk logic **Grz** is the modal logic obtained by adding to **S4** the axiom-schema

$$(grz) \equiv \Box(\Box(p \to \Box p) \to p) \to p.$$

A natural deduction calculus $\mathcal{ND}_{\mathbf{Grz}}$ for this logic can be obtained by adding to the natural deduction calculus $\mathcal{ND}_{\mathbf{S4}}$ the axiom-rule

$$\frac{}{\vdash \Box(\Box(A \to \Box A) \to A) \to A}\,\mathrm{grz},$$

where $\Box(\Box(A \to \Box A) \to A) \to A$ is any instance of the axiom-schema (grz). To treat this logic in our framework, we can consider the notion of **S4**-evaluation and the following rules:

$$\frac{\vdash \Box(A \to \Box A) \to A}{\vdash A \to \Box A}\,\mathrm{GRZ}_1, \qquad \frac{\vdash \Box(A \to \Box A) \to A}{\vdash A}\,\mathrm{GRZ}_2.$$

It is easy to check that both are e-rules for $\mathcal{ND}_{\mathbf{Grz}}$. Let $\mathbb{D}_{\mathbf{Grz}}([\Pi])$ denote the extraction calculus $\mathbb{D}(\{\mathrm{SLD}_\Box, \mathrm{GRZ}_1, \mathrm{GRZ}_2\}, [\Pi])$.

LEMMA 4.13. *Let* Π *be a recursive set of proofs of* $\mathcal{ND}_{\mathbf{Grz}}$. *For every proof* $\pi : \Gamma \vdash A$ *belonging to* $[\Pi]$, *if* $\mathbb{D}_{\mathbf{Grz}}([\Pi]) \rhd_{\mathbf{S4}} \Gamma$ *then* $\mathbb{D}_{\mathbf{Grz}}([\Pi]) \rhd_{\mathbf{S4}} A$.

PROOF. The proof proceeds as for Lemma 4.2. We only need to prove that the sequent introduced by the rule grz is evaluated in the extraction calculus. So, let us suppose that

$$\frac{}{\vdash \Box(\Box(A \to \Box A) \to A) \to A}\,\mathrm{grz}$$

belongs to $[\Pi]$ and let us suppose that $\mathbb{D}_{\mathbf{Grz}}([\Pi]) \rhd_{\mathbf{S4}} \Box(\Box(A \to \Box A) \to A)$. We must prove that $\mathbb{D}_{\mathbf{Grz}}([\Pi]) \rhd_{\mathbf{S4}} A$. By the definition of **S4**-evaluation, we have

(i) $\mathbb{D}_{\mathbf{Grz}}([\Pi]) \rhd_{\mathbf{S4}} \Box(A \to \Box A) \to A$ *and* there exists $\tau : \vdash \Box(A \to \Box A) \to A \in \mathbb{D}_{\mathbf{Grz}}([\Pi])$.

First of all we prove that

(ii) $\mathbb{D}_{\mathbf{Grz}}([\Pi]) \rhd_{\mathbf{S4}} \Box(A \to \Box A)$.

By point (i), using the extraction rule GRZ_1 we can build the proof

$$\frac{\tau : \vdash \Box(A \to \Box A) \to A}{\vdash A \to \Box A}\,\text{GRZ}_1$$

in $\mathbb{ID}_{\mathbf{Grz}}([\Pi])$. Now, let us suppose that A is **S4**-evaluated in the extraction calculus; to prove that $\Box A$ is **S4**-evaluated, we only need to build a proof of $\vdash A$ in $\mathbb{ID}_{\mathbf{Grz}}([\Pi])$; this can be done by applying GRZ_2 to τ, and this concludes the proof of Point (ii). By points (i) and (ii) we have $\mathbb{ID}_{\mathbf{Grz}}([\Pi]) \rhd_{\mathbf{S4}} A$. □

By Lemma 4.13, the following holds:

THEOREM 4.14. *If $\pi : \vdash \Box A \vee \Box B \in \mathcal{ND}_{\mathbf{Grz}}$, then either $\vdash A$ or $\vdash B$ is provable in $\mathbb{ID}_{\mathbf{Grz}}([\pi])$.*

To study the complexity of the extraction calculus we consider the map

$$\begin{aligned} E_\Sigma(\Delta) \;=\; & \{ \vdash A \mid \Box B_1, \ldots, \Box B_n \vdash A \in \Sigma \text{ and } \{\vdash B_1, \ldots, \vdash B_n\} \subseteq \Delta\} \\ & \bigcup \{ \vdash A \to \Box A \mid \vdash \Box(A \to \Box A) \to A \in \Delta\} \\ & \bigcup \{ \vdash A \mid \vdash \Box(A \to \Box A) \to A \in \Delta\}. \end{aligned}$$

Reasoning as in the previous cases, we get

THEOREM 4.15. **Grz** *has the feasible disjunction property.*

4.4 **S4.1**

S4.1 is obtained by adding to **S4** the McKinsey axiom (see Chagrov and Zakharyaschev [1997])

$$(ma) \;\equiv\; \Box\Diamond p \to \Diamond\Box p,$$

where $\Diamond p$ is an abbreviation for $\neg\Box\neg p$. A natural deduction calculus $\mathcal{ND}_{\mathbf{S4.1}}$ for this logic can be obtained by adding to the natural deduction calculus $\mathcal{ND}_{\mathbf{S4}}$ the axiom-rule

$$\frac{}{\vdash \Box\Diamond A \to \Diamond\Box A}\,\text{M},$$

where $\Box\Diamond A \to \Diamond\Box A$ is any instance of the axiom-schema (ma). To treat this logic, we can use the extraction calculus $\mathbb{ID}(\text{SLD}_\Box, [\Pi])$ used for **S4** without adding any new e-rule. The proof proceeds as for **S4**. Note that

— $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} \Diamond A$ iff $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} A$ *or* $\mathbb{ID}(\text{SLD}_\Box, [\Pi])$ does not contain any proof of the sequent $\vdash \neg A$.

To prove the main lemma for **S4.1**, we only need to consider the case of proofs $\pi : \vdash \Box\Diamond A \to \Diamond\Box A$ of depth zero. Let us assume that $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} \Box\Diamond A$; to prove that $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} \Diamond\Box A$, we show that $\mathbb{ID}(\text{SLD}_\Box, [\Pi])$ does not contain any proof of the sequent $\vdash \neg\Box A$. Let us assume that such a proof exists; this means that $\neg\Box A$ belongs to **S4.1**, which implies $\neg\Diamond\Box A \in$ **S4.1**. On the other hand, since $\mathbb{ID}(\text{SLD}_\Box, [\Pi]) \rhd_{\mathbf{S4}} \Box\Diamond A$, there exists a proof $\tau : \vdash \Diamond A \in \mathbb{ID}(\text{SLD}_\Box, [\Pi])$; hence $\Diamond A$ belongs to **S4.1**, which implies $\Diamond\Box A \in$ **S4.1**, a contradiction.

Proceeding as in previous sections, we easily get the following:

THEOREM 4.16. **S4.1** *has the feasible disjunction property.*

Table III. Hilbert Calculus $\mathcal{H}_{\mathbf{Cl}}$ for Classical Logic

$Ax1$	$A \wedge B \to A$
$Ax2$	$A \wedge B \to B$
$Ax3$	$A \to (B \to (A \wedge B))$
$Ax4$	$A \to A \vee B$
$Ax5$	$B \to A \vee B$
$Ax6$	$(A \to C) \to ((B \to C) \to (A \vee B \to C))$
$Ax7$	$A \to (B \to A)$
$Ax8$	$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
$Ax9$	$\bot \to A$
$Ax10$	$\neg\neg A \to A$
MP	$\dfrac{A \quad A \to B}{B}$

4.5 Gödel-Löb Logic

To treat Gödel-Löb Logic **GL**, we consider a Hilbert-style calculus (the sequent calculi given in Avron [1984] and Valentini [1983] can be used as well). The Hilbert-style calculus $\mathcal{H}_{\mathbf{GL}}$ for **GL** is obtained by adding to the calculus $\mathcal{H}_{\mathbf{Cl}}$ for classical logic of Table III the axiom-schemata (K) and (4), the Löb axiom (see Chagrov and Zakharyaschev [1997])

$$(la) \equiv \Box(\Box p \to p) \to \Box p,$$

and the necessitation rule

$$\frac{A}{\Box A}\,\text{NEC}.$$

As usual, a proof $\pi : \vdash A$ of $\mathcal{H}_{\mathbf{GL}}$ is any finite sequence of formulas $B_1, \ldots, B_n$ such that $B_n \equiv A$ and, for every $i = 1, \ldots, n$, either B_i is an instance of an axiom-schema, or it is obtained by applying modus ponens to two formulas $C \to D$ and C that occur before in the sequence, or it is obtained by applying the necessitation rule to a formula C that occurs before in the sequence. A subproof of a proof π of $\mathcal{H}_{\mathbf{GL}}$ is any subsequence of π which is a proof of $\mathcal{H}_{\mathbf{GL}}$. We remark that, given a proof $\pi : \vdash A$, the set $\text{Seq}([\pi])$ only contains sequents with an empty set of assumptions.

We note that **GL** is "incompatible" with the reflexivity axiom $\Box p \to p$; indeed, adding this axiom to **GL**, we obtain an inconsistent logic. We introduce a new notion of evaluation that differs from **S4**-evaluation in the case of boxed formulas.

Definition 4.17 (**GL**-*Evaluation*). Given a set of proofs Π of a calculus **C** and a formula A, A is **GL**-*evaluated* in Π (in symbols $\Pi \rhd_{\mathbf{GL}} A$) iff one of the following inductive conditions holds:

(1) A is a propositional variable;
(2) $A \equiv B \wedge C$ and $\Pi \rhd_{\mathbf{GL}} B$ and $\Pi \rhd_{\mathbf{GL}} C$;
(3) $A \equiv B \vee C$ and either $\Pi \rhd_{\mathbf{GL}} B$ or $\Pi \rhd_{\mathbf{GL}} C$;
(4) $A \equiv B \to C$ and, if $\Pi \rhd_{\mathbf{GL}} B$ then $\Pi \rhd_{\mathbf{GL}} C$;
(5) $A \equiv \Box B$ and there exists a proof $\tau : \vdash B \in \Pi$.

We point out that $\Pi \rhd_{\mathbf{GL}} \neg A$ iff $\Pi \rhd_{\mathbf{GL}} A$ does not hold. If the symbol $\Diamond$ is used, $\Pi \rhd_{\mathbf{GL}} \Diamond A$ iff there is no proof of $\vdash \neg A$ in Π. Given a set of formulas Γ, $\Pi \rhd_{\mathbf{GL}} \Gamma$ iff $\Pi \rhd_{\mathbf{GL}} A$ for every $A \in \Gamma$.

Let us consider the following inference rules:

$$\frac{\vdash A \quad \vdash A \to B}{\vdash B}\text{RMP}, \qquad \frac{\vdash A \quad \vdash \Box A \to \Box\Box A}{\vdash \Box A}\text{R}_{\Box}, \qquad \frac{\vdash \Box A \to A}{\vdash A}\text{RLA}.$$

It is easy to check that these rules are e-rules for $\mathcal{H}_{\mathbf{GL}}$. Let Π be a set of proofs of $\mathcal{H}_{\mathbf{GL}}$; we denote with $\mathbb{ID}_{\mathbf{GL}}([\Pi])$ the extraction calculus $\mathbb{ID}(\{\text{RMP}, \text{R}_{\Box}, \text{RLA}\}, [\Pi])$. We point out that the presence of the premise $\vdash \Box A \to \Box\Box A$ in $\text{R}_{\Box}$ is needed to prevent unnecessary applications of the rule in the extraction calculus.

LEMMA 4.18. *Let Π be a recursive set of proofs of $\mathcal{H}_{\mathbf{GL}}$. For every $\pi : \vdash A$ belonging to $[\Pi]$, $\mathbb{ID}_{\mathbf{GL}}([\Pi]) \rhd_{\mathbf{GL}} A$.*

PROOF. The proof is by induction on the number k of applications of the rules MP and NEC in π. If $k = 0$, A is an axiom of $\mathcal{H}_{\mathbf{GL}}$. If A is an axiom of $\mathcal{H}_{\mathbf{Cl}}$, the assertion immediately follows by the definition of **GL**-evaluation (there is no need to apply e-rules). Let us analyze the case of modal axioms.

—*Axiom (K)*. Let us assume that $\mathbb{ID}_{\mathbf{GL}}([\Pi]) \rhd_{\mathbf{GL}} \Box(B \to C)$. Then there exists a proof $\tau : \vdash B \to C$ in $\mathbb{ID}_{\mathbf{GL}}([\Pi])$. We have to prove that $\mathbb{ID}_{\mathbf{GL}}([\Pi]) \rhd_{\mathbf{GL}} \Box B \to \Box C$. Let us assume that $\mathbb{ID}_{\mathbf{GL}}([\Pi]) \rhd_{\mathbf{GL}} \Box B$; then there exists a proof $\tau' : \vdash B$ in $\mathbb{ID}_{\mathbf{GL}}([\Pi])$. By applying the e-rule RMP to τ and τ', we get a proof of $\vdash C$ and this proves that $\mathbb{ID}_{\mathbf{GL}}([\Pi]) \rhd_{\mathbf{GL}} \Box C$.

—*Axiom* (4). Let us assume that $\mathbb{ID}_{\mathbf{GL}}([\Pi]) \rhd_{\mathbf{GL}} \Box B$. Then there exists a proof $\tau : \vdash B$ in $\mathbb{ID}_{\mathbf{GL}}([\Pi])$. Since $\vdash \Box B \to \Box\Box B$ is an axiom of $\mathbb{ID}_{\mathbf{GL}}([\Pi])$, by applying the e-rule $\text{R}_{\Box}$ we can build a proof of $\vdash \Box B$, and this proves that $\mathbb{ID}_{\mathbf{GL}}([\Pi]) \rhd_{\mathbf{GL}} \Box\Box B$.

—*Axiom (la)*. Let us assume that $\mathbb{ID}_{\mathbf{GL}}([\Pi]) \rhd_{\mathbf{GL}} \Box(\Box B \to B)$. Then there exists a proof $\tau : \vdash \Box B \to B$ in $\mathbb{ID}_{\mathbf{GL}}([\Pi])$. By applying the e-rule RLA, we can build a proof of $\vdash B$ and this proves that $\mathbb{ID}_{\mathbf{GL}}([\Pi]) \rhd_{\mathbf{GL}} \Box B$.

Let $k > 0$. If the last rule applied in π is MP, the lemma immediately follows by the induction hypothesis and the definition of **GL**-evaluation. If the last rule is NEC, then $A \equiv \Box B$ and $\vdash B$ is an axiom of $\mathbb{ID}_{\mathbf{GL}}([\Pi])$; therefore $\mathbb{ID}_{\mathbf{GL}}([\Pi]) \rhd_{\mathbf{GL}} \Box B$. □

As a consequence:

THEOREM 4.19. *If $\pi : \vdash \Box A \vee \Box B$ is a proof of $\mathcal{H}_{\mathbf{GL}}$, then either $\vdash A$ or $\vdash B$ is provable in $\mathbb{ID}_{\mathbf{GL}}([\pi])$.*

Let SEQ be the set of all the sequents of $\mathcal{L}_{\Box}$. The operator needed to study the complexity of the extraction calculus is

$$\begin{aligned} E_{\Sigma}(\Delta) \;=\; & \Sigma \bigcup \{ \vdash B \mid \{\vdash A, \vdash A \to B\} \subseteq \Delta\} \\ & \bigcup \{ \vdash \Box A \mid \{\vdash A, \vdash \Box A \to \Box\Box A\} \subseteq \Delta\} \\ & \bigcup \{ \vdash A \mid \vdash \Box A \to A \in \Delta\}. \end{aligned}$$

Arguing as in the previous cases we can conclude:

Table IV. Axioms and Rules for **IK**

FS1	$\Diamond(A \vee B) \rightarrow \Diamond A \vee \Diamond B$
FS2	$\Box A \wedge \Box B \rightarrow \Box(A \wedge B)$
FS3	$\neg\Diamond\bot$
FS4	$\Diamond(A \rightarrow B) \rightarrow (\Box A \rightarrow \Diamond B)$
FS5	$(\Diamond A \rightarrow \Box B) \rightarrow \Box(A \rightarrow B)$
FS6	$\dfrac{A \rightarrow B}{\Diamond A \rightarrow \Diamond B}$
FS7	$\dfrac{A \rightarrow B}{\Box A \rightarrow \Box B}$

THEOREM 4.20. **GL** *has the feasible disjunction property.*

To conclude this section, we remark that the modal logic obtained by adding the axiom-schema (ma) to **GL** also has the feasible disjunction property. Indeed, as the reader can easily check, (ma) is **GL**-evaluated in the extraction calculus using the e-rules defined in this section.

5. INTUITIONISTIC MODAL LOGICS

To conclude the article, we show that the feasible disjunction property also holds for the intuitionistic modal logic **IK** defined in Fischer Servi [1984]. Here we consider the language $\mathcal{L}_{\Box,\Diamond}$ consisting of the logical constants $\bot$, $\wedge$, $\vee$, $\rightarrow$ and the modal operators $\Box$ and $\Diamond$. Let $\mathcal{H}_{\mathbf{Int}}$ be the Hilbert-style calculus consisting of the axioms (Ax1)–(Ax9) and the rule MP of Table III. The Hilbert-style calculus $\mathcal{H}_{\mathbf{IK}}$ for **IK** defined in Fischer Servi [1984] is obtained by adding to $\mathcal{H}_{\mathbf{Int}}$ axioms and rules of Table IV. In the case of intuitionistic modal logics the disjunction property and the feasible disjunction property are defined as for intuitionistic logic.

We use a notion of evaluation which extends intuitionistic evaluation so that evaluation of formulas of the kind $\Box A$ only requires provability, while formulas of the kind $\Diamond A$ are never evaluated.

Definition 5.1 (**IK**-*Evaluation*). Given a set of proofs Π of a calculus **C** and a formula A, A is **IK**-*evaluated* in Π (in symbols $\Pi \rhd_{\mathbf{IK}} A$) iff the following conditions hold:

(i) There exists a proof $\pi :\vdash A \in \Pi$.
(ii) One of the following inductive conditions holds:
  (a) A is a propositional variable or $A \equiv \Box B$;
  (b) $A \equiv B \wedge C$ and $\Pi \rhd_{\mathbf{IK}} B$ and $\Pi \rhd_{\mathbf{IK}} C$;
  (c) $A \equiv B \vee C$ and either $\Pi \rhd_{\mathbf{IK}} B$ or $\Pi \rhd_{\mathbf{IK}} C$;
  (d) $A \equiv B \rightarrow C$ and, if $\Pi \rhd_{\mathbf{IK}} B$, then $\Pi \rhd_{\mathbf{IK}} C$.

To treat this logic we only need the rule RMP of Section 4.5 which is an e-rule for $\mathcal{H}_{\mathbf{IK}}$.

LEMMA 5.2. *Let* Π *be a recursive set of proofs of* $\mathcal{H}_{\mathbf{IK}}$. *For every* $\pi :\vdash A$ *belonging to* $[\Pi]$, $\mathbb{ID}(\text{RMP}, [\Pi]) \rhd_{\mathbf{IK}} A$.

PROOF. Since $\vdash A$ is an axiom of $\mathbb{ID}(\text{RMP}, [\Pi])$, point (i) of Definition 5.1 is immediate. To prove point (ii), we proceed by induction on the number k of applications of the rules MP, FS6, and FS7 in π. If $k = 0$, A is an axiom of $\mathcal{H}_{\mathbf{IK}}$. If A is an intuitionistic axiom, the proof immediately follows by the definition of **IK**-evaluation. Axioms FS1, FS3, and FS4 are trivial, since the antecedent of these axioms cannot be **IK**-evaluated. Let us consider the case of axiom FS2, namely, $A \equiv \Box B \wedge \Box C \rightarrow \Box(B \wedge C)$. If $\mathbb{ID}(\text{RMP}, [\Pi]) \rhd_{\mathbf{IK}} \Box B \wedge \Box C$, there exists a proof $\tau : \vdash \Box B \wedge \Box C$ in $\mathbb{ID}(\text{RMP}, [\Pi])$. By applying RMP, we get a proof of $\vdash \Box(B \wedge C)$, and this proves that $\mathbb{ID}(\text{RMP}, [\Pi]) \rhd_{\mathbf{IK}} \Box(B \wedge C)$. The case $A \equiv$ FS5 is similar.

Suppose $k > 0$. If the last rule applied in π is MP, the assertion follows by the induction hypothesis and the definition of **IK**-evaluation. If the last rule applied in π is FS6 ($A \equiv \Diamond B \rightarrow \Diamond C$), the assertion is trivial since $\mathbb{ID}(\text{RMP}, [\Pi]) \rhd_{\mathbf{IK}} \Diamond B$ does not hold. Suppose that the last rule applied in π is FS7 ($A \equiv \Box B \rightarrow \Box C$). If $\mathbb{ID}(\text{RMP}, [\Pi]) \rhd_{\mathbf{IK}} \Box B$, then $\mathbb{ID}(\text{RMP}, [\Pi])$ contains a proof of $\vdash \Box B$. Applying RMP, we get a proof of $\Box C$; thus $\mathbb{ID}(\text{RMP}, [\Pi]) \rhd_{\mathbf{IK}} \Box C$. □

Using the operator $E_\Sigma(\Delta) = \Sigma \cup \{ \vdash B \mid \{\vdash A, \vdash A \rightarrow B\} \subseteq \Delta\}$ and reasoning as in the previous cases, one easily gets

THEOREM 5.3. **IK** *has the feasible disjunction property.*

Using a suitable notion of evaluation (see, e.g., the variant of *Kleene's slash* quoted in Amati and Pirri [1994]), the feasible disjunction property can be easily proved also for the intuitionistic modal logics **ID**, **IT**, **IKDB**, **IB**, **IKD4**, **IS4**, and **IS5** studied in Amati and Pirri [1994].

REFERENCES

AMATI, G. AND PIRRI, F. 1994. A uniform tableau method for intuitionistic modal logics I^*. *Studia Logica 53*, 1, 29–60.

AVELLONE, A., FERRARI, M., AND FIORENTINI, C. 2001. A formal framework for synthesis and verification of logic programs. In *Logic Based Program Synthesis and Transformation, 10th International Workshop, LOPSTR 2000, Selected Papers*, K.-K. Lau, Ed. Lecture Notes in Computer Science, vol. 2042. Springer-Verlag, Berlin, Germany, 1–17.

AVRON, A. 1984. On modal systems having arithmetical interpretations. *J. Symbol. Logic 49*, 3, 935–942.

BUSS, S. 1999. Propositional proof complexity—an introduction. In *Computational Logic (Marktoberdorf, 1997)*. NATO Adv. Sci. Inst. Ser. F Comput. Systems Sci., vol. 165. Springer, Berlin, Germany, 127–178.

BUSS, S. AND MINTS, G. 1999. The complexity of the disjunction and existential properties in intuitionistic logic. *Ann. Pure Appl. Logic 99*, 3, 93–104.

BUSS, S. AND PUDLÁK, P. 2001. On the computational content of intuitionistic propositional proofs. *Ann. Pure Appl. Logic 109*, 1-2, 49–64.

CHAGROV, A. AND ZAKHARYASCHEV, M. 1997. *Modal Logic*. Oxford University Press, Oxford, U.K.

FERRARI, M. AND FIORENTINI, C. 2003. A proof-theoretical analysis of semiconstructive intermediate theories. *Studia Logica 73*, 1, 21–49.

FERRARI, M., FIORENTINI, C., AND FIORINO, G. 2002. On the complexity of disjunction and explicit definability properties in some intermediate logics. In *LPAR 2002: Logic for Programming Artificial Intelligence and Reasoning*. Lecture Notes in Artificial Intelligence, vol. 2514. Springer-Verlag, Berlin, Germany, 175–189.

FERRARI, M., FIORENTINI, C., AND MIGLIOLI, P. 1999. Goal oriented information extraction in uniformly constructive calculi. In *Argentinian Workshop on Theoretical Computer Science* (WAIT'99). Sociedad Argentina de Informática e Investigación Operativa, 51–63.

FERRARI, M., MIGLIOLI, P., AND ORNAGHI, M. 2003. On uniformly constructive and semiconstructive formal systems. *Logic J. IGPL 11*, 1, 1–49.

FISCHER SERVI, G. 1984. Axiomatizations for some intuitionistic modal logics. *Rend. Sem. Mat. Univers. Polit. Torino 42*, 179–194.

KRAJÍČEK, J. 1995. Bounded arithmetic, propositional logic, and complexity theory. *Encyclopedia of Mathematics and its Applications*, vol. 60. Cambridge University Press, Cambridge, U.K.

PRAWITZ, D. 1965. *Natural Deduction*. Almquist and Winksell, Stockholm, Sweden.

PUDLÁK, P. 1999. On the complexity of the propositional calculus. In *Sets and Proofs (Leeds, 1997)*. London Math. Soc. Lecture Note Ser., vol. 258. Cambridge University Press, Cambridge, U.K., 197–218.

TROELSTRA, A. AND SCHWICHTENBERG, H. 1996. *Basic Proof Theory*. Cambridge Tracts in Theoretical Computer Science, vol. 43. Cambridge University Press, Cambridge, U.K.

VALENTINI, S. 1983. The modal logic of provability: cut-elimination. *J. Philos. Logic 12*, 4, 471–476.

Received July 2003; revised December 2003; accepted December 2003