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

Stéphane Demri[1] and Rajeev Goré[2⋆]

[1] Laboratoire LEIBNIZ - C.N.R.S.
46 av. Félix Viallet, 38000 Grenoble, France
demri@imag.fr
[2] Automated Reasoning Project and Dept. of Computer Science
Australian National University
ACT 0200 Canberra, Australia
rpg@arp.anu.edu.au

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. [Var97,Ben99]). By far the most popular method for automating deduction in these logics has been the method of analytic tableaux (see e.g. [Fit83,Rau83,Gor99]), particularly because of the close connection between tableaux calculi and known cut-free Gentzen systems for these logics.

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. [Mor76,Ohl88,Her89,dMP95,Non96,Ohl98]). Let FO^n be the

⋆ Supported by an Australian Research Council Queen Elizabeth II Fellowship.

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 for some fixed $n \geq 2$. 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 delineated by the translation is decidable. The only known first-order decision procedure for that particular fragment except the one that mimicks the rules for K4 is the one recently published in [GHMS98]. 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. [Mor76,Ben83]) 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) [Gor94].

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 [Ohl93]. Similarly, the provability logic G[3] that admits arithmetical interpretations [Sol76] is treated within the set-theoretical framework defined in [dMP95]. Both techniques in [Ohl93,dMP95] 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 [BH94] and then a translation from K4 into classical logic (see e.g. [Ben83]).

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 *(decision) 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. [Pap94]), for

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

any fragment of classical logic that is **C**-hard with respect to $\mathbf{C}'$ many-one reductions[4], 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. [BH94,Lad77]), validity in FO^2 is **NEXPTIME**-hard [Für81] (see also [Lew80]) and **PSPACE** $\subseteq$ **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 [Ohl93,BH94,dMP95] 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 [Min88] 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 [CCM97] (see also [Fit88]). The reduction announced in the title can be obtained by translating T into FO^2, which is known to be decidable (see e.g. [Mor75]). Furthermore, the formula obtained by reduction belongs to the decidable guarded fragment of classical logic (see e.g. [ANB98]) for which a resolution decision procedure has been defined in [Niv98].

In [Boo93, Chapter 12], a (non polynomial-time) transformation from Grz into G is defined. By using renamings of subformulae, it is easy to extract from that transformation, an $\mathcal{O}(n.log\ n)$-time transformation from Grz into G [Boo93, Chapter 12]. There exists an $\mathcal{O}(n)$-time transformation from G into K4 [BH94]. There exists an $\mathcal{O}(n^4.log\ n)$-time transformation from K4 into K using [CCM97] and renamings of subformulae. Finally, there exists an $\mathcal{O}(n)$-time transformation from K into FO^2 [Ben83].

[4] Also called "transformation", see e.g. [Pap94].

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 [Hud96], 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 [Boo93,BH94,CCM97]. 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 [Gor94] (see also [DG99] for a generalisation and extension in the Display Logic framework [Bel82]). This paper is a completed version of [DG98].

2 Basic Notions

In the present paper, we assume that the modal formulae are built from a countably infinite set $\mathtt{For}_0 \stackrel{\text{def}}{=} \{\mathtt{p}_{i,j} : i, j \in \omega\}$ 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 For. An occurrence of the subformula ψ in ϕ is *positive* [resp. *negative*] iff it is in the scope of an even [resp. odd] number of negations, where as usual, every occurrence of $\phi_1 \Rightarrow \phi_2$ is treated as an occurence of $\neg(\phi_1 \wedge \neg\phi_2)$. For instance $\Box\mathtt{p}_{0,0}$ [resp. $\Box\mathtt{p}_{0,1}$] has a positive [resp. negative] occurrence in $(\Box\Box\mathtt{p}_{0,1}) \Rightarrow (\mathtt{p}_{0,1} \wedge \Box\mathtt{p}_{0,0})$. We write $mwp(\phi)$ [resp. $mwn(\phi)$] to denote the number of positive [resp. negative] occurrences of $\Box$ in ϕ. We write $|\phi|$ to denote the *size* of the formula ϕ, that is the number of symbols occurring in ϕ. ϕ is also represented as a string of characters.

We recall that the standard Hilbert system K is composed of the following axiom schemes: 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 $\mathtt{p} \Rightarrow \mathtt{q}$ 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 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 + $\Box(\Box(\mathtt{p} \Rightarrow \Box\mathtt{p}) \Rightarrow \mathtt{p}) \Rightarrow \Box\mathtt{p}$. Numerous variants of the system Grz (having the same set of theorems) can be found in the literature (see for instance [GHH97]).

We call $\mathtt{G}T$, $\mathtt{G}S4$ and $\mathtt{G}Grz$ the cut-free versions of the Gentzen-style calculi defined in [OM57,Avr84] where the sequents are built from finite sets of formulae. Moreover, the weakening rule is absorbed in the initial sequents. 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 set union. The common core of rules for the systems $\mathtt{G}T$, $\mathtt{G}S4$ and $\mathtt{G}Grz$ are presented in Figure 1.

$$\Gamma, \phi \vdash \Delta, \phi \text{ (initial sequents)} \qquad \frac{\Gamma \vdash \Delta, \phi}{\Gamma, \neg\phi \vdash \Delta}\ (\neg \vdash) \qquad \frac{\Gamma, \phi \vdash \Delta}{\Gamma \vdash \Delta, \neg\phi}\ (\vdash \neg)$$

$$\frac{\Gamma, \phi_1, \phi_2 \vdash \Delta}{\Gamma, \phi_1 \wedge \phi_2 \vdash \Delta}\ (\wedge \vdash) \qquad \frac{\Gamma \vdash \Delta, \phi_1 \quad \Gamma \vdash \Delta, \phi_2}{\Gamma \vdash \Delta, \phi_1 \wedge \phi_2}\ (\vdash \wedge)$$

$$\frac{\Gamma \vdash \Delta, \phi_1 \quad \Gamma, \phi_2 \vdash \Delta}{\Gamma, \phi_1 \Rightarrow \phi_2 \vdash \Delta}\ (\Rightarrow\vdash) \qquad \frac{\Gamma, \phi_1 \vdash \Delta, \phi_2}{\Gamma \vdash \Delta, \phi_1 \Rightarrow \phi_2}\ (\vdash\Rightarrow) \qquad \frac{\Gamma, \Box\phi, \phi \vdash \Delta}{\Gamma, \Box\phi \vdash \Delta}\ (\Box \vdash)$$

Fig. 1. Common core of rules

The introduction rules for $\Box$ on the right-hand side are the following:

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

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

where $\Box\Gamma \stackrel{\text{def}}{=} \{\Box\psi : \psi \in \Gamma\}$. Moreover, we assume that in Σ, there is no formula of the form $\Box\psi$. This restriction is not essential for completeness (and for soundness) but it is used in the proof of Lemma 5. 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 for any sequent $\Gamma \vdash \Delta$, the formula $(\bigwedge_{\phi\in\Gamma} \phi) \Rightarrow (\bigvee_{\phi\in\Delta} \phi) \in \mathcal{L}$ iff[5] the sequent $\Gamma \vdash \Delta$ is derivable in $\mathtt{G}\mathcal{L}$ (see e.g. [OM57,Avr84,Gor99]). Consequently, if $\Gamma \vdash \Delta$ is derivable in $\mathtt{G}\mathcal{L}$, then so is $\Gamma, \Gamma' \vdash \Delta, \Delta'$.

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

3 A transformation from Grz into S4

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

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

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 [BH94] for the translation from G into K4. Observe that if we replace the definition of $f(\Box\phi, 1)$ above by $f(\Box\phi, 1) \stackrel{\text{def}}{=} \Box(f(\Box(\phi \Rightarrow \Box\phi) \Rightarrow \phi, 1))$, we get the same map.

Since the rule of *replacement of equivalents* is admissible in Grz, one can show by induction on the length of ϕ that for any $\phi \in \texttt{For}$ and for any $i \in \{0, 1\}$, $\phi \Leftrightarrow f(\phi, i) \in Grz$. Moreover,

Lemma 1. *For any $\phi \in \texttt{For}$, $\phi \Rightarrow f(\phi, 1) \in K \subseteq S4$ and $f(\phi, 0) \Rightarrow \phi \in K \subseteq S4$.*

Proof. The proof is by simultaneous induction on the structure 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) $\phi_1 \wedge \phi_2 \Rightarrow f(\phi_1 \wedge \phi_2, 1) \in K$ (2) $\Box\phi_1 \Rightarrow f(\Box\phi_1, 1) \in K$

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

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

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

Proof. 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 $\mathtt{G}Grz$. 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 in $\mathtt{G}S4$. Here, f is extended to sets of formulae in the natural way. So, we shall conclude that $\vdash f(\phi, 1)$ is derivable in $\mathtt{GS4}$ and therefore $f(\phi, 1) \in S4$. The proof is by induction on the structure of the derivations.

Base case: When $\Gamma \vdash \Delta$ is an initial sequent $\Gamma', \psi \vdash \psi, \Delta'$, we can show that $f(\Gamma', 0), f(\psi, 0) \vdash f(\psi, 1), f(\Delta', 1)$ has a cut-free proof in $\mathtt{G}S4$ since $f(\psi, 0) \Rightarrow f(\psi, 1) \in S4$. By completeness of $\mathtt{G}S4$, $f(\psi, 0) \vdash f(\psi, 1)$ has a proof in $\mathtt{G}S4$.

Induction step: The structural rules pose no difficulties because by definition f is homomorphic with respect to the comma. By way of example, the proof step (in $\mathtt{G}Grz$)

$$\dfrac{\vdots \atop \Box\Gamma', \Box(\psi \Rightarrow \Box\psi) \vdash \psi}{\Gamma, \Box\Gamma' \vdash \Box\psi, \Delta} \; (\vdash \Box)_{Grz}$$

is transformed into the proof steps (in $\mathtt{G}S4$)

$$\dfrac{\dfrac{\vdots \atop \Box f(\Gamma', 0), \Box(f(\psi, 1) \Rightarrow \Box f(\psi, 0)) \vdash f(\psi, 1)}{\Box f(\Gamma', 0) \vdash \Box(f(\psi, 1) \Rightarrow \Box f(\psi, 0)) \Rightarrow f(\psi, 1)} \; (\vdash\Rightarrow)}{f(\Gamma, 0), \Box f(\Gamma', 0) \vdash \Box(\Box(f(\psi, 1) \Rightarrow \Box f(\psi, 0)) \Rightarrow f(\psi, 1)), f(\Delta, 1)} \; (\vdash \Box)_{S4}$$

The induction hypothesis is used here since $\Box f(\Gamma', 0), \Box(f(\psi, 1) \Rightarrow \Box f(\psi, 0)) \vdash f(\psi, 1)$ has a (cut-free) proof in $\mathtt{G}S4$. Furthermore, by definition,

- $f(\Box\Gamma', 0) = \Box f(\Gamma', 0)$; $f(\Box\psi, 1) = \Box(\Box(f(\psi, 1) \Rightarrow \Box f(\psi, 0)) \Rightarrow f(\psi, 1))$;
- $f(\Box(\psi \Rightarrow \Box\psi), 0) = \Box(\Box(f(\psi, 1) \Rightarrow \Box f(\psi, 0)))$.

Observe that $f(\Gamma, 0)$ does not contain any formula of the form $\Box\psi'$. The proof (in $\mathtt{G}Grz$)

$$\dfrac{\vdots \atop \Gamma, \Box\psi, \psi \vdash \Delta}{\Gamma, \Box\psi \vdash \Delta} \; (\Box \vdash)$$

is transformed into the proof (in $\mathtt{G}S4$)

$$\frac{\begin{array}{c}\vdots\\ f(\Gamma,0), \Box f(\psi,0), f(\psi,0) \vdash f(\Delta,1)\end{array}}{f(\Gamma,0), \Box f(\psi,0) \vdash f(\Delta,1)}\ (\Box \vdash)$$

Indeed, $f(\Box\psi, 0) = \Box f(\psi, 0)$. The other cases are not difficult to obtain and they are omitted here.

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 [Min88]. Specifically, we have, (Renaming) $\phi \in S4$ 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 enumeration (without repetition) of all the subformulae of ϕ in increasing order with respect to the size such that the n first formulae are all the atomic propositions occurring in ϕ. 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 $i \in \{1, \ldots, m\}$, we associate a formula ψ_i as shown in Figure 2 and let $g(\phi) \stackrel{\text{def}}{=} (\bigwedge_{i=1}^{m} \psi_i) \Rightarrow \mathtt{p}_{m,1}$.

Form of ϕ_i	ψ_i
$\mathtt{p}$	$\Box(\mathtt{p}_{i,0} \Leftrightarrow \mathtt{p}_{i,1})$
$\neg\phi_j$	$\Box(\mathtt{p}_{i,1} \Leftrightarrow \neg\mathtt{p}_{j,0}) \wedge \Box(\mathtt{p}_{i,0} \Leftrightarrow \neg\mathtt{p}_{j,1})$
$\phi_{i_1} \wedge \phi_{i_2}$	$\Box(\mathtt{p}_{i,1} \Leftrightarrow (\mathtt{p}_{i_1,1} \wedge \mathtt{p}_{i_2,1})) \wedge \Box(\mathtt{p}_{i,0} \Leftrightarrow (\mathtt{p}_{i_1,0} \wedge \mathtt{p}_{i_2,0}))$
$\phi_{i_1} \Rightarrow \phi_{i_2}$	$\Box(\mathtt{p}_{i,1} \Leftrightarrow (\mathtt{p}_{i_1,0} \Rightarrow \mathtt{p}_{i_2,1})) \wedge \Box(\mathtt{p}_{i,0} \Leftrightarrow (\mathtt{p}_{i_1,1} \Rightarrow \mathtt{p}_{i_2,0}))$
$\Box\phi_j$	$\Box(\mathtt{p}_{i,1} \Leftrightarrow \Box(\Box(\mathtt{p}_{j,1} \Rightarrow \Box\mathtt{p}_{j,0})) \Rightarrow \mathtt{p}_{j,1})) \wedge \Box(\mathtt{p}_{i,0} \Leftrightarrow \Box\mathtt{p}_{j,0})$

Fig. 2. Definition of ψ_i

Lemma 2.
(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* $\mathcal{O}(|\phi|)$.

Proof. (2)-(4) is by simple inspection of the definition of $g(\phi)$. The idea of the proof of (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 (2)-(4)) since g translates and renames simultaneously.
(1) Let us build $g(\phi)$ from $f(\phi, 1)$ by successively applying transformations based on (Renaming). For any atomic proposition $\mathtt{q} = \phi_i$ occurring in $f(\phi, 1)$, replace the positive [resp. negative] occurrences of $\mathtt{q}$ by $\mathtt{p}_{i,1}$ [resp. $\mathtt{p}_{i,0}$]. Let us say that we obtain the formula ψ (this shall be our current working formula). The *constraint* formula, say C, is defined as $C \stackrel{\text{def}}{=} \bigwedge_{i=1}^{n} \Box(\mathtt{p}_{i,1} \Leftrightarrow \mathtt{p}_{i,0})$. Along the steps, we shall have that $f(\phi, 1) \in S4$ iff $C \Rightarrow \psi \in S4$. The next steps consist of replacing subformulae ψ' in ψ by their renaming equivalent and then to update C appropriately until $\psi = \mathtt{p}_{m,1}$. For instance, take a subformula $\psi' = \mathtt{p}_{i,1} \wedge \mathtt{p}_{j,1}$ in ψ. Replace every occurrence of $\mathtt{p}_{i,1} \wedge \mathtt{p}_{j,1}$ in ψ by $\mathtt{p}_{k,1}$ with $\phi_k = \phi_i \wedge \phi_j$. The constraint formula C is updated as follows: $C := C \wedge \Box(\mathtt{p}_{k,1} \Leftrightarrow (\mathtt{p}_{i,1} \wedge \mathtt{p}_{j,1}))$. The other cases are omitted and they use the decomposition from Figure 2. So, when ψ is equal to $\mathtt{p}_{m,1}$, $f(\phi, 1) \in S4$ iff $C \Rightarrow \mathtt{p}_{m,1} \in S4$. It is easy to see that $(\bigwedge_{i=1}^{m} \psi_i) \Rightarrow \mathtt{p}_{m,1} \in S4$ iff $C \Rightarrow \mathtt{p}_{m,1}$. Indeed, the set of conjuncts of C is a subset of the set of conjuncts of $\bigwedge_{i=1}^{m} \psi_i$. So, if $C \Rightarrow \mathtt{p}_{m,1} \in S4$, then $g(\phi) \in S4$. In order to show that the converse also holds, let us define the binary relation DEP between atomic propositions. Let $\mathtt{p}_{i_1,j_1}$ and $\mathtt{p}_{i_2,j_2}$ be atomic propositions occurring in $\bigwedge_{i=1}^{m} \psi_i$. We write $\mathtt{p}_{i_1,j_1}$ DEP $\mathtt{p}_{i_2,j_2}$ to denote that there is a conjunct of $\bigwedge_{i=1}^{m} \psi_i$ of the form $\Box(\psi'_1 \Leftrightarrow \psi'_2)$ such that either $\mathtt{p}_{i_1,j_1}$ occurs in ψ'_1 and $\mathtt{p}_{i_2,j_2}$ occurs in ψ'_2 or $\mathtt{p}_{i_1,j_1}$ occurs in ψ'_2 and $\mathtt{p}_{i_2,j_2}$ occurs in ψ'_1. Let DEP^* be the smallest equivalence relation including DEP. It is easy to see that if $g(\phi) \in S4$, then $C \Rightarrow \mathtt{p}_{m,1} \in S4$ since for all the atomic propositions $\mathtt{q}$ occurring in $\bigwedge_{i=1}^{m} \psi_i$ but not in C, not $\mathtt{q} DEP^* \mathtt{p}_{m,1}$.

Theorem 2. *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 $\mathcal{O}(n^2.log\ n)$ [Hud96], 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 $\mathcal{O}(|\phi|^2.(log\ |\phi|)^3)$. By the way, one can show that Grz is

PSPACE-hard by using mappings from propositional intuitionistic logic into Grz (see e.g. [CZ97]).

4 A transformation from S4 into T

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

- for any $\texttt{p} \in \texttt{For}_0$, $h(\texttt{p}, n, 0) \stackrel{\text{def}}{=} h(\texttt{p}, n, 1) \stackrel{\text{def}}{=} \texttt{p}$
- $h(\neg\phi, n, i) \stackrel{\text{def}}{=} \neg h(\phi, n, 1-i)$
- $h(\phi_1 \wedge \phi_2, n, i) \stackrel{\text{def}}{=} h(\phi_1, n, i) \wedge h(\phi_2, n, i)$
- $h(\phi_1 \Rightarrow \phi_2, n, i) \stackrel{\text{def}}{=} h(\phi_1, n, 1-i) \Rightarrow h(\phi_2, n, i)$
- $h(\Box\phi, n, 1) \stackrel{\text{def}}{=} \Box h(\phi, n, 1)$
- $h(\Box\phi, n, 0) \stackrel{\text{def}}{=} \begin{cases} \Box^n h(\phi, n, 0) \text{ if } n \geq 1 \\ \Box h(\phi, n, 0) \text{ otherwise} \end{cases}$

The map h is a slight variant of the map $\mathcal{M}_{S4,T}$ defined in [CCM97] which itself is a variant of a map defined in [Fit88]. The main difference is that we do not assume that the formulae are in negative normal form (which is why a third argument dealing with polarity is introduced here). In that sense, we follow [Fit88, Section 3]. Furthermore, since we are dealing here with validity instead of inconsistency, the treatment of the modal operators is dual.

Lemma 3. *For any formula $\phi \in \texttt{For}$ and for any $0 \leq m \leq n$,*

(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* $h(\phi, m, 1) \Rightarrow h(\phi, n, 1) \in T$.
(3) $h(\phi, n, 0) \Rightarrow h(\phi, n, 1) \in T$.

Proof. The proof of (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 (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 $\Box^n h(\phi, n, 0) \Rightarrow \Box^m h(\phi, m, 0) \in T$.
(3) If $n = 0$, then $h(\phi, n, 0) = h(\phi, n, 1) = \phi$. Now assume $n \geq 1$. The proof is by induction on the structure of ϕ. The base case when ϕ is

an atomic proposition is immediate. Let us treat the cases $\phi = \neg\phi'$ and $\phi = \Box\phi'$ in the induction step. By Induction Hypothesis, $h(\phi', n, 0) \Rightarrow h(\phi', n, 1) \in T$. By manipulation at the propositional level, $\neg h(\phi', n, 1) \Rightarrow \neg h(\phi', n, 0) \in T$. By definition of h, $h(\neg\phi', n, 0) \Rightarrow h(\neg\phi', n, 1) \in T$. Moreover, by applying n times the regular rule (admissible in T) on $h(\phi', n, 0) \Rightarrow h(\phi', n, 1)$, we get $\Box^n h(\phi', n, 0) \Rightarrow \Box^n h(\phi', n, 1) \in T$. Moreover,

- $\Box^n h(\phi', n, 1) \Rightarrow \Box h(\phi', n, 1) \in T$;
- $\Box^n h(\phi', n, 0) = h(\Box\phi', n, 0)$;
- $\Box h(\phi', n, 1) = h(\Box\phi', n, 1)$.

So, $h(\Box\phi', n, 0) \Rightarrow h(\Box\phi', n, 1) \in T$.

The map h is extended to sets of formulae in the most natural way.

Lemma 4. *Let $\Gamma \vdash \Delta$ be a sequent that has a (cut-free) proof Π in* $\mathtt{G}S4$ *such that the maximum number of $(\vdash \Box)_{S4}$-rule inferences in any branch is at most n. Then, $h(\Gamma, n, 0) \vdash h(\Delta, n, 1)$ has a (cut-free) proof in* $\mathtt{G}T$*.*

Lemma 4 is an extension of Lemma 2.2 in [CCM97].

Proof. The proof is by double induction on n and then on the length of the proof Π of $\Gamma \vdash \Delta$. The length of Π is just the number of nodes of the proof tree.
Base case (i): $n = 0$. By definition, $h(\Gamma, 0, 0) = \Gamma$ and $h(\Delta, 0, 1) = \Delta$. Any proof of $\Gamma \vdash \Delta$ in $\mathtt{G}S4$ with no applications of $(\vdash \Box)_{S4}$ is also a proof of $\Gamma \vdash \Delta$ in $\mathtt{G}T$.
Induction step (i): assume that for any sequent $\Gamma \vdash \Delta$ having a (cut-free) proof in GS4 such that the maximum number of $(\vdash \Box)_{S4}$-rule inferences in any branch is at most $n - 1 \geq 0$, $h(\Gamma, n-1, 0) \vdash h(\Delta, n-1, 1)$ has a (cut-free) proof in GT. Now, let $\Gamma \vdash \Delta$ be a sequent that has a (cut-free) proof Π in GS4 such that the maximum number of $(\vdash \Box)_{S4}$-rule inferences in any branch is at most n. We use an induction on the length of Π.
Base case (ii): $\Gamma \vdash \Delta$ is an initial sequent $\Gamma', \phi \vdash \Delta', \phi$. By Lemma 3(3), $h(\phi, n, 0) \Rightarrow h(\phi, n, 1) \in T$. So, $h(\phi, n, 0) \vdash h(\phi, n, 1)$ has a cut-free proof in $\mathtt{G}T$ by completeness of $\mathtt{G}T$ with respect to T. Hence, $h(\Gamma', n, 0), h(\phi, n, 0) \vdash h(\Delta', n, 1), h(\phi, n, 1)$ has a cut-free proof in $\mathtt{G}T$.
Induction step (ii): assume that for any sequent $\Gamma \vdash \Delta$ having a (cut-free) proof Π of length at most $n' - 1 \geq 1$ in GS4 such that the maximum number of $(\vdash \Box)_{S4}$-rule inferences in any branch is at most n, $h(\Gamma, n, 0) \vdash h(\Delta, n, 1)$ has a (cut-free) proof in GT. Now, let $\Gamma \vdash \Delta$ be a sequent that has a (cut-free) proof Π in GS4 of length n' such that the

maximum number of $(\vdash \Box)_{S4}$-rule inferences in any branch is at most n. Among the Boolean connectives, we only treat here the case for the conjunction since the cases for $\neg$ and $\Rightarrow$ are similar. The proof Π below (in $\mathtt{G}S4$)

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma', \phi_1, \phi_2 \vdash \Delta'\end{array}}{\Gamma', \phi_1 \wedge \phi_2 \vdash \Delta'}\ (\wedge \vdash)$$

is transformed into the proof below (in $\mathtt{G}T$) using the induction hypothesis (ii)

$$\dfrac{\begin{array}{c}\vdots\\ h(\Gamma', n, 0), h(\phi_1, n, 0), h(\phi_2, n, 0) \vdash h(\Delta', n, 1)\end{array}}{h(\Gamma', n, 0), h(\phi_1 \wedge \phi_2, n, 0) \vdash h(\Delta', n, 1)}\ (\wedge \vdash)$$

The proof Π below (in $\mathtt{G}S4$)

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma' \vdash \Delta', \phi_1 \quad \Gamma' \vdash \Delta', \phi_2\end{array}}{\Gamma' \vdash \Delta', \phi_1 \wedge \phi_2}\ (\vdash \wedge)$$

is transformed into the proof below (in $\mathtt{G}T$) using the induction hypothesis (ii)

$$\dfrac{\begin{array}{c}\vdots\\ h(\Gamma', n, 0) \vdash h(\Delta', n, 1), h(\phi_1, n, 1) \quad h(\Gamma', n, 0) \vdash h(\Delta', n, 1), h(\phi_2, n, 1)\end{array}}{h(\Gamma', n, 0) \vdash h(\Delta', n, 1), h(\phi_1 \wedge \phi_2, n, 1)}\ (\vdash \wedge)$$

Consider the proof Π below:

$$\dfrac{\begin{array}{c}\Pi'\\ \vdots\\ \Box\Gamma'' \vdash \phi\end{array}}{\Gamma', \Box\Gamma'' \vdash \Box\phi, \Delta'}\ (\vdash \Box)_{S4}$$

In the proof Π' of $\Box\Gamma'' \vdash \phi$ in $\mathtt{G}S4$, the maximum number of $(\vdash \Box)_{S4}$-rule inferences in any branch is less than $n-1$. By induction hypothesis (i), $h(\Box\Gamma'', n-1, 0) \vdash h(\phi, n-1, 1)$ has a cut-free proof, say Π'', in $\mathtt{G}T$. So, the proof below is obtained in $\mathtt{G}T$:

$$\dfrac{\begin{array}{c}\Pi''\\ \vdots\\ \Box^{n-1}h(\Gamma'', n-1, 0) \vdash h(\phi, n-1, 1)\end{array}}{h(\Gamma', n, 0), \Box^{n}h(\Gamma'', n-1, 0) \vdash \Box h(\phi, n-1, 1), h(\Delta', n, 1)}\ (\vdash \Box)_T$$

For $\psi \in \Gamma''$, $h(\psi, n, 0) \Rightarrow h(\psi, n-1, 0) \in T$ by Lemma 3(2). By using n applications of the regular rule, for $\psi \in \Gamma''$, $\Box^n h(\psi, n, 0) \Rightarrow \Box^n h(\psi, n-1, 0) \in T$. Similarly, by Lemma 3(2) $h(\Box\phi, n-1, 1) \Rightarrow h(\Box\phi, n, 1) \in T$. By soundness of $\mathtt{G}T$, the formula $\varphi \in T$ where:

$$\varphi \stackrel{\text{def}}{=} ((\bigwedge_{\psi \in \Gamma'} h(\psi, n, 0)) \wedge (\bigwedge_{\psi \in \Gamma''} \Box^n h(\psi, n-1, 0))) \Rightarrow (h(\Box\phi, n-1, 1) \vee \bigvee_{\psi \in \Delta'} h(\psi, n, 1)).$$

For $\psi \in \Gamma''$, $\Box^n h(\psi, n-1, 0)$ occurs negatively in φ and $h(\Box\phi, n-1, 1)$ occurs positively in φ. By the Monotonicity of Entailment Lemma [AM86],

$$((\bigwedge_{\psi \in \Gamma'} h(\psi, n, 0)) \wedge (\bigwedge_{\psi \in \Gamma''} \Box^n h(\psi, n, 0))) \Rightarrow (h(\Box\phi, n, 1) \vee \bigvee_{\psi \in \Delta'} h(\psi, n, 1)) \in T$$

By completeness of $\mathtt{G}T$, we get that $h(\Gamma', n, 0), h(\Box\Gamma'', n, 0) \vdash h(\Box\phi, n, 1), h(\Delta', n, 1)$ has a cut-free proof in $\mathtt{G}T$. In order to conclude the proof, let us treat the last case. Consider the proof Π below in $\mathtt{G}S4$:

$$\dfrac{\begin{matrix}\vdots \\ \Gamma', \Box\phi, \phi \vdash \Delta'\end{matrix}}{\Gamma', \Box\phi \vdash \Delta'}\ (\Box \vdash)$$

By induction hypothesis (ii), $h(\Gamma', n, 0), \Box^n h(\phi, n, 0), h(\phi, n, 0) \vdash h(\Delta', n, 1)$ has a cut-free proof in $\mathtt{G}T$. So,

$$s_1 \stackrel{\text{def}}{=} h(\Gamma', n, 0), \Box^n h(\phi, n, 0), \Box^{n-1} h(\phi, n, 0), \ldots, \Box h(\phi, n, 0), h(\phi, n, 0) \vdash h(\Delta', n, 1)$$

has also a cut-free proof in $\mathtt{G}T$. The above proof is transformed into (in $\mathtt{G}T$)

$$\dfrac{\dfrac{\begin{matrix}\vdots \\ s_1\end{matrix}}{h(\Gamma', n, 0), \Box^n h(\phi, n, 0), \Box^{n-1} h(\phi, n, 0), \ldots, \Box h(\phi, n, 0) \vdash h(\Delta', n, 1)}\ (\Box \vdash)}{h(\Gamma', n, 0), \Box^n h(\phi, n, 0), \Box^{n-1} h(\phi, n, 0), \ldots, \Box^2 h(\phi, n, 0) \vdash h(\Delta', n, 1)}\ (\Box \vdash)$$

$$\dfrac{\begin{matrix}\vdots \\ h(\Gamma', n, 0), \Box^n h(\phi, n, 0), \Box^{n-1} h(\phi, n, 0) \vdash h(\Delta', n, 1)\end{matrix}}{h(\Gamma', n, 0), h(\Box\phi, n, 0) \vdash h(\Delta', n, 1)}\ (\Box \vdash)$$

Lemma 5. *Let $\Gamma \vdash \Delta$ be a sequent such that the number of negative occurrences of $\Box$ in $\bigwedge_{\phi \in \Gamma} \phi \Rightarrow \bigvee_{\psi \in \Delta} \psi$ is n. If $\Gamma \vdash \Delta$ has a (cut-free) proof in $\mathtt{G}S4$, then $\Gamma \vdash \Delta$ has a (cut-free) proof in $\mathtt{G}S4$ such that the $(\vdash \Box)_{S4}$-rule is applied at most $n+1$ times to the same formula in every branch.*

Lemma 5 is also an extension of Lemma 2.4 in [CCM97]. However, its proof mainly relies on the analysis of the proof of [CCM97, Lemma 2.4]. So it is included here in order to make the paper self-contained.

Proof. First, observe that if $\Gamma \vdash \Delta$ is derivable in $\mathtt{G}S4$ and if ψ has a negative [resp. positive] occurrence in $(\bigwedge_{\phi \in \Gamma} \phi) \Rightarrow (\bigvee_{\phi \in \Delta} \phi)$, then for any cut-free proof Π of $\Gamma \vdash \Delta$, every occurrence of ψ in Π can only occur in the left-hand side [resp. in the right-hand side] of sequents. So if the inference below

$$\frac{\Box\Gamma'' \vdash \phi}{\Gamma', \Box\Gamma'' \vdash \Box\phi, \Delta'} \ (\vdash \Box)_{S4}$$

occurs in a proof Π of $\Gamma \vdash \Delta$, then any $\Box\psi \in \Box\Gamma''$ occurs with negative polarity in $(\bigwedge_{\phi \in \Gamma} \phi) \Rightarrow (\bigvee_{\phi \in \Delta} \phi)$. Moreover, consider the following $(\vdash \Box)_{S4}$ inferences in a proof Π of $\Gamma \vdash \Delta$:

$$\begin{array}{c}
\dfrac{\Box\Gamma'_2 \vdash \phi_2}{\Gamma_2, \Box\Gamma'_2 \vdash \Box\phi_2, \Delta_2} \ (\vdash \Box)_{S4} \\
\vdots \\
\dfrac{\Box\Gamma'_1 \vdash \phi_1}{\Gamma_1, \Box\Gamma'_1 \vdash \Box\phi_1, \Delta_1} \ (\vdash \Box)_{S4} \\
\vdots
\end{array}$$

Then $\Gamma'_1 \subseteq \Gamma'_2$. Let Π be a (cut-free) proof of $\Gamma \vdash \Delta$ in $\mathtt{G}S4$. Assume there is a branch in Π containing $n + 1 + k$ $(k \geq 1)$ $(\vdash \Box)_{S4}$ inferences introducing the same formula $\Box\psi$. Let us eliminate at least one $(\vdash \Box)_{S4}$ inference on that branch as done in [CCM97]. Consider the sequence inf_1, $\ldots$, inf_{n+1+k} of inferences of the form $(1 \leq i \leq n + 1 + k)$,

$$\frac{\Box\Gamma'_i \vdash \psi}{\Gamma_i, \Box\Gamma'_i \vdash \Box\psi, \Delta_i} \ (\vdash \Box)_{S4}$$

We assume that if $i < j$, then inf_j occurs above inf_i. Let Γ' be the set of the formulae of the form $\Box\psi'$ where $\Box\psi'$ has a negative occurrence in $(\bigwedge_{\phi \in \Gamma} \phi) \Rightarrow (\bigvee_{\phi \in \Delta} \phi)$. Since $\Gamma'_1 \subseteq \ldots \subseteq \Gamma'_{n+1+k}$ and $card(\Gamma') = n$, there exist $i_0 \in \{1, \ldots, n+1\}$ and $j_0 \in \{i_0, \ldots, n+2\}$ such that $\Gamma'_{i_0} = \Gamma'_{j_0}$. So, in that branch of Π, we can replace the sequence shown below left by the sequence shown below right:

$$\dfrac{\dfrac{\begin{matrix}\Pi' \\ \vdots \\ \Box\Gamma'_{j_0} \vdash \psi\end{matrix}}{\Gamma_{j_0}, \Box\Gamma'_{j_0} \vdash \Box\psi, \Delta_{j_0}} (\vdash \Box)_{S4} \\ \vdots \\ \Box\Gamma'_{i_0} \vdash \psi}{\Gamma_{i_0}, \Box\Gamma'_{i_0} \vdash \Box\psi, \Delta_{i_0}} (\vdash \Box)_{S4} \qquad \dfrac{\begin{matrix}\Pi' \\ \vdots \\ \Box\Gamma'_{j_0} \vdash \psi\end{matrix}}{\Gamma_{j_0}, \Box\Gamma'_{j_0} \vdash \Box\psi, \Delta_{j_0}} (\vdash \Box)_{S4}$$

Theorem 3. *A formula* $\phi \in S4$ *iff* $h(\phi, (mwn(\phi) + 1).mwp(\phi), 1) \in T$.

Theorem 3 is a mere consequence of Lemma 4 and Lemma 5. Its proof uses the sequent calculi $\mathtt{G}S4$ and $\mathtt{G}T$ whereas in [CCM97] the proofs manipulate Fitting's non prefixed calculi for S4 and T [Fit83]. Observe the map h is a variant of a map defined in [Fit88]. Let us write $h'(\phi)$ to denote the formula $h(\phi, (mwn(\phi) + 1).mwp(\phi), 1)$.

By close examination of the definition of $h'(\phi)$,

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

So a formula $\phi \in Grz$ iff $h'(g(\phi)) \in T$.

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

The relational translation from T into FO^2 (see e.g. [Ben83]) 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 (see e.g. [ANB98]), for which a proof procedure based on resolution is proposed in [Niv98]. Alternatively, after translating Grz into T, the techniques from [Sch97] 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). But the set of valid formulae for first-order Gödel-Löb logic, a close cousin of FOGrz, is not recursively enumerable [Boo93, Chapt. 17], and we suspect that this result also holds for FOGrz.

References

[AM86] M. Abadi and Z. Manna. Modal theorem proving. In J. H. Siekmann, editor, *CADE-8*, pages 172–189. Springer Verlag, LNCS 230, 1986.

[ANB98] H. Andreka, I. Nemeti, and J. van Benthem. Modal languages and bounded fragments of predicate logic. *Journal of Philosophical Logic*, 27(3):217–274, 1998.

[Avr84] A. Avron. On modal systems having arithmetical interpretations. *The Journal of Symbolic Logic*, 49(3):935–942, 1984.

[Bel82] N. Belnap. Display logic. *Journal of Philosophical Logic*, 11:375–417, 1982.

[Ben83] J. van Benthem. *Modal logic and classical logic.* Bibliopolis, 1983.

[Ben99] J. van Benthem. The Range of Modal Logic - An Essay in Memory of George Gargov. *Journal of Applied Non-Classical Logics*, 1999. To appear.

[BH94] 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.

[Boo93] G. Boolos. *The Logic of Provability.* Cambridge University Press, 1993.

[CCM97] 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.

[CZ97] A. Chagrov and M. Zakharyaschev. *Modal Logic.* Clarendon Press, Oxford, 1997.

[DG98] S. Demri and R. Goré. An $\mathcal{O}((n.log\ n)^3)$-time transformation from Grz into decidable fragments of classical first-order logic. In *2nd International Workshop on First-Order Theorem Proving, Vienna*, pages 127–134. TU-Wien Technical Report E1852-GS-981, 1998.

[DG99] S. Demri and R. Goré. Theoremhood preserving maps as a characterisation of cut elimination for provability logics. Technical Report, A.R.P., A.N.U., 1999. Forthcoming.

[dMP95] G. d'Agostino, A. Montanari, and A. Policriti. A set-theoretical translation method for polymodal logics. *Journal of Automated Reasoning*, 15:317–337, 1995.

[Fit83] M. Fitting. *Proof methods for modal and intuitionistic logics.* D. Reidel Publishing Co., 1983.

[Fit88] M. Fitting. First-order modal tableaux. *Journal of Automated Reasoning*, 4:191–213, 1988.

[Für81] 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.

[GHH97] R. Goré, W. Heinle, and A. Heuerding. Relations between propositional normal modal logics: an overview. *Journal of Logic and Computation*, 7(5):649–658, 1997.

[GHMS98] H. Ganzinger, U. Hustadt, C. Meyer, and R. Schmidt. A resolution-based decision procedure for extensions of K4. In *2nd Workshop on Advances in Modal Logic (AiML'98), Uppsala, Sweden*, 1998. to appear.

[Gor94] R. Goré. Cut-free sequent and tableau systems for propositional Diodorian modal logics. *Studia Logica*, 53:433–457, 1994.

[Gor99] 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, Dordrecht, 1999. To appear.

[Her89] A. Herzig. *Raisonnement automatique en logique modale et algorithmes d'unification*. PhD thesis, Université P. Sabatier, Toulouse, 1989.

[Hud96] J. Hudelmaier. Improved decision procedures for the modal logics K, T and S4. In H. Buning, editor, *Computer Science Logic (CSL'95)*, pages 320–334. LNCS 1092, Springer-Verlag, 1996.

[Lad77] R. Ladner. The computational complexity of provability in systems of modal propositional logic. *SIAM Journal of Computing*, 6(3):467–480, 1977.

[Lew80] H. Lewis. Complexity results for classes of quantificational formulas. *Journal of Computer and System Sciences*, 21:317–353, 1980.

[Min88] G. Mints. Gentzen-type and resolution rules part I: propositional logic. In P. Martin-Löf and G. Mints, editors, *International Conference on Computer Logic, Tallinn*, pages 198–231. Springer Verlag, LNCS 417, 1988.

[Mor75] M. Mortimer. On language with two variables. *Zeitschrift für Mathematik Logik und Grundlagen der Mathematik*, 21:135–140, 1975.

[Mor76] Ch. Morgan. Methods for automated theorem proving in non classical logics. *IEEE Transactions on Computers*, 25(8):852–862, 1976.

[Niv98] H. de Nivelle. A resolution decision procedure for the guarded fragment. In C. Kirchner and H. Kirchner, editors, *CADE-15, Lindau, Germany*, pages 191–204. LNAI 1421, Springer-Verlag, 1998.

[Non96] A. Nonnengart. Resolution-based calculi for modal and temporal logics. In M. McRobbie and J. Slaney, editors, *CADE-13*, pages 599–612. LNAI 1104, Springer-Verlag, 1996.

[Ohl88] H.J. Ohlbach. *A resolution calculus for modal logics*. PhD thesis, FB Informatik Univ. of Kaiserslautern, 1988.

[Ohl93] 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.

[Ohl98] H. J. Ohlbach. Combining Hilbert style and semantic reasoning in a resolution framework. In C. Kirchner and H. Kirchner, editors, *CADE-15, Lindau, Germany*, pages 205–219. LNAI 1421, Springer-Verlag, 1998.

[OM57] M. Ohnishi and K. Matsumoto. Gentzen method in modal calculi. *Osaka Mathematical Journal*, 9:113–130, 1957.

[Pap94] Ch. Papadimitriou. *Computational Complexity*. Addison-Wesley Publishing Company, 1994.

[Rau83] W. Rautenberg. Modal tableau calculi and interpolation. *The Journal of Philosophical Logic*, 12:403–423, 1983.

[Sch97] R. Schmidt. *Optimised Modal Translation and Resolution*. PhD thesis, Fakultät der Universität des Saarlandes, 1997.

[Sol76] R. Solovay. Provability interpretations of modal logics. *Israel Journal of Mathematics*, 25:287–304, 1976.

[Var97] M. Vardi. Why is modal logic so robustly decidable? In *Descriptive complexity and finite models, A.M.S.*, 1997.