An $\mathcal{O}((n.log\ n)^3)$-time transformation from Grz into decidable fragments of classical first-order logic

Stéphane Demri*
Laboratoire LEIBNIZ - C.N.R.S.
46 Avenue Félix Viallet
38031 Grenoble, France

Rajeev Goré†
Automated Reasoning Project and
Department of Computer Science
Australian National University
Canberra ACT 0200, Australia

November 6, 1998

Abstract

The provability logic Grz is characterized by a class of modal frames that is not first-order definable. We present a simple embedding of Grz into decidable fragments of classical first-order logic such as FO_2 and the guarded fragment. The embedding is an $\mathcal{O}((n.log\ n)^3)$-time transformation that neither involves first principles about Turing machines (and therefore is easy to implement), nor the semantical characterization of Grz (and therefore does not use any second-order machinery). Instead, we use the syntactic relationships between cut-free sequent-style calculi for Grz, S4 and T. We first translate Grz into T, and then we use the relational translation from T into FO_2.

1 Introduction

Propositional modal logics have proved useful in many areas of computer science because they capture interesting properties of binary relations (Kripke frames) whilst retaining decidability (see e.g. [28]). By far the most popular method for automating deduction in these logics has been the method of analytic tableaux (see e.g. [6]), particularly because of the close connection between tableaux calculi and known cut-free Gentzen systems for these logics (see e.g. [11]).

An alternative approach is to translate propositional modal logics into classical first-order logic since this allows us to use the wealth of knowledge in first-order theorem proving to mechanize modal deduction (see e.g. [17, 20, 12, 5]). Let FO_n be the fragment of classical first-order logic using at most n individual variables and no function symbols. Any modal logic characterized by a first-order definable class of modal frames can be translated into FO_n where $n > 2$ is the number of variables in the first-order formula characterizing the class of frames. The *decidable* modal logic K4, for example, is characterised by transitive frames, definable using the first-order formula $(\forall x, y, z)(R(x, y) \wedge R(y, z) \Rightarrow R(x, z))$ containing 3 variables. Since FO_3 is undecidable and FO_2 is decidable, translating K4 into first-order logic does not automatically retain decidability. Of course, the exact fragment

*demri@imag.fr
†Supported by an Australian Research Council Queen Elizabeth II Fellowship.rpg@arp.anu.edu.au

delineated by the translation is decidable, but there is no known first-order decision procedure for that particular fragment except the one that mimicks the rules for K4. Therefore, blind translation is not useful if this means giving up decidability.

Moreover, it is well-known that many *decidable* propositional modal logics are characterised by classes of Kripke frames which are not first-order definable, and that the "standard" relational translation (see e.g. [17, 27]) is unable to deal with such logics. The class of such "second order" modal logics includes logics like G and Grz which have been shown to have "arithmetical" interpretations as well as logics like S4.3.1 which have interpretations as logics of linear time (without a next-time operator) [9].

Somewhat surprisingly, faithful translations into classical logic (usually augmented with theories) have been found for some propositional modal logics even when these logics are characterized by classes of frames that are not first-order definable. For instance, the modal logic K augmented with the McKinsey axiom is captured by the framework presented in [21]. Similarly, the provability logic G[1] that admits arithmetical interpretations [25] is treated within the set-theoretical framework defined in [5]. Both techniques in [21, 5] use a version of classical logic augmented with a theory. Alternatively, G can also be translated into classical logic by first using the translation into K4 defined in [2] and then a translation from K4 into classical logic (see e.g. [27]).

The fact that G can be translated into a *decidable* fragment of classical logic follows from a purely complexity theory viewpoint, as shown next. Take a modal logic $\mathcal{L}$ that is in the complexity class $\mathbf{C}$ and let $\mathbf{C}'$ be another complexity class. Here a *logic* is to be understood as a set of formulae and therefore a logic is exactly a *problem* in the usual sense in complexity theory. That is, as a language viewed as a set of strings built upon a given alphabet. By definition (see e.g. [23]), for any fragment of classical logic that is $\mathbf{C}$-hard with respect to $\mathbf{C}'$ many-one reductions[2], there is a mapping f in $\mathbf{C}'$ such that any modal formula $\phi \in \mathcal{L}$ iff $f(\phi)$ is valid in such a first-order fragment. From the facts that G is in **PSPACE** (see e.g. [2, 15]), validity in FO_2 is **NEXPTIME**-hard [8] and $\mathbf{PSPACE} \subseteq \mathbf{NEXPTIME}$, it is easy to conclude that there exists a polynomial-time transformation from G into validity in FO_2.

As is well-known, this illustrates the difference between the fact that a propositional modal logic K + ϕ is characterised by a class of frames which is not first-order definable, and the existence of a translation from K + ϕ into first-order logic. The weak point with this theoretical result is that the definition of f might require the use of first principles about Turing machines. If this is so, then realising the map f requires cumbersome machinery since we must first completely define a Turing machine that solves the problem. This is why the translations in [21, 2, 5] are much more refined and practical (apart from the fact that they allow to mechanise the modal logics under study).

Another well-known modal logic that is characterized by a class of modal frames that is not first-order definable is the provability logic Grz (for Grzegorczyk). The main contribution of this paper is the definition of an $\mathcal{O}(n.log\ n)$-time transformation from Grz into S4, using cut-free sequent-style calculi for these respective logics. Renaming techniques from [16] are used in order to get the $\mathcal{O}(n.log\ n)$-time bound. Then, we present a cubic-time transformation from S4 into T, again using the cut-free sequent-style calculi for these respective logics. Both reductions proceed via an analysis of the proofs in cut-free sequent calculi from the literature. The second reduction is a slight variant of the one presented in [4] (see also [7]). The reduction announced in the title can be obtained by

[1] Also called GL (for Gödel and Löb), KW, K4W, PrL.

[2] Also called "transformation", see e.g. [23].

translating T into FO_2, which is known to be decidable (see e.g. [18]). Furthermore, the formula obtained by reduction belongs to the decidable guarded fragment of classical logic for which a resolution decision procedure has been defined in [19].

In [3, Chapter 12], a (non polynomial-time) transformation from Grz into G is defined. By using renamings of subformulae, there also exists an $\mathcal{O}(n.log\ n)$-time transformation from Grz into G [3, Chapter 12]. There exists an $\mathcal{O}(n)$-time transformation from G into K4 [2]. There exists an $\mathcal{O}(n^4.log\ n)$-time transformation from K4 into K [4] (which uses renamings of subformulae). Finally, there exists an $\mathcal{O}(n)$-time transformation from K into FO_2 [27]. Combining these results gives an $\mathcal{O}(n^4.(log\ n)^5)$-time transformation from Grz into FO_2, a decidable fragment of first-order logic.

The translation proposed in this paper is therefore a more refined alternative since it requires only time in $\mathcal{O}((n.log\ n)^3)$. As a side-effect, we obtain an $\mathcal{O}(n.log\ n)$-time transformation from Grz into S4 and an $\mathcal{O}((n.log\ n)^3)$-time transformation from Grz into T. Using the space upper bound for S4-validity from [13], we obtain that Grz requires only space in $\mathcal{O}(n^2.(log\ n)^3)$. We are not aware of any tighter bound for Grz in the literature. Furthermore, our purely proof-theoretical analyses of the cut-free sequent-style calculi, and sometimes of the Hilbert-style proof systems, gives a simple framework to unify the transformations involved in [3, 2, 4]. As we intend to report in a longer paper, it is also possible to generalise our method to handle other "second order" propositional modal logics like S4.3.1 using the calculi from [9].

2 Basic Notions

In the present paper, we assume that the modal formulae are built from a countably infinite set $\texttt{For}_0 \stackrel{\text{def}}{=} \{\mathtt{p}_{i,j} : i, j \in \omega\}$ of atomic propositions using the usual connectives $\Box$, $\neg$, $\Rightarrow$, $\wedge$. Other standard abbreviations include $\vee, \Leftrightarrow, \Diamond$. The set of modal formulae is denoted $\texttt{For}$. We write $mwn(\phi)$ (resp. $mwp(\phi)$) to denote the number of positive[3] (resp. negative) occurrences of $\Box$ in ϕ.

We recall that the standard Hilbert system K is composed of the following axiom schemata: the tautologies of the Propositional Calculus (PC) and $\Box\mathtt{p} \Rightarrow (\Box(\mathtt{p} \Rightarrow \mathtt{q}) \Rightarrow \Box\mathtt{q})$. The inference rules of K are *modus ponens* (from $\mathtt{p}$ and $\mathtt{p} \Rightarrow (\mathtt{p} \Rightarrow \mathtt{q})$ infer $\mathtt{q}$) and *necessitation* (from $\mathtt{p}$ infer $\Box\mathtt{p}$). By abusing our notation, we may identify the system K with its set of theorems, allowing us to write $\phi \in K$ to denote that ϕ is a *theorem* of K. Analogous notation is used for the following well-known conservative extensions of K: T $\stackrel{\text{def}}{=}$ K + $\Box\mathtt{p} \Rightarrow \mathtt{p}$, K4 $\stackrel{\text{def}}{=}$ K + $\Box\mathtt{p} \Rightarrow \Box\Box\mathtt{p}$, S4 $\stackrel{\text{def}}{=}$ K4 + $\Box\mathtt{p} \Rightarrow \mathtt{p}$ and Grz $\stackrel{\text{def}}{=}$ S4 + $\Box(\Box(\mathtt{p} \Rightarrow \Box\mathtt{p}) \Rightarrow \mathtt{p}) \Rightarrow \Box\mathtt{p}$. Clearly, $\phi \in$ S4 implies $\phi \in$ Grz.

We call $\texttt{GT}$, $\texttt{G}$S4 and $\texttt{G}$Grz the cut-free versions of the Gentzen-style calculi defined in [22, 1] where the sequents are built from multisets of formulas. Moreover, we assume that the contraction and the weakening rules are absorbed in the introduction rules and axioms (see e.g. [26, Section 3.4 and Section 9.1]. For instance, the initial sequents of all the Gentzen-style calculi used in the paper are of the form $\Gamma, \phi \vdash \Delta, \phi$ where "," denotes multiset union. The introduction rules for $\Box$ are the following:

$$\frac{\Gamma \vdash \phi}{\Sigma, \Box\Gamma \vdash \Box\phi, \Delta}\ (\vdash \Box)_T \qquad\qquad \frac{\Box\Gamma \vdash \phi}{\Sigma, \Box\Gamma \vdash \Box\phi, \Delta}\ (\vdash \Box)_{S4}$$

[3] We use the standard notions of *positive* and *negative* occurrences. For instance $\Box\mathtt{p}_{0,0}$ (resp. $\Box\mathtt{p}_{0,1}$) has a positive (resp. negative) occurrence in $(\Box\Box\mathtt{p}_{0,1}) \Rightarrow (\mathtt{p}_{0,1} \wedge \Box\mathtt{p}_{0,0})$.

$$\frac{\Box\Gamma, \Box(\phi \Rightarrow \Box\phi) \vdash \phi}{\Sigma, \Box\Gamma \vdash \Box\phi, \Delta}\ (\vdash \Box)_{Grz} \qquad\qquad \frac{\Gamma, \Box\phi, \phi \vdash \Delta}{\Gamma, \Box\phi \vdash \Delta}\ (\Box \vdash)$$

where $\Box\Gamma \stackrel{\text{def}}{=} \{\Box\psi : \psi \in \Gamma\}$. The rule $(\Box \vdash)$ belongs to the three systems $\mathtt{G}$T, $\mathtt{G}$S4 and $\mathtt{G}$Grz and each rule $(\vdash \Box)_T$, $(\vdash \Box)_{S4}$ and $(\vdash \Box)_{Grz}$ belongs respectively to $\mathtt{G}$T, $\mathtt{G}$S4 and $\mathtt{G}$Grz. For each $\mathcal{L} \in \{T, S4, Grz\}$, we know that $\phi \in \mathcal{L}$ iff the sequent $\vdash \phi$ is derivable in $\mathtt{G}\mathcal{L}$ (see e.g. [22, 1]). Further details can be found in [11].

3 A transformation from Grz into S4

Let $f : \mathtt{For} \times \{0, 1\} \rightarrow \mathtt{For}$ be the following map:

- for any $\mathtt{p} \in \mathtt{For}_0$, $f(\mathtt{p}, 0) \stackrel{\text{def}}{=} f(\mathtt{p}, 1) \stackrel{\text{def}}{=} \mathtt{p}$
- $f(\neg\phi, i) \stackrel{\text{def}}{=} \neg f(\phi, 1 - i)$ for $i \in \{0, 1\}$
- $f(\phi_1 \wedge \phi_2, i) \stackrel{\text{def}}{=} f(\phi_1, i) \wedge f(\phi_2, i)$ for $i \in \{0, 1\}$
- $f(\phi_1 \Rightarrow \phi_2, 1) \stackrel{\text{def}}{=} f(\phi_1, 0) \Rightarrow f(\phi_2, 1)$ $\qquad f(\phi_1 \Rightarrow \phi_2, 0) \stackrel{\text{def}}{=} f(\phi_1, 1) \Rightarrow f(\phi_2, 0)$
- $f(\Box\phi, 1) \stackrel{\text{def}}{=} \Box(\Box(f(\phi, 1) \Rightarrow \Box f(\phi, 0)) \Rightarrow f(\phi, 1))$ $\qquad f(\Box\phi, 0) \stackrel{\text{def}}{=} \Box f(\phi, 0)$.

In $f(\phi, i)$, the index i should be seen as information about the *polarity* of ϕ in the translation process as is done in [2] for the translation from G into K4. Since the rule of *replacement of equivalents* is admissible in Grz, one can show by induction on the length of ϕ that for any $\phi \in \mathtt{For}$ and for any $i \in \{0, 1\}$, $\phi \Leftrightarrow f(\phi, i) \in Grz$. Moreover,

Lemma 3.1. For any $\phi \in \mathtt{For}$, $\phi \Rightarrow f(\phi, 1) \in S4$ and $f(\phi, 0) \Rightarrow \phi \in S4$.

Most of the proofs in this extended abstract are just sketched because of lack of space. The proof of Lemma 3.1 is therefore an exception.

Proof: The proof is by simultaneous induction on the length of ϕ. The base case when ϕ is an atomic proposition is immediate. By way of example, let us treat the cases below in the induction step:

(1) $\phi_1 \wedge \phi_2 \Rightarrow f(\phi_1 \wedge \phi_2, 1) \in S4$ $\quad$ (2) $\Box\phi_1 \Rightarrow f(\Box\phi_1, 1) \in S4$

(3) $f(\neg\phi_1, 0) \Rightarrow \neg\phi_1 \in S4$ $\quad$ (4) $f(\Box\phi_1, 0) \Rightarrow \Box\phi_1 \in S4$.

(1) By the induction hypothesis, $\phi_1 \Rightarrow f(\phi_1, 1) \in S4$ and $\phi_2 \Rightarrow f(\phi_2, 1) \in S4$. By easy manipulation at the propositional level, $\phi_1 \wedge \phi_2 \Rightarrow f(\phi_1, 1) \wedge f(\phi_2, 1) \in S4$. By definition of f, $\phi_1 \wedge \phi_2 \Rightarrow f(\phi_1 \wedge \phi_2, 1) \in S4$.
(2) By the induction hypothesis, $\phi_1 \Rightarrow f(\phi_1, 1) \in S4$. By easy manipulation at the propositional level, $\phi_1 \Rightarrow (\Box(f(\phi, 1) \Rightarrow \Box f(\phi, 0)) \Rightarrow f(\phi_1, 1)) \in S4$. It is known that the *regular rule* (from $\psi_1 \Rightarrow \psi_2$ infer $\Box\psi_1 \Rightarrow \Box\psi_2$) is admissible in $S4$. So, $\Box\phi_1 \Rightarrow \Box(\Box(f(\phi, 1) \Rightarrow \Box f(\phi, 0)) \Rightarrow f(\phi_1, 1)) \in S4$. By the definition of f, $\Box\phi_1 \Rightarrow f(\Box\phi_1, 1) \in S4$.
(3) By the induction hypothesis, $\phi_1 \Rightarrow f(\phi_1, 1) \in S4$. By easy manipulation at the propositional level, $\neg f(\phi_1, 1) \Rightarrow \neg\phi_1 \in S4$. By definition of f, $f(\neg\phi_1, 0) \Rightarrow \neg\phi_1 \in S4$.
(4) By the induction hypothesis, $f(\phi_1, 0) \Rightarrow \phi_1 \in S4$. Since the regular rule is admissible in S4, $\Box f(\phi_1, 0) \Rightarrow \Box\phi_1 \in S4$. By the definition of f, $f(\Box\phi_1, 0) \Rightarrow \Box\phi_1 \in S4$. **Q.E.D.**

It is worth observing that Lemma 3.1 still holds true if in its statement we replace S4 by K. The property of f stated in Lemma 3.1 can be put in parallel with the maps transforming structures into formulas in Display Logic (see e.g. [14, 10]).

Theorem 3.2. A formula $\phi \in Grz$ iff $f(\phi, 1) \in S4$.

Proof: (sketch) If $f(\phi, 1) \in S4$, then *a fortiori* $f(\phi, 1) \in Grz$, and since $\phi \Leftrightarrow f(\phi, 1) \in Grz$, we then obtain $\phi \in Grz$. Now assume $\phi \in Grz$, hence the sequent $\vdash \phi$ has a cut-free proof in GGrz. We can show that in the given cut-free proof of $\vdash \phi$, for every sequent $\Gamma \vdash \Delta$ with cut-free proof Π', the sequent $f(\Gamma, 0) \vdash f(\Delta, 1)$ admits a cut-free proof, say $f(\Pi')$, in GS4. Here, f is extended to multisets of formulae in the natural way. So, we shall conclude that $\vdash f(\phi, 1)$ is derivable in GS4 and therefore $f(\phi, 1) \in S4$. The proof is by induction on the length of the derivations. **Q.E.D.**

A close examination of f shows that f is not computable in $\mathcal{O}(n.log\ n)$-time. Indeed, the right-hand side in the definition of $f(\Box\phi, 1)$ requires several recursive calls to f and the computation of f is therefore exponential-time. However, we can use a slight variant of f that uses renamings as done in [16]. Specifically, we have,

(Renaming) a formula $\phi \in S4$ iff $\Box(\mathtt{p}_{new} \Leftrightarrow \psi) \Rightarrow \phi' \in S4$

where ϕ' is obtained from ϕ by replacing every occurrence of ψ in ϕ by the atomic proposition $\mathtt{p}_{new}$ not occurring in ϕ.

Let ϕ be a modal formula we wish to translate from Grz into S4. Let $\phi_1, \ldots, \phi_m$ be an arbitrary enumeration (without repetition) of all the subformulae of ϕ. For any subformula ψ of ϕ, we write $[\psi]$ to denote the unique natural number in $\{1, \ldots, m\}$ such that $\phi_{[\psi]} = \psi$. We shall build a formula $g(\phi)$ using $\{\mathtt{p}_{i,j} : 1 \leq i \leq m,\ j \in \{0, 1\}\}$ such that $g(\phi) \in S4$ iff $f(\phi, 1) \in S4$. Moreover, $g(\phi)$ can be computed in time $\mathcal{O}(|\phi|.log\ |\phi|)$. For each subformula ψ of ϕ we associate a formula ϕ^{ψ} as shown in Figure 1 and let

$$g(\phi) \stackrel{\text{def}}{=} \bigwedge_{i=1}^{m} \phi^{\phi_i} \Rightarrow \mathtt{p}_{[\phi],1}$$

Form of ψ	ϕ^{ψ}
$\mathtt{p}$	$\Box(\mathtt{p}_{[\psi],0} \Leftrightarrow \mathtt{p}_{[\psi],1})$
$\neg\psi_1$	$\Box(\mathtt{p}_{[\psi],1} \Leftrightarrow \neg\mathtt{p}_{[\psi_1],0}) \wedge \Box(\mathtt{p}_{[\psi],0} \Leftrightarrow \neg\mathtt{p}_{[\psi_1],1})$
$\psi_1 \wedge \psi_2$	$\Box(\mathtt{p}_{[\psi],1} \Leftrightarrow (\mathtt{p}_{[\psi_1],1} \wedge \mathtt{p}_{[\psi_2],1})) \wedge \Box(\mathtt{p}_{[\psi],0} \Leftrightarrow (\mathtt{p}_{[\psi_2],0} \wedge \mathtt{p}_{[\psi_2],0}))$
$\psi_1 \Rightarrow \psi_2$	$\Box(\mathtt{p}_{[\psi],1} \Leftrightarrow (\mathtt{p}_{[\psi_1],0} \Rightarrow \mathtt{p}_{[\psi_2],1})) \wedge \Box(\mathtt{p}_{[\psi],0} \Leftrightarrow (\mathtt{p}_{[\psi_1],1} \Rightarrow \mathtt{p}_{[\psi_2],0}))$
$\Box\psi_1$	$\Box(\mathtt{p}_{[\psi],1} \Leftrightarrow \Box(\Box(\mathtt{p}_{[\psi_1],1} \Rightarrow \Box\mathtt{p}_{\psi_1,0}) \Rightarrow \mathtt{p}_{\psi_1,1})) \wedge \Box(\mathtt{p}_{[\psi],0} \Leftrightarrow \Box\mathtt{p}_{[\psi_1],0})$

Figure 1: Definition of ϕ^{ψ}

Lemma 3.3.

(1) $f(\phi, 1) \in S4$ iff $g(\phi) \in S4$ (2) computing $g(\phi)$ requires time in $\mathcal{O}(|\phi|.log\ |\phi|)$

(3) $|g(\phi)|$ is in $\mathcal{O}(|\phi|.log\ |\phi|)$ (4) $mwp(g(\phi)) + mwn(g(\phi))$ is in $\mathcal{O}(|\phi|)$.

The proof of Lemma 3.3:(2)-(4) is by simple inspection of the definition of $g(\phi)$. The idea of the proof of Lemma 3.3(1) is to effectively build $g(\phi)$ from $f(\phi, 1)$ by successively applying transformations based on (Renaming). Such a process requires exponential-time in ϕ (since $|f(\phi, 1)|$ can be exponential in $|\phi|$). However, we can build $g(\phi)$ in a tractable way (see Lemma 3.3(2)-(4)) since g translates and renames simultaneously.

Theorem 3.4. Grz requires space in $\mathcal{O}(n^2.(log\ n)^3)$.

An equivalent statement is that there exists a deterministic Turing machine in

$$\mathbf{SPACE}(\mathcal{O}(n^2.(log\ n)^3))$$

that solves the Grz-provability problem. This follows from the facts that S4 requires space in $\mathcal{O}(n^2.log\ n)$ [13], computing $g(\phi)$ requires space in $\mathcal{O}(|\phi|.log\ |\phi|)$, and $|g(\phi)|$ is in $\mathcal{O}(|\phi|.log\ |\phi|)$. Putting these together gives that checking whether $g(\phi)$ is an S4-theorem requires space in $\mathcal{O}((|\phi|.log\ |\phi|)^2.log(|\phi|.log\ |\phi|))$, that is space in $\mathcal{O}(|\phi|^2.(log\ |\phi|)^3)$.

4 A transformation from S4 into T

Let $h : \texttt{For} \times \omega^+ \times \{0,1\} \rightarrow \texttt{For}$ be the following map ($n \in \omega^+$):

- for any $\texttt{p} \in \texttt{For}_0$, $h(\texttt{p}, n, 0) \stackrel{\text{def}}{=} h(\texttt{p}, n, 1) \stackrel{\text{def}}{=} \texttt{p}$
- $h(\neg\phi, n, i) \stackrel{\text{def}}{=} \neg h(\phi, n, 1-i)$ for $i \in \{0,1\}$
- $h(\phi_1 \wedge \phi_2, n, i) \stackrel{\text{def}}{=} h(\phi_1, n, i) \wedge h(\phi_2, n, i)$ for $i \in \{0,1\}$
- $h(\phi_1 \Rightarrow \phi_2, n, 1) \stackrel{\text{def}}{=} h(\phi_1, n, 0) \Rightarrow f(\phi_2, n, 1)$
- $h(\phi_1 \Rightarrow \phi_2, n, 0) \stackrel{\text{def}}{=} h(\phi_1, n, 1) \Rightarrow h(\phi_2, n, 0)$
- $h(\Box\phi, n, 1) \stackrel{\text{def}}{=} \Box h(\phi, n, 1)$ $\qquad h(\Box\phi, n, 0) \stackrel{\text{def}}{=} \Box^n h(\phi, n, 0)$.

Lemma 4.1. For any formula $\phi \in \texttt{For}$ and for any $1 \leq m \leq n$,

1. $\phi \Leftrightarrow h(\phi, n, 0) \in S4$ and $\phi \Leftrightarrow h(\phi, n, 1) \in S4$
2. $h(\phi, n, 0) \Rightarrow h(\phi, m, 0) \in T$ and $h(\phi, m, 1) \Rightarrow h(\phi, n, 1) \in T$.

The proof of Lemma 4.1(1) uses the facts that the rule of *replacement of equivalents* is admissible in S4 and $\Box^n\psi \Leftrightarrow \Box\psi \in S4$ for any $n \geq 1$ and for any $\psi \in \texttt{For}$. The proof of Lemma 4.1(2) is by simultaneous induction on the size of the formula. By way of example, let us show in the induction step that $h(\Box\phi, n, 0) \Rightarrow h(\Box\phi, m, 0) \in T$. By induction hypothesis, $h(\phi, n, 0) \Rightarrow h(\phi, m, 0) \in T$. It is known that the *regular rule* is admissible for T. So, by applying this rule n times on $h(\phi, n, 0) \Rightarrow h(\phi, m, 0)$, we get that $\Box^n h(\phi, n, 0) \Rightarrow \Box^n h(\phi, m, 0) \in T$. Since $\Box^n h(\phi, m, 0) \Rightarrow \Box^m h(\phi, m, 0) \in T$ (remember $m \leq n$ and $\Box\psi \Rightarrow \psi \in T$), then $\Box^n h(\phi, n, 0) \Rightarrow \Box^m h(\phi, m, 0) \in T$.

Theorem 4.2. A formula $\phi \in S4$ iff $h(\phi, (mwn(\phi)+1).mwp(\phi), 1) \in T$.

The map h is a slight variant of the map $\mathcal{M}_{S4,T}$ defined in [4]. The main difference is that we do not assume that the formulae are in negative normal form (that is why a third argument dealing with polarity is introduced here). Furthermore, since we are dealing here with validity instead of inconsistency, the treatment of the modal operators is dual. The proof of Theorem 4.2 uses the sequent calculi GS4 and GT whereas in [4] the proofs manipulate Fitting's non prefixed calculi for S4 and T [6]. Actually, in order to prove Theorem 4.2, we can show the following two properties:

1. Let $\Gamma \vdash \Delta$ be a sequent that has a (cut-free) proof in GS4 such that the maximum number of $(\vdash \Box)_{S4}$-rule inferences in any branch is n. Then, $h(\Gamma, n, 0) \vdash h(\Delta, n, 1)$ has a (cut-free) proof in GT. This is an extension of Lemma 2.2 in [4].
2. Let $\Gamma \vdash \Delta$ be a sequent such that the number of negative occurrences of $\Box$ in[4] $\bigwedge_{\phi\in\Gamma} \phi \Rightarrow \bigvee_{\psi\in\Delta} \psi$ is n. If $\Gamma \vdash \Delta$ has a (cut-free) proof in GS4, then $\Gamma \vdash \Delta$ has a (cut-free) proof in GS4 such that the $(\vdash \Box)_{S4}$-rule is applied at most $n+1$ times to the same formula in every branch. This is also an extension of Lemma 2.4 in [4].

By close examination of the definition of $h(\phi, (mwn(\phi)+1).mwp(\phi), 1)$,

1. computing $h(\phi, (mwn(\phi)+1).mwp(\phi), 1)$ requires time in $\mathcal{O}(|\phi|^3)$;
2. $|h(\phi, (mwn(\phi)+1).mwp(\phi), 1)|$ is in $\mathcal{O}(|\phi|^3)$.

So a formula $\phi \in Grz$ iff $h(g(\phi), (mwn(g(\phi))+1).mwp(g(\phi)), 1) \in T$.

1. Computing $h(g(\phi), (mwn(g(\phi))+1).mwp(g(\phi)), 1)$ requires time in $\mathcal{O}((|\phi|.log\ |\phi|)^3)$;
2. $|h(g(\phi), (mwn(g(\phi))+1).mwp(g(\phi)), 1)|$ is in $\mathcal{O}((|\phi|.log\ |\phi|)^3)$.

The relational translation from T into FO_2 (see e.g. [27]) with a smart recycling of the variables requires only linear-time and the size of the translated formula is also linear in the size of the initial formula. We warn the reader that in various places in the literature it is stated that the relational translation exponentially increases the size of formulae; this is erroneous. Using this "smart" relational transformation, the composition of various transformations in the paper provides an $\mathcal{O}((n.log\ n)^3)$-time transformation from Grz into the decidable fragment FO_2 of classical logic. It is easy to see that the resulting formula is in the guarded fragment of classical logic, for which a proof procedure based on resolution is proposed in [19]. Alternatively, after translating Grz into T, the techniques from [24] could also be used to translate T into classical logic. These are possibilities to obtain a decision procedure for Grz using theorem provers for classical logic.

We are currently investigating whether this translation can be extended to first-order Grz (FOGrz) where increasing, decreasing, and cumulative domain conditions complicate matters. But since full first-order logic is a subset of FOGrz, we clearly will not be able to ensure that the translation remains within FO_2.

References

[1] A. Avron. On modal systems having arithmetical interpretations. *The Journal of Symbolic Logic*, 49(3):935–942, September 1984.

[2] Ph. Balbiani and A. Herzig. A translation from the modal logic of provability into K4. *Journal of Applied Non-Classical Logics*, 4:73–77, 1994.

[3] G. Boolos. *The Logic of Provability.* Cambridge University Press, 1993.

[4] S. Cerrito and M. Cialdea Mayer. A polynomial translation of S4 into T and contraction-free tableaux for S4. *Logic Journal of the IGPL*, 5(2):287–300, 1997.

[5] G. D'Agostino, A. Montanari, and A. Policriti. A set-theoretical translation method for polymodal logics. *Journal of Automated Reasoning*, 15:317–337, December 1995.

[4] As is usual, the empty conjunction is understood as the *verum* logical constant $\top$ (or simply $p_{0,0} \vee \neg p_{0,0}$) and the empty disjunction is understood as the *falsum* logical constant $\bot$ (or simply $p_{0,0} \wedge \neg p_{0,0}$).

[6] M. Fitting. *Proof methods for modal and intuitionistic logics.* D. Reidel, 1983.

[7] M. Fitting. First-order modal tableaux. *J. of Automated Reasoning*, 4:191–213, 1988.

[8] M. Fürer. The computational complexity of the unconstrained limited domino problem (with implications for logical decision problems). In *Logical machines: Decision problems and complexity*, pages 312–319. LNCS 171, Springer-Verlag, 1981.

[9] R. Goré. Cut-free sequent and tableau systems for propositional Diodorian modal logics. *Studia Logica*, 53:433–457, 1994.

[10] R Goré. Cut-free display calculi for relation algebras. In *CSL96: Proc. Computer Science Logic*, pages 198–210. Springer-Verlag, LNCS 1258, 1997.

[11] R Goré. Tableaux methods for modal and temporal logics. In M. d'Agostino, D. Gabbay, R. Hähnle, and J. Posegga, editors, *Handbook of Tableaux Methods.* Kluwer, 1998.

[12] A. Herzig. *Raisonnement automatique en logique modale et algorithmes d'unification.* PhD thesis, Université P. Sabatier, Toulouse, 1989.

[13] J. Hudelmaier. Improved decision procedures for the modal logics K, T and S4. In *CSL95: Proc. Computer Science Logic*, LNCS 1092:320–334, Springer-Verlag, 1996.

[14] M. Kracht. Power and weakness of the modal display calculus. In H. Wansing, editor, *Proof theory of modal logic*, pages 93–121. Kluwer Academic Publishers, 1996.

[15] R. Ladner. The computational complexity of provability in systems of modal propositional logic. *SIAM Journal of Computing*, 6(3):467–480, September 1977.

[16] G. Mints. Gentzen-type and resolution rules part I: propositional logic. In *Int. Conf. on Computer Logic, Tallinn*, Springer Verlag, LNCS 417:198–231, 1988.

[17] Ch. Morgan. Methods for automated theorem proving in non classical logics. *IEEE Transactions on Computers*, 25(8):852–862, August 1976.

[18] M. Mortimer. On language with two variables. *Zeitschrift für Mathematik Logik und Grundlagen der Mathematik*, 21:135–140, 1975.

[19] H. de Nivelle. A resolution decision procedure for the guarded fragment. In *Proc. CADE-15*, Germany, LNAI 1421:191–204, Springer-Verlag, 1998.

[20] H.J. Ohlbach. *A resolution calculus for modal logics.* PhD thesis, FB Informatik Univ. of Kaiserslautern, 1988.

[21] H.J. Ohlbach. Optimized translation of multi modal logic into predicate logic. In A. Voronkov, editor, *LPAR'93*, pages 253–264. Springer-Verlag, LNAI 698, 1993.

[22] M. Ohnishi and K. Matsumoto. Gentzen method in modal calculi. *Osaka Mathematical Journal*, 9:113–130, 1957.

[23] Ch. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[24] R. Schmidt. Resolution is a decision procedure for many propositional modal logics. Technical Report MPI-I-97-2-002, Max-Planck-Institute Für Informatik, 1997.

[25] R. Solovay. Provability interpretations of modal logics. *Israel Journal of Mathematics*, 25:287–304, 1976.

[26] A. Troelstra and H. Schwichtenberg. *Basic Proof Theory.* CUP, 1996.

[27] J. van Benthem. *Modal logic and classical logic.* Bibliopolis, 1983.

[28] M. Vardi. Why is modal logic so robustly decidable? In *Descriptive complexity and finite models, A.M.S.*, 1997.