2009

TR-2009003: On Proof Realization on Modal Logic

Ren-June Wang

On Proof Realization on Modal Logic

Ren-June Wang
Computer Science
CUNY Graduate Center
365 Fifth Avenue, New York, NY 10016
rwang@gc.cuny.edu

April 5, 2009

Abstract

Artemov's *Logic of Proof*, LP, is an explicit proof counterpart of S4. Their formal connection is built through the *realization theorem*, that every S4 theorem can be converted to an LP theorem by substituting *proof terms* for provability modals. Instead of the realization of theorems, what is concerned in this paper is the realization of proofs. We will show that only a subclass of S4 proofs, called non-circular proofs, can be realized as LP proofs in this way. Furthermore, we introduce a numerical version of LP, called $S4^{\Delta}$, to constructively prove that every S4 theorem has a non-circular proof. These results provide a new algorithmic proof of the *realization theorem*.

1 Introduction

Providing an arithmetic foundation to the intuitionistic logic is a long standing problem, which Gödel ([14]) took a first step to solve by embedding the intuitionistic logic into a calculus of provability known as S4, and was eventually solved by Artemov with his *Logic of Proofs*, LP ([1, 2]). LP includes formulas of the type $t{:}F$, read as "*t is a proof of F*," to represent explicit proofs in formal arithmetic with t called *proof terms* or *proof polynomials*. This idea was also suggested by Gödel ([13]) but unpublished until appearing in [8]. In [1, 2] an intended arithmetic interpretation of proof terms is given together with a completeness result. Finally, the *realization theorem* shows that every S4 theorem can be converted to an LP theorem by substituing proof terms for provability modal occurrences. This completes the project.

Rencently, LP and other LP-style logics have joined the family of epistemic logics to be *Justifcation Logics*, where formulas $t : F$ are re-understood as "*t is a justfication of F*", and semantics based on the reading has been built. Accordingly, the validity of the *realization theorem* shows that there is justification structure inherent in S4 and other normal modal logics, which have long been considered as standard epistemic logics (cf. [12], [11], [3], [4]).

The *realization theorem* connects logics LP and S4 by theorems, but it also suggests a deeper connection between proofs in the two logics. As we can see that the axioms and inference rules in the standard S4 system and LP are almost entirely corresponding to each other, we can consider – once we make variations on the sytems – such a concept of *proof realization* which demands that the substitution of proof terms for modals produces an *axiom to axiom and derived line to derived line* correspondence beteeen proofs. Then we discover, despite the parallelism of the two systems and the validity of the *realization theorem*, that not every S4 proof can be converted to an LP proof. Some kind of non-circularity among modals is essential to have realizable proofs. In the paper the definiton of non-circular proofs will be given based on examining interrelations between formula occurrences in proofs. One of our goal is to provide an algorithm to realize these proofs.

Once the realizability of non-circular S4 proofs is established, here the burden of realizing an S4 theorem can be shifted to find a non-circular proof of the theorem. The natural next move would be to find an algorithm to directly turn a circular proof into a non-circular one. But unfortunately we couldn't provide such an algorithm, and the reason is familiar: there's no such tool in Hilbert style proof systems as cut-elimination in Genzten systems or normalization in Natural Deduction. So instead, we consider converting cut-free Gentzen style proofs to S4 proofs, and prove the latter's non-circularity.

To accomplish the above goals, we find a logical system, $\mathtt{S4}^{\Delta}$. In the system, every formula prefixed by a box is accompanied with a number label, and non-propositional axiom schemes are those from S4 joined with conditions set on the numbers involved in the schemes. The non-circularity of S4 proofs implies a linear order on modals, and this leads to the introduction of $\mathtt{S4}^{\Delta}$. We will show that non-circular S4 proofs are equal to $\mathtt{S4}^{\Delta}$ proofs regardless of number labels, and then realize $\mathtt{S4}^{\Delta}$ proofs as LP-style proofs.

We also find a Δ-style cut-free Gentzen system which is just the cut-free Gentzen system for S4 joined with numerical conditions set for modal rules such that these Δ-modal rules are sound with respect to $\mathtt{S4}^{\Delta}$. It is shown that every proof in the Gentzen system is a proof in its Δ-style counterpart regardless of number labels. This result plus the soundness of the Δ-style Gentzen system implies that every $\mathtt{S4}$ theorem can be realized to an $\mathtt{S4}^{\Delta}$ theorem and hence has a non-circular proof. Then, we also provide algorithms to convert proofs in $\mathtt{S4}^{\Delta}$ to proofs in its variants, to find the right proofs whose realizations are exactly $\mathtt{LP}$ proofs.

Our concepts of non-circular proofs and proof realization can be adapted to other normal modal logics with their $\mathtt{LP}$-style couterparts, and the realization procedure provided here can be extended to these logics with their cut-free Gentzen system. All we need is to provide the right numerical conditions set for modal rules. In the end of the paper, as examples, we will particularly discuss the normal modal logics $\mathtt{GL}$, and $\mathtt{S5}$, which has a peculiar cut-free Gentzen system introduced by Fitting [10, 9].

The plan of this paper is as follows. Systems including $\mathtt{S4}$, $\mathtt{LP}$ and their variants are presented later in this section, and the concept of non-circular proofs in $\mathtt{S4}$ and its variants is defined in the next section. In Section 3, the logical system $\mathtt{S4}^{\Delta}$ and its variants, $\mathtt{S4}'^{\Delta}$ and $\mathtt{S4}''^{\Delta}$, are introduced. We prove that non-circular proofs are proofs in these systems regardless of number labels, and provide realizations of proofs in these systems. In Section 4, a complete (theorem) realization procedure is given. There are three subsetions. The first is an algorithm to convert a cut-free $\mathtt{S4}$ proof to an $\mathtt{S4}^{\Delta}$ proof. The second offers an algorithm to convert an $\mathtt{S4}^{\Delta}$ proof to an $\mathtt{S4}'^{\Delta}$ proof. Here the relationship between the inference rules *necessitaion*, and *axiom necessitation* is the issue. In the third subsection, we provide an algorithm to produce $\mathtt{S4}''^{\Delta}$ proofs whose proof realizations are exacly $\mathtt{LP}$ proofs, where the function of "+" operator will play a role. In Section 5, the realization procedure for other loigcs will be discussed.

Preliminaries

The languages present in this paper will all be extensions of the propositional language. The propositional language used here is built from a set of propositional variables $\mathcal{P}$ and the full set of boolean connectives: $\{\neg, \vee, \wedge, \rightarrow\}$. The language $L_{\Box}$ for $\mathtt{S4}$ and its variants has the non-propositional formula formation rule: if $F \in L_{\Box}$, $(\Box F) \in L_{\Box}$. Parentheses will be omitted in the conventional way.

Definition 1.1 ($\mathtt{S4}$).

Axiom Schemes:

A0 *axiom schemes of classical propositional logic*

A1 $\Box(F \rightarrow G) \rightarrow \Box F \rightarrow \Box G$

A2 $\Box F \to \Box\Box F$
A3 $\Box F \to F$
Inference rules
R1 $F, F \to G \vdash G$ *"modus ponens"*
R2 $\vdash \Box F$, *if* $\vdash F$ *"necessitation"*

The axiom scheme A0 is actually a set of schemes. Any complete classical propositional axiom schemes can be A0. We are going to see several Hilbert style systems in this paper. All their A0 axiom scheme (or schemes) are presupposed to be the same. Any one axiom scheme other than A0 will be called a modal axiom scheme. When we need to specify in which system the axiom or the inference rule is, such as A0 in `S4`, we write `S4`A0 instead.

The set of proof terms Tm contains a set $\mathcal{C}$ of proof constants and a set $\mathcal{X}$ of proof variables. For any s, t in Tm, $(s \cdot t)$, $(s + t)$, $(!t)$ are also in Tm, where $\cdot$, $+$, and $!$ are functional symbols for combining terms. The non-propositional formula formation rule for the language $L_:$ of `LP` and its variants is: if $F \in L_:$ then $t{:}F \in L_:$ for any $t \in Tm$.

Definition 1.2 (Logic of Proofs, `LP`)**.**
Axiom Schemes:
A0 *axiom schemes of classical propositional logic*
A1 $s{:}(F \to G) \to t{:}F \to (s \cdot t){:}G$
A2 $s{:}F \to !s{:}s{:}F$
A3 $s{:}F \to F$
A4 $s{:}F \to (s + t){:}F,\ s{:}F \to (t + s){:}F$
Inference rules:
R1 $F, F \to G \vdash G$ *"modus ponens"*
R2 $\vdash c{:}F$ *for* $c \in \mathcal{C}$, *if* $\vdash F$ *and* F *is an axiom*
"axiom necessitation"

This system is what was originally introduced in [2], but for the elegance of the correspondence between proofs, our discussion won't be directly about this system until dealing with the *realization theorem*. Instead, we adopt the following extended version of `LP`. (Below $o(s)$ and $\dot{o}(s)$ both denote proof terms with s as their summand, where $o(s)$ can be equal to s while $\dot{o}(s)$ can't.)

Definition 1.3 (`ELP`)**.**
Axiom Schemes:
A0 *axiom schemes of classical propositional logic*
A1 $s{:}(F \to G) \to t{:}F \to o(s \cdot t){:}G$

A2 $s:F \to o(!s):s:F$
A3 $s:F \to F$
A4 $s:F \to \dot{o}(s):F$
Inference rules:
R1 $F, F \to G \vdash G$ *"modus ponens"*
R2 $\vdash o(c):F$ *for* $c \in \mathcal{C}$, *if* $\vdash F$ *and* F *is an axiom*
"axiom necessitation"

Two more variants of `LP` are $\mathtt{ELP}^-$, which is `ELP` with the axiom `ELP`A4 being removed, and $\mathtt{GELP}^-$, which is $\mathtt{ELP}^-$ with the *axiom necessitation* replaced by the *necessitation* "$\vdash o(c):F$ for $c \in \mathcal{C}$, if $\vdash F$" as its R2 rule. Note that these logics are not equivalent. That the permitted set of formulas applied by the (*axiom*) *necessitation* rule are different makes the difference. However every `S4` theorem has a realization counterpart in each of these variants.

On the other side we have equivalent `S4` systems, `S4`, $\mathtt{S4}'$, and $\mathtt{S4}''$. $\mathtt{S4}'$ is `S4` with the the *necessitation* replaced by *axiom necessitation*, "$\vdash \Box F$, if $\vdash F$, and F is an axiom," as its R2 rule . $\mathtt{S4}''$ is $\mathtt{S4}'$ with the axiom $\mathtt{S4}''$A4, $\Box F \to \Box F$, being added. Algorithms to convert `S4` proofs to $\mathtt{S4}'$ proofs are implicit in the proof of Proposition 4.10. The axiom $\mathtt{S4}''$A4 is an $\mathtt{S4}'$ theorem, and this makes $\mathtt{S4}'$ and $\mathtt{S4}''$ equivalent.

Comparisons will be made only between proofs in systems whose axioms and inference rules correspond to each other. That is, we will consider proof realization between `S4` and $\mathtt{GELP}^-$, between $\mathtt{S4}'$ and $\mathtt{ELP}^-$, and between $\mathtt{S4}''$ and `ELP`.

In this paper we need to deal with formula occurrences. They are formulas with their positions in another formula, or a sequence of formulas. In the following definition, we will take a path x of the parse tree of a formula F to denote the position, *occurrence*, of a subformula occurrence in F, and $F(x)$ to be the subformula at the occurrence. $\circ$ denotes a connective.

Definition 1.4 (occurrence)**.**
Let F *be a formula in* $L_\Box$. *We define the set* $\mathcal{O}(F)$ *of the occurrences and the function, also denoted as* F, *which maps an occurrence to the subformula of* F *at the occurrence simultaneously. Let* ϵ *be the empty sequence.*

1. $\epsilon \in \mathcal{O}(F)$ *and* $F(\epsilon) = F$,
2. *If* $x \in \mathcal{O}(F)$ *and* $F(x) = (G \circ H)$, *then* $x.a, x.b \in \mathcal{O}(F)$ *and* $F(x.a) = G$, *and* $F(x.b) = H$,
3. *if* $x \in \mathcal{O}(F)$ *and* $F(x) = (\circ G)$, *then* $x.\star \in \mathcal{O}(F)$ *and* $F(x.\star) = G$,

4. *Furthermore, we extend the defintion on formulas to sequences of formulas in* $L_\Box$*, such as proofs. Let* F *be the* n*-th element of a sequence* $\mathcal{D}$*, then* $n \in \mathcal{O}(\mathcal{D})$ *and* $\mathcal{D}(n) = F$*.*

In occurreces a, b denotes the left and right operand of binary operators and $\star$ the operand of unary operators. Here's some facts about the notation of occurrences.

1. $\epsilon.x \equiv x \equiv x.\epsilon$,
2. if $x \in \mathcal{O}(\mathcal{D})$ and $y \in \mathcal{O}(\mathcal{D}(x))$, then $x.y \in \mathcal{O}(\mathcal{D})$, and $\mathcal{D}(x.y) = \mathcal{D}(x)(y)$,
3. if $\mathcal{E}$ is a substitutional instance of $\mathcal{D}$ then $\mathcal{O}(\mathcal{D}) \subseteq \mathcal{O}(\mathcal{E})$
4. $\{\, \mathcal{D}(x) \mid x \in \mathcal{O}(\mathcal{D}) \,\}$ is the set of subformulas of $\mathcal{D}$,

We use *m-formula* to name all the formulas built from the non-propositional rules, i.e. $\Box F$ and $t\!:\!F$ are m-formulas. $m(\mathcal{D})$ is the set of occurrences of m-formulas in $\mathcal{D}$.

2 Non-circular Proofs

Consider the following example. Let

$$\phi_1 \equiv \Box(P \to Q) \to \Box P \to \Box Q$$
$$\phi_2 \equiv \Box(Q \to P) \to \Box Q \to \Box P$$
$$\phi_3 \equiv \Box(P \to Q) \to \Box(Q \to P) \to ((\Box P \to \Box P)\wedge (\Box Q \to \Box Q))$$

Then the sequence ϕ_1, ϕ_2, $\phi_1 \to \phi_2 \to \phi_3$, $\phi_2 \to \phi_3$, ϕ_3 is a proof, where $\phi_1 \to \phi_2 \to \phi_3$ is a classical tautology. Given that ϕ_1 and ϕ_2 are axioms, they should be realized to

$$\phi_1^r \equiv s\!:\!(P \to Q) \to t\!:\!P \to (s \cdot t)\!:\!Q$$
$$\phi_2^r \equiv u\!:\!(Q \to P) \to v\!:\!Q \to (u \cdot v)\!:\!P$$

for some proof terms s, t, u, v. But in order to realize $\phi_1 \to \phi_2 \to \phi_3$ as a classical tautology, we need $v = s \cdot t$ and $t = u \cdot v$. Since there is no solution to the equations, there's no way to realize the proof. The problem in this example comes from some kind of circularity among m-formula occurrences, especially among m-formula occurrences in modal axioms. Our goal is to show that all `S4` proofs without circularity of this kind are realizable.

Here we need to find a way to partition formula occurrenes in a proof such that the movements of fomulas in the proof can be reflected. We use labels to induce partitions.

Definition 2.1. *(label function)*

Given $\mathcal{D}$ a formula or a sequence of formulas in $L_\Box$, and $\mathbf{I}$ a label set, we call $l\colon m(\mathcal{D}) \to \mathbf{I}$ a label funciton on $\mathcal{D}$. Any set can be a label set. Also label function $l_x\colon m(\mathcal{D}(x)) \to \mathbf{I}$ is defined as for any $y \in m(\mathcal{D}(x))$, $l_x(y) = l(x.y)$.

Every label function l induces an equivalence relation $\overset{l}{\sim}$ on $\mathcal{O}(\mathcal{D})$ such that for any x, $y \in \mathcal{O}(\mathcal{D})$ $x \overset{l}{\sim} y$ iff $\mathcal{D}(x) = \mathcal{D}(y)$ and for any $x.z$, $y.z \in m(\mathcal{D})$ $l(x.z) = l(y.z)$.

Contrary to Gentzen systems, where inference rules share some structural features, it is not obvious how to trace a formula moving in a proof in Hilbert style, where axioms are the main body of proof systems. Here's the idea. The different occurrences of a propositional letter in an axiom scheme mark the stops a formula should stay in an axiom when the proof grows[1]. That is, we demand that substitutional instances of a propositional letter's different occurrences in an axiom scheme be equivalent. Other than that, modal axiom schemes also may set conditions for the movements of m-formulas. In our case, the two $\Box F$ occurrences in the scheme $\Box F \to \Box\Box F$ should be equivalent. Here's the definition.

Definition 2.2 (proof label function)**.**

A label function l on a proof $\mathcal{D}$ in S4*,* S4′ *or* S4″ *is a proof label function provided:*

1. *if $\mathcal{D}(n) = A^\rho$ and $A(x) = A(y) \in \mathcal{P}$ with A an axiom shceme and ρ a propositional letter substitution, then $n.x \overset{l}{\sim} n.y$,*
2. *if $\mathcal{D}(n)$ is $\Box F \to \Box\Box F$, then $l(n.a) = l(n.b.\star)$, i.e. (combining the above) $n.a \overset{l}{\sim} n.b.\star$,*
3. *if $\mathcal{D}(n) = G$ is derived from $\mathcal{D}(m) = F$ and $\mathcal{D}(k) = F \to G$ by modus ponens, then $n \overset{l}{\sim} k.b$ and $m \overset{l}{\sim} k.a$,*
4. *if $\mathcal{D}(n) = \Box F$ is derived from $\mathcal{D}(m) = F$ by necessitation (for $\mathcal{D}$ in* S4*) or axiom necessitation (for $\mathcal{D}$ in* S4′ *or* S4″*), then $n.\star \overset{l}{\sim} m$.*

An example will help here. Given an axiom instance $(\Box Q \to \Box P) \to (\Box Q \to \Box P) \to (\Box Q \to \Box P)$ of the axiom scheme $P \to Q \to P$, there are three formula occurrences of $\Box P$. Among these formula occurrenes, the first and the third have to be given the same label, while there is no restriction on the label given to the second. Actually, all the subformulas

[1] We don't distinguish axiom schemes from their simpliest propositional letter substitutional instances.

within the first pair of parentheses should be considered as moving into the third pair of parentheses since subformulas in these pairs are subformulas of substitutional instances of the same propositional letter P of the axiom scheme. One of the labeling of the given axiom can be explicitly expressed as $(\Box Q^v \to \Box P^w) \to (\Box Q^u \to \Box P^x) \to (\Box P^v \to \Box Q^w)$.

Definition 2.3. *For any two label functions l, l' on the same domain, we say l' covers l if $x \overset{l'}{\sim} y$, whenever $x \overset{l}{\sim} y$ for any x, y in the domain.*

Lemma 2.4. *If l is a proof label function on a proof $\mathcal{D}$, and l' is a label function on $\mathcal{D}$ such that l' covers l, then l' is also a proof label function on $\mathcal{D}$.*

Our definition of proof label function is liberal. There can be more than one proof label function on a proof. But only the samllest one with respect the covering relation completely reflects the structure of the proof. We can constructively find a such one by following the conditions listed in the defintion. Later we need this lemma.

Lemma 2.5. *Given a proof $\mathcal{D}$, and a label function l on $\mathcal{D}$, if for any $x, y \in m(\mathcal{D})$ with $x \overset{l}{\sim} y$, $l'(x) = l'(y)$, then l' covers l.*

As our earlier observation shows, what matter here are the relations (called a *stamp*) among m-formula occurrences in modal axioms. The relations defined below are suggested by `LP`, though all the results concerning circularity here can be applied to those determined by any stamps of any proof systems of any modal logics.

Definition 2.6 (the standard stamp of `S4`)**.**

A stamp $\mathcal{A}$ of a proof system is a collection of binary relations $\xrightarrow{A}$ on $m(A)$ with A a modal axiom scheme.

The standard stamp of `S4` *and* `S4`$'$ *include (the scheme names stand for the schemes)*

$\xrightarrow{A_1} = \{ \langle a, b.b \rangle, \langle b.a, b.b \rangle \}$,

$\xrightarrow{A_2} = \{ \langle a, b \rangle \}$,

and, one more for `S4`$''$,

$\xrightarrow{A_4} = \{ \langle a, b \rangle \}$.

That is, we concern directed edges from $\Box(F \to G)$ to $\Box G$ and from $\Box F$ to $\Box G$ in the scheme $\Box(F \to G) \to \Box F \to \Box G$, from $\Box F$ to $\Box\Box F$ in the scheme $\Box F \to \Box\Box F$, and from the first $\Box F$ to the second $\Box F$ in the scheme $\Box F \to \Box F$.

Below $[x]^l$ denotes the equivalence class containing the occurrence x induced by the label function l.

Definition 2.7. *Given a proof label function l on $\mathcal{D}$ in a system with stamp $\mathcal{A}$, if $\mathcal{D}(n)$ is an axiom instance of an axiom scheme A, we will write $[n.x]^l \xrightarrow{\mathcal{A}} [n.y]^l$ for $x \xrightarrow{A} y$.*

We say a sequence of equivalence classes E_1, E_2, ... is an $\mathcal{A}$-stamping chain, or just a stamping chain of the proof label function l if for any i, $E_i \xrightarrow{\mathcal{A}} E_{i+1}$.

A stamping chain is circular if there are $i \neq j$, $E_i = E_j$.

Definition 2.8 (non-circular proof)**.**

A proof label function is said to be circular if one of its stamping chain is circular; otherwise non-circular.

A proof $\mathcal{D}$ is non-circular if there exists a non-circular proof label function defined on $\mathcal{D}$.

Before ending this section, let's see some examples.

$\Box(P \to Q)^x \to \Box P^u \to \Box Q^v$

$\Box(Q \to P)^y \to \Box Q^v \to \Box P^w$

$\Box(P \to Q)^x \to \Box(Q \to P)^y \to \Box P^u \to \Box P^w$

This is a proof in S4, and also in S4$'$ and S4$''$, with some non-crucial steps skipped, and one of the labeling of the proof defined by some proof lable function is expressed. $\Box(P \to Q)^x$, $\Box Q^v$, $\Box P^w$, and $\Box P^u$, $\Box Q^v$, $\Box P^w$ are instances of non-circular stamping chains with the labels kept to express the equivalence classes. It's not difficult to see that no non-circular chain can be made in this case. If we replace the label w by the label u in our example, the result is still a labeling defined by a proof label function, but $\Box P^u$, $\Box Q^v$, $\Box P^u$ will be a circular stamping chain. Here's another example.

$\Box(P \to Q)^x \to \Box P^u \to \Box Q^v$

$\Box(Q \to P)^w \to \Box Q^v \to \Box P^u$

$\Box(P \to Q)^x \to \Box(Q \to P)^x \to ((\Box P^u \to \Box P^u) \wedge (\Box Q^v \to \Box Q^v))$

A stamping chain of this labeling is $\Box(Q \to P)^x$, $\Box P^u$, $\Box Q^v$, $\Box P^u$, $\Box Q^v$, which is circular. And it can be checked that every proof label function defined on this proof has a circular stamping chain.

3 $\mathtt{S4}^\Delta$ and Non-circular Proof Realization

3.1 $\mathtt{S4}^\Delta$

Two things lead us to find $\mathtt{S4}^\Delta$. One is that the non-circularity can be detected by number labels. The other is that instead of directly dealing with m-formula occurrences, it will be easier to work on formulas but with their labels built in. We'll begin with the preliminary work.

Definition 3.1 (increasing proof label function)**.**
A proof label function $\mathit{\Delta}\colon m(\mathcal{D}) \to \mathbb{N}$ on a proof $\mathcal{D}$ in $\mathtt{S4}$, $\mathtt{S4}'$, or $\mathtt{S4}''$ is increasing if $\mathit{\Delta}(n.x) < \mathit{\Delta}(n.y)$, for any substitutional instance $\mathcal{D}(n)$ of an axiom scheme A, and any occurrences $x \xrightarrow{A} y$.

Lemma 3.2. *$\mathit{\Delta}$ is an increasing proof label function on a proof $\mathcal{D}$, if and only if for any $x, y \in \mathcal{O}(\mathcal{D})$, if $[x]^{\mathit{\Delta}} \xrightarrow{\mathcal{A}} [y]^{\mathit{\Delta}}$, then $\mathit{\Delta}(x) < \mathit{\Delta}(y)$.*

Proof. By the definitions of increasing proof label function and the fact that if $w \overset{\mathit{\Delta}}{\sim} z$, then $\mathit{\Delta}(w) = \mathit{\Delta}(z)$. $\dashv$

Proposition 3.3. *A proof $\mathcal{D}$ is non-circular if and only if there exists an increasing label function $\mathit{\Delta}$ on $\mathcal{D}$.*

Proof. When $\mathit{\Delta}$ is increasing, by the lemma, the stamping chains of $\mathit{\Delta}$ can't be circular. Hence every increasing proof label function is non-circular. For the other direction, when $\mathcal{D}$ is non-circular, there exists a proof label function l on $\mathcal{D}$ such that stamping chains of l is non-circular. Based on l, we can define a function $\mathit{\Delta}_0\colon m(\mathcal{D}) \to \mathbb{N}$ such that $\mathit{\Delta}_0(x) = \max\{k \mid [x]^l \text{ is the k-th element of a stamping chain of } l\}$. Since for any $x \overset{\mathit{\Delta}}{\sim} y$ in $m(\mathcal{D})$, $\mathit{\Delta}_0(x) = \mathit{\Delta}_0(y)$, $\mathit{\Delta}_0$ covers l; $\mathit{\Delta}_0$ is a proof label function. Also since for $[x]^l \xrightarrow{\mathcal{A}} [y]^l$, $\mathit{\Delta}_0(x) < \mathit{\Delta}_0(y)$, $\mathit{\Delta}_0$ is increasing. This completes the proof. $\dashv$

Based on $\mathit{\Delta}_0$, other increasing proof label function $\mathit{\Delta}$ covering l can be built.

Definition 3.4. *An equivalence class $[x]^l$ in the proof is said to be initial if there's no $[y]^l$ such that $[y]^l \xrightarrow{\mathcal{A}} [x]^l$.*

Corollary 3.5. *Given a proof $\mathcal{D}$ and its proof label function l, let S be the set of initial equivalence classes and $f\colon S \to \mathbb{N}$. There exists an increasing proof label function $\mathit{\Delta}$ covering l such that for any $[x]^l \in S$, $\mathit{\Delta}(x) = f([x]^l)$.*

Proof. Let $m = \max\{f([x]^l) \mid [x]^l \in S\}$, and Δ_0 be the function built by the construction in the above proposition. Then the numerical function Δ such that for any $x \in m(\mathcal{D})$, $\Delta(x) = f([x]^l)$ if $[x]^l$ is initial, otherwise $\Delta(x) = \Delta_0(x) + m$ will do the job. $\dashv$

Let $\mathbf{I}$ be a label set. The language $L_{\mathbf{I}}$ is an extended propositional language with the non-propositional formula formation rule: if $F \in L_{\mathbf{I}}$ and $u \in \mathbf{I}$, $(\Box F^u) \in L_{\mathbf{I}}$. We will call the label u in $\Box F^u$ the principal label of the formula, denoted as $\nu(\Box F^u)$. $\Box F^u$ is an m-formula.

Our Definition 1.4 can be well-adapted to define formula ocurrences of formulas or sequences of formulas in $L_{\mathbf{I}}$ for any label set $\mathbf{I}$ with the following clause about m-formulas: if $x \in \mathcal{O}(F)$ and $F(x) = (\Box G^u)$, then $x.\star \in \mathcal{O}(F)$ and $F(x.\star) = G$.

Several translations defined on formula occurrences will be given in the rest of the paper. They will all fix the propositional letter occurrences and commute with boolean connectives. Let $\mathcal{D}$ be a sequence of formulas in $L_\Box$, $\mathcal{F}$ a sequence of formulas in $L_{\mathbf{I}}$.

Definition 3.6.

For every label function $l \colon m(\mathcal{D}) \to \mathbf{I}$, there is an induced translation, also denoted by l, such that for any $x \in \mathcal{O}(\mathcal{D})$, $\mathcal{D}^l(x) = \Box\mathcal{D}^{l_{x.\star}}(x.\star)^u$ where $u = l(x)$.

A $\Box$-translation on $\mathcal{F}$ is a translation such that for every $x \in m(\mathcal{F})$, $\mathcal{F}^\Box(x) = \Box\mathcal{F}^\Box(x.\star)$,

$l_\mathcal{F}$ is a label function on $\mathcal{F}^\Box$ induced by $\mathcal{F}$ such that for every $x \in m(\mathcal{F}^\Box)$, $l_\mathcal{F}(x) = \nu(\mathcal{F}(x))$.

The $l_\mathcal{F}$ is well-defined since $x \in m(\mathcal{F}^\Box)$ if and only if $x \in m(\mathcal{F})$.

Lemma 3.7. *For x, $y \in \mathcal{O}(\mathcal{D})$, $x \overset{l}{\sim} y$ iff $\mathcal{D}^l(x) = \mathcal{D}^l(y)$.*

Proposition 3.8. *$\mathcal{F} = \mathcal{D}^l$ iff $\mathcal{F}^\Box = \mathcal{D}$ and $l_\mathcal{F} = l$.*

The language of $\texttt{S4}^\Delta$ and its variants are L_Δ, which is an $L_{\mathbf{I}}$ with natural numbers as labels.

Definition 3.9 ($\texttt{S4}^\Delta$)**.**

Axiom Schemes:

A0 *axiom schemes of classical propositional logic*

A1 $\Box(F \to G)^i \to \Box F^j \to \Box G^k$, i, $j < k$

A2 $\Box F^i \to \Box(\Box F^i)^j$, $i < j$

A3 $\Box F^i \to F$

Inference rules

R1 $F, F \to G \vdash G$ *"modus ponens"*

R2 $\vdash \Box F^i$ *for any* i, *if* $\vdash F$ *"necessitation"*

$\mathtt{S4}'^{\Delta}$ is $\mathtt{S4}^{\Delta}$ with the *necessitation* replaced by the *axiom necessitation*, "$\vdash \Box F^i$ for any i, if $\vdash F$ and F is an axiom,", and $\mathtt{S4}''^{\Delta}$ is $\mathtt{S4}^{\Delta}$ with axiom $\mathtt{S4}''^{\Delta}$A4, $\Box F^i \to \Box F^j, i < j$, being added

Next is the main theorem of this subsection.

Theorem 3.10. *A proof $\mathcal{D}$ in $\mathtt{S4}$, $\mathtt{S4}'$, or $\mathtt{S4}''$ is non-circular if and only if there is a proof label function $\Delta\colon m(\mathcal{D}) \to \mathbb{N}$ such that $\mathcal{D}^{\Delta}$ is a proof in $\mathtt{S4}^{\Delta}$, $\mathtt{S4}'^{\Delta}$, or $\mathtt{S4}''^{\Delta}$, respectively.*

Proof. When $\mathcal{D}^{\Delta} = \mathcal{F}$ is a proof in $\mathtt{S4}^{\Delta}$ [$\mathtt{S4}'^{\Delta}$, $\mathtt{S4}''^{\Delta}$], it is not difficult to check that $\mathcal{D}$ $(= \mathcal{F}^{\Box})$ is a proof in $\mathtt{S4}$ [$\mathtt{S4}'$, $\mathtt{S4}''$], and Δ $(= l_{\mathcal{F}})$ is a proof label function on $\mathcal{D}$. As to Δ's being increasing it is exactly because of our conditions set on the modal axiom schemes of the system. So $\mathcal{D}$ is non-circular. For the other direction when $\mathcal{D}$ is a non-circular proof, there is, by Proposition 3.3, an increasing proof label function, say Δ, on $\mathcal{D}$. Then we only need to show $\mathcal{D}^{\Delta}$ is a proof in $\mathtt{S4}^{\Delta}$ [$\mathtt{S4}'^{\Delta}$, $\mathtt{S4}''^{\Delta}$]. Since Δ is a proof label function, when A is an axiom, by Lemma 3.7, A^{Δ} will still be an axiom, except that we have to check that those conditions we set on modal axiom schemes are fulfilled. And this is the case because Δ is increasing. Furthermore, when ϕ is derived from previous lines of the proof, it is routine to check that ϕ^{Δ} is still a derived line in $\mathcal{D}^{\Delta}$ by the same inference rule. $\dashv$

3.2 Non-circular Proof Realization

Definition 3.11 (proof assignment)**.**

Given a sequence $\mathcal{F}$ of formulas in L_{Δ}, a proof assignment p on $\mathcal{F}$ assigns each pair (F, i) to a subformula $\Box F^i$ in $\mathcal{F}$ a proof term.

Each proof assignment p induces a translation on $\mathcal{F}$ to a sequence of $L_{:}$ formulas such that $(\Box F^i)^p = p(F,i) : (F^p)$

Here's a characterization of m-formulas in a proof.

Definition 3.12. *Given a proof in an $\mathtt{S4}^{\Delta}$ system,*

1. *if axiom $\Box(F \to G)^i \to \Box F^j \to \Box G^k$ is in the proof, we say $\Box G^k$ is an A1-formula, and $< \Box(F \to G)^i, \Box F^j >$ is a predecessor pair of $\Box G^k$ with $\Box(F \to G)^i$ the α-predecessor and $\Box F^j$ the β-predecessor of $\Box G^k$.*

2. *if an axiom $\Box F^i \to \Box(\Box F^i)^j$ is in the proof, we say $\Box(\Box F^i)^j$ is an A2-formula, and $\Box F^j$ is a γ-predecessor of $\Box(\Box F^i)^j$;*
3. *if an axiom $\Box F^i \to \Box F^j$ is in the proof, we say $\Box F^j$ is an A4-formula and $\Box F^i$ is a δ-predecessor of $\Box F^j$;*
4. *if $\Box F^i$ is derived from* necessitation *(in an $\mathtt{S4}^\Delta$ proof), or from* axiom necessitation *(in an $\mathtt{S4}'^\Delta$ proof or an $\mathtt{S4}''^\Delta$ proof), we say $\Box F^i$ is an R2-formula .*

An m-formula can fall into more than one of those categories. If a formula is at most in one of the above categories we say the formula is stable. Especially when the formula is, say, only an A1-formula or in none of the above categories, we will say the formula is A1-stable. We will need this definition in the Subsection 4.3.

Definition 3.13 (characteristic proof assignment)**.**

Each proof $\mathcal{F}$ in $\mathtt{S4}^\Delta$, $\mathtt{S4}'^\Delta$, or $\mathtt{S4}''^\Delta$ will be associated with a system of equations $\mathbf{E}_\mathcal{F}$ for an unknow proof assignment p. The system consists of:

1. *$p(F,i) = o(p(G,j)\cdot p(H,k))$ when $< \Box G^j, \Box H^k >$ is a predecessor pair of $\Box F^i$,*
2. *$p(F,i) = o(!p(G,j))$ when $\Box G^j$ is a γ-predecessor of $\Box F^i$,*
3. *$p(F,i) = \dot{o}(p(G,j))$ when $\Box G^j$ is a δ-predecessor of $\Box F^i$,*
4. *$p(F,i) = o(c)$, for some $c \in \mathcal{C}$, when $\Box F^i$ is an R2-formula. In particular, we request different constants for different equations.*

A characteristic proof assignment of a proof $\mathcal{F}$ in $\mathtt{S4}^\Delta$, $\mathtt{S4}'^\Delta$, or $\mathtt{S4}''^\Delta$ is a proof assignment which satisfies all the equations in $\mathbf{E}_\mathcal{F}$.

Lemma 3.14. *Each proof $\mathcal{F}$ in $\mathtt{S4}^\Delta$, $\mathtt{S4}'^\Delta$, or $\mathtt{S4}''^\Delta$ has a characteristic proof assignment.*

Proof. We prove this by induction on the principal labels of m-formulas in $\mathcal{F}$. In the base case, for m-formulas $\Box F^i$ with i the smallest principal label of m-formulas in $\mathcal{F}$, if they are derived from (*axiom) necessitation*, we assign pairs (F,i) the proof constants c they need to have; otherwise they are assigned arbitrary terms. Especially, we assign different variables for different pairs.

At the induction step, suppose we want to determine the proof assignment value of $\Box F^i$, namely $p(F,i)$. By induction hypothesis, the proof assignment values of the predecessors of $\Box F^i$ have been constructed, since their principal labels are smaller than i. When $\Box F^i$ has no predecessor, assign a new proof variable to $p(F,i)$. If $\Box F^i$ has only one predecessor $\Box G^j$ which is a δ-predecessor with $p(G,j) = s$, let $p(F,i) = s + t$ for a term t. In other cases, let S be the set of proof terms built up from the proof assignment value of the predecessors of $\Box F^i$. That is, S contains $s \cdot t$ if $< \Box G^j, \Box H^k >$ is a predecessor pair of $\Box F^i$ with $p(G,j) = s$ and $p(H,k) = t$, $!s$ if $\Box G^j$ is a γ-predecessor with $p(G,j) = s$, s if $\Box G^j$ is an δ-predecessor with $p(G,j) = s$, and constant c if $p(F,i) = o(c)$ is in $\mathbf{E}_{\mathcal{F}}$. Let $p(F,i) = \sum_{s \in S} s$. Then p is a characteristic proof assignment. $\dashv$

Theorem 3.15. *$\mathcal{H}$ is a proof in* $\mathtt{GELP}^-$ [$\mathtt{ELP}^-$, $\mathtt{ELP}$] *if and only if there is a proof $\mathcal{F}$ in* $\mathtt{S4}^\Delta$ [$\mathtt{S4}'^\Delta$, $\mathtt{S4}''^\Delta$] *and a characteristic proof assignment p on $\mathcal{F}$ such that $\mathcal{H} = \mathcal{F}^p$.*

Proof. Given a proof $\mathcal{F}$ in $\mathtt{S4}^\Delta$ [$\mathtt{S4}'^\Delta$, $\mathtt{S4}''^\Delta$] and a characteristic proof assignment p on $\mathcal{F}$, it's not hard to check that $\mathcal{H} = \mathcal{F}^p$ is a proof in $\mathtt{GELP}^-$ [$\mathtt{ELP}^-$, $\mathtt{ELP}$]. For the other direction, let $Tm(\mathcal{H})$ be the set of proof terms in $\mathcal{H}$, and $\eta\colon Tm(\mathcal{H}) \to \mathbb{N}$ be an injective function linearizing the subterm relation on $Tm(\mathcal{H})$. Then there is a translation on $\mathcal{H}$ induced by η such that $(t\!:\!F)^\eta = \Box(F^\eta)^{\eta(t)}$. Then $\mathcal{F} = \mathcal{H}^\eta$ is a proof in $\mathtt{S4}^\Delta$ [$\mathtt{S4}'^\Delta$, $\mathtt{S4}''^\Delta$]. Now take the proof assignment p such that for any $\Box F^i$ in $\mathcal{F}$, $p(F,i) = \eta^{-1}(i)$. p will satisfy all the equations in $\mathbf{E}_{\mathcal{F}}$, and $\mathcal{F}^p$ will be $\mathcal{H}$. $\dashv$

Theorem 3.16. *A proof $\mathcal{D}$ in* $\mathtt{S4}$ [$\mathtt{S4}'$, $\mathtt{S4}''$] *is non-circular if and only if there exists a realization r such that $\mathcal{D}^r$ is a proof in* $\mathtt{GELP}^-$ [$\mathtt{ELP}^-$, $\mathtt{ELP}$].

Proof. To realize a non-circular proof $\mathcal{D}$ in $\mathtt{S4}$ [$\mathtt{S4}'$, $\mathtt{S4}''$], by Theorem 3.10, there is a Δ such that $\mathcal{D}^\Delta$ is a proof in $\mathtt{S4}^\Delta$ [$\mathtt{S4}'^\Delta$, $\mathtt{S4}''^\Delta$], and, by the theorem above, there is a p such that $(\mathcal{D}^\Delta)^p$ is a proof in $\mathtt{GELP}^-$ [$\mathtt{ELP}^-$, $\mathtt{ELP}$]. Take $r = p \circ \Delta$. Then the translation induced from this r is the one we want. For the other direction, let $\mathcal{H} = \mathcal{D}^r$ be a proof in $\mathtt{GELP}^-$ [$\mathtt{ELP}^-$, $\mathtt{ELP}$]. Then $\mathcal{H} = \mathcal{F}^p$ for some proof $\mathcal{F}$ in $\mathtt{S4}^\Delta$ [$\mathtt{S4}'^\Delta$, $\mathtt{S4}''^\Delta$] and some proof assignment p. It can be checked that $\mathcal{D} = \mathcal{F}^\Box$. $\mathcal{D}$ is a non-circular proof.

In fact, for this direction, we can directly prove it from $\mathcal{H}$. If we disregard the superficial symbolic difference, language $L_:$ is one of labeled modal language $L_{\mathbf{I}}$ with proof terms as labels. Then $\mathcal{D} = \mathcal{H}^\Box$ and $l_{\mathcal{H}} = r$. However r will be a non-circular proof label function on $\mathcal{D}$ because of the conditions of proof terms set on modal axiom schemes. $\dashv$

When trying to prove the *realization theorem* by induction on a Hilbert style proof, researchers find difficulty in dealing with *modus ponens* that if theorems F and $F \to G$ are realizable, meaning there are theorems F^{r_1} and $(F \to G)^{r_2}$ in an LP-style logic, it is hard to unify the realizations r_1 and r_2 as one realization. Here we provide an explanation. Suppose for theorems F^{r_1} and $(F \to G)^{r_2}$, we have their proofs $\mathcal{D}^{r_1}$ and $\mathcal{D}'^{r_2}$ where the underlying sequences $\mathcal{D}$ and $\mathcal{D}'$ are non-circular. Now though the concatenation sequence $\mathcal{D}\mathcal{D}'G$ is a proof of G, it doesn't have to be non-circular. Hence there is no immediate r such that $(\mathcal{D}\mathcal{D}'G)^r$ is a proof. As a result, the difficulty to find an unified realization r of F and $F \to G$ is the same as the difficulty to find an algorithm to directly convert a circular proof to a non-circular one.

Our research also show that not all proofs but only non-circular proofs are coded by proof terms. This is different from the cases for λ-calculus (Natural Deduction) and combinatory logic (Hilbert style proofs), where every intuitionistic proof is represented. We can say LP (and so is $\mathtt{S4}^{\Delta}$) is a study of non-circular proofs, where substitutive proof terms code the interstructure of the proofs. While one LP proof has more information than the other, only the smallest one with respect to the covering relation has the full strutural information of its underlying non-circular proof. But if the complexity is taken into account, it is possible that for an S4 theorem ϕ, in any of its realization there is a proof term whose length is far more longer than the length of ϕ's shortest proof. Of course, this statement needs more reasearches on non-circular proofs to confirm.

The following are some further features of our proof realization algorithm.

Remark 1. Normal realization is the kind of theorem realization which demands that different negative m-formula occurrences be realized by different proof variables. In our proof realization procedure, if in a Δ-style proof every negative formula has only one occurrence in the conclusion and is intial, i.e. having no predecessors, then the conclusion can be normally realized. Let's call proofs of this kind normal. Then it is not difficult to check Δ-style proofs produced in the next section, with some number label adjustments, will be normal, and hence our theorem realization procedure can produce normal realization.

Remark 2. An alternative to the *axiom necessitation* is that a formula $c{:}A$ with a constant $c \in \mathcal{C}$ and an axioms A can be derived only if it is in a *Constant Specification* set. In this case, we just have to delay the providing of specific proof constants until the end of the proof realization algorithm.

Remark 3. For two Δ-style proofs $\mathcal{D}^{\Delta}$ and $\mathcal{D}^{\Delta'}$, though they have the same underlying sequence, their proof realizations can be different. Especially, when Δ' covers Δ, the proof realzation result of $\mathcal{D}^{\Delta'}$ can have longer proof terms. So if the complexity is the issue, the smallest Δ on $\mathcal{D}$ with respect to the covering relation should be taken.

4 A (Thereom) Realization Procedure

In the first subsection, we show that every $\mathtt{S4}$ theorem can be realized to an $\mathtt{S4}^{\Delta}$ theorem by examining the theorem's cut-free proof. In the second, we show how to produce an $\mathtt{S4}'^{\Delta}$ proof from an $\mathtt{S4}^{\Delta}$ proof. Finally, from an $\mathtt{S4}'^{\Delta}$ proof, we create an $\mathtt{S4}''^{\Delta}$ proofs of a type, called stable, whose realization will be an $\mathtt{LP}$ proof.

4.1 From $\mathtt{S4}$ to $\mathtt{S4}^{\Delta}$

A sequent $\Gamma \Rightarrow \Gamma'$ is a pair of finite multisets Γ, Γ' of formulas. It is convenient for us to view a sequenct as a formula $C_1 \rightarrow (\ldots \rightarrow (C_n \rightarrow \bigvee \Gamma')\ldots)$. Given a multiset $\Gamma = \{C_i\}$ of formulas in $L_{\Box}$, $\Box\Gamma = \{\Box C_i\}$. Given a multiset $\Gamma = \{C_i\}$ of formulas in L_{Δ}, $\Box\Gamma^{\iota} = \{\Box C_i^{j_i}\}$, for j_i a number in the multiset ι. $|\Gamma|$ is the number of formulas in Γ. Here's the Gentzen systems[2].

Definition 4.1 ($\mathtt{S4}G^{-}$).
The only axiom is that $P \Rightarrow P$, for a propositional letter P.
The rules for weakening (W) and constraction (C)

$$LW\,\frac{\Gamma \Rightarrow \Gamma'}{A, \Gamma \Rightarrow \Gamma'} \qquad RW\,\frac{\Gamma \Rightarrow \Gamma'}{\Gamma \Rightarrow \Gamma', A}$$

$$LC\,\frac{A, A, \Gamma \Rightarrow \Gamma'}{A, \Gamma \Rightarrow \Gamma'} \qquad RC\,\frac{\Gamma \Rightarrow \Gamma', A, A}{\Gamma \Rightarrow \Gamma', A}$$

The classical logical rules (i=0,1):

$$L\neg\,\frac{\Gamma \Rightarrow \Gamma', A}{\neg A, \Gamma \Rightarrow \Gamma'} \qquad R\neg\,\frac{\Gamma, A \Rightarrow \Gamma'}{\Gamma \Rightarrow \Gamma', \neg A}$$

$$L\wedge\,\frac{A_i, \Gamma \Rightarrow \Gamma'}{A_0 \wedge A_1, \Gamma \Rightarrow \Gamma'} \qquad R\wedge\,\frac{\Gamma \Rightarrow \Gamma', A \quad \Gamma \Rightarrow \Gamma', B}{\Gamma \Rightarrow \Gamma', A \wedge B}$$

$$L\vee\,\frac{A, \Gamma \Rightarrow \Gamma' \quad B, \Gamma \Rightarrow \Gamma'}{A \vee B, \Gamma \Rightarrow \Gamma'} \qquad R\vee\,\frac{\Gamma \Rightarrow \Gamma', A_i}{\Gamma \Rightarrow \Gamma', A_0 \vee A_1}$$

$$L\rightarrow\,\frac{\Gamma \Rightarrow \Gamma', A \quad B, \Gamma \Rightarrow \Gamma'}{A \rightarrow B, \Gamma \Rightarrow \Gamma'} \qquad R\rightarrow\,\frac{A, \Gamma \Rightarrow \Gamma', B}{\Gamma \Rightarrow \Gamma', A \rightarrow B}$$

[2]Our system $\mathtt{S4}G^{-}$ is similar to the cut-free propositional fragment of **G1s** in [18] but for language with only one modal operator $\Box$, and with the negation $\neg$ connective instead of the falsehood $\bot$.

The modal rules are

$$L\Box \ \frac{A, \Gamma \Rightarrow \Gamma'}{\Box A, \Gamma \Rightarrow \Gamma'} \qquad R\Box \ \frac{\Box\Gamma \Rightarrow A}{\Box\Gamma \Rightarrow \Box A}$$

Definition 4.2 ($\mathtt{S4}^{\Delta}G^{-}$)**.**

$\mathtt{S4}^{\Delta}G^{-}$ is a system on formulas in L_{Δ}. It is just the $\mathtt{S4}G^{-}$ with the following Δ-modal rules

$$L\Box \ \frac{A, \Gamma \Rightarrow \Gamma'}{\Box A^{i}, \Gamma \Rightarrow \Gamma'}\ , \quad \textit{for any } i$$

$$R\Box \ \frac{\Box\Gamma^{\iota} \Rightarrow A}{\Box\Gamma^{\iota} \Rightarrow \Box A^{i}}\ , \quad \textit{for any } i > \max(\iota) + |\Gamma| + 1\textit{, when } |\Gamma| \neq 0\textit{, and for any } i \textit{ when } |\Gamma| = 0$$

In the following, when we adjust m-formula occurrences' number labels, we adjust all the related fomulas of premises and conclusions of rules to the same number. Recall that cut-free proofs respect the polarity of formulas.

Lemma 4.3. *If in an $\mathtt{S4}^{\Delta}G^{-}$ proof we adjust the number labels such that the principal labels of negative m-formula occurrences become smaller, and those of positive m-formula occurrences become larger, the result will still be an $\mathtt{S4}^{\Delta}G^{-}$ proof.*

Proof. The only apllications of inference rule will be affected by this adjustment are the applications of the right Δ-modal rule . However, the condition set on the rule certainly is still fulfilled after the adjustment. ⊣

Proposition 4.4. *Every $\mathtt{S4}G^{-}$ proof is a proof of $\mathtt{S4}^{\Delta}G^{-}$ without number labels.*

Proof. The proof is quite staightforward. We can give suitable labels to an $\mathtt{S4}G^{-}$ proof by induction on the depth of the prooftree. There are some cases, like applications of two-premise inference rules, in which the labels need adjustments. In these cases, we can apply the previous lemma to have adequate labels. Nevertheless, the most efficient method is to let all negative formula occurrences have label 0, and all positive formula occurrences have label equal to the nubmer of m-formula occurrecs in the $\mathtt{S4}G^{-}$ proof. Then the condition for the right Δ-modal rule will be satisfied. But notice that this efficient method won't work when the Δ-modal rule have conditions such that the priniciple label of a positive m-formula relys on principal labels of other positve m-formulas. ⊣

Proposition 4.5. *Every $\mathtt{S4}^{\Delta}G^{-}$ proof of can be converted to an $\mathtt{S4}^{\Delta}$ proof with the same conclusion.*

Proof. The procedure is just to convert each application of an inference rule (including axioms) to a sequence of formulas. Here we only have to check there are such conversion for applications of Δ-modal rules, especially the right Δ-modal rule. We need the following lemma:

Lemma 4.6. *For* $|\Gamma| > 0$ *and* $i > \max(\iota, e) + |\Gamma| + 1$, $\Box(\Box\Gamma^\iota \Rightarrow A)^e \to (\Box\Gamma^\iota \Rightarrow \Box A^i)$ *is provable in* $\mathtt{S4}^\Delta$.

Proof. It's equivalent to prove that for $|\Theta| \geq 0$ and $i > \max(\iota, j, e) + |\Theta| + 2$

$(*)$ $\Box(\Box C^j \to (\Box\Theta^\iota \Rightarrow\ A))^e \to (\Box C^j \to (\Box\Theta^\iota \Rightarrow \Box A^i))$

is provable in $\mathtt{S4}^\Delta$. We will prove this by induction on $|\Theta|$. First let $e' > max(e, j+1)$ then

$\Box(\Box C^j \to (\Box\Theta^\iota \Rightarrow\ A))^e \to \Box(\Box C^j)^{j+1} \to \Box(\Box\Theta^\iota \Rightarrow A)^{e'}$

is an A1 axiom, and

$\Box C^j \to \Box(\Box C^j)^{j+1}$ is an A2 axiom, and hence

$(**)$ $\Box(\Box C^j \to (\Box\Theta^\iota \Rightarrow\ A))^e \to \Box C^j \to \Box(\Box\Theta^\iota \Rightarrow A)^{e'}$

is provable in $\mathtt{S4}^\Delta$. When Θ is empty, let $e' = i > \max(e, j) + 2 > \max(e, j+1)$, then $(**)$ holds, and hence the base case of $(*)$ is proved. At the induction step suppose $|\Theta| = n+1$. Let $e' = \max(j+1, e) + 1$ and $i > \max(\iota, j, e) + |\Theta| + 2$ and hence $i > \max(\iota, e') + |\Theta| + 1$. Then $(**)$ holds. By induction hypothesis, $\Box(\Box\Theta^\iota \Rightarrow\ A)^{e'} \to (\Box\Theta^\iota \Rightarrow \Box A^i)$, which is equivalent to the formula $\Box(\Box C'^{j'} \to (\Box\Theta'^{\iota'} \Rightarrow\ A))^{e'} \to (\Box C'^j \to (\Box\Theta'^{\iota'} \Rightarrow \Box A^i))$ with $|\Theta'| = n$, holds. Then by classical propositional logic $(*)$ is provable in $\mathtt{S4}^\Delta$. This finishes the proof for the induction step. $\dashv$

Since if $\Box\Gamma^\iota \Rightarrow\ A$ is provable in $\mathtt{S4}^\Delta$, when Γ is empty, by *necessitation*, $\Rightarrow \Box A^i$ is provable, and when Γ is not empty, $\Box(\Box\Gamma^\iota \Rightarrow\ A)^0$ is a theorem, and hence, by the lemma, $\Box\Gamma^\iota \Rightarrow \Box A^i$ is provable in $\mathtt{S4}^\Delta$, whenever $i > \max(\iota) + |\Gamma| + 1$. $\dashv$

Corollary 4.7. *Every* $\mathtt{S4}$ *theorem has a non-circular proof.*

Proof. From all above in this subsection we can conclude that every $\mathtt{S4}$ theorem ϕ can be realized to an $\mathtt{S4}^\Delta$ theorem ϕ^Δ. Let $\mathcal{F}$ be an $\mathtt{S4}^\Delta$ proof of ϕ^Δ. Then by Theorem 3.10, $\mathcal{F}^\Box$ is a non-circular proof of ϕ. $\dashv$

4.2 From $\mathtt{S4}^\Delta$ to $\mathtt{S4}'^\Delta$

In this subsection we will convert an $\mathtt{S4}^\Delta$ proof to an $\mathtt{S4}'^\Delta$ proof. We will provide two methods: one is called the inductive and the other is the structural. They have different purposes. We will discuss them later. Now we need to do some preliminary work. First, we will presuppose that in the $\mathtt{S4}^{\Delta}$ proof in discussion every R2-formula is initial, that is, it has no predecessors. This is the case when the proof is coverted from an $\mathtt{S4}^{\Delta}G^{-}$ proof. However, in general if an R2-formula $\Box F^{i}$ has predecessors, we can extend the proof by adding formulas including

$\Box F^0$, $F \to F$, $\Box(F \to F)^0$, $\Box(F \to F)^0 \to \Box F^0 \to \Box F^i$, $\Box F^0 \to \Box F^i$,

and a proof of the tautology $F \to F$ if it is not an axiom.

Second, since now in our proof every R2-formula is initial, we can adjust the labels in the proof such that the number labels of these initial formulas have the numbers we want them to have, as suggested by the Corollary 3.5. Now given an $\mathtt{S4}^{\Delta}$ proof, before we extend the proof to an $\mathtt{S4'}^{\Delta}$ proof, we will first modify the number label of an R2-formulas derive from the n-th element of the proof to be a^{n+1} for some constant a in the inductive method, and to n in the structural method. We first see the inductive method.

Lemma 4.8. *For any $\mathtt{S4'}^{\Delta}$ proof $\mathcal{F}$, there is an $\mathtt{S4'}^{\Delta}$ proof $\mathcal{F}'$ such that if ϕ is the k-th element of $\mathcal{F}$, then $\Box\phi^{ka}$ is the i-th element of $\mathcal{F}'$, where a is a constant and i at most ka.*

Proof. The proof is by induction on the length of $\mathcal{F}$. The axiom case and the modus ponens case are trivial. We consider the application of *axiom necessitation*. Suppose the k-th $\Box A^i$ is derived from axiom A, and $i < ka$, then add $\Box A^i \to \Box(\Box A^i)^{ka}$, $\Box(\Box A^i)^{ka}$ to the proof. If $i \geq ka$, then it can be checked that there is a number e independent of the choice of i such that $\Box(\Box A^0 \to \Box A^i)^e$ and $\Box(\Box A^0)^1$ is provable in $\mathtt{S4'}^{\Delta}$, then pick a large enough such that $\Box(\Box A^i)^{ka}$ can be derived by adding at most a formulas. ⊣

Proposition 4.9. *(inductive method) Every proof in $\mathtt{S4}^{\Delta}$ can be extended to a proof in $\mathtt{S4'}^{\Delta}$.*

Proof. Here we use the term *extend* in a broad sense that before amplifying the proof, adjustments on the numbers are allowed. We will show that if ϕ has $\mathtt{S4}^{\Delta}$ proof of length n then ϕ has an $\mathtt{S4'}^{\Delta}$ proof of length at most a^{n+1}. We only check the case of application of *necessitation*. If $\Box F^{a^{n+1}}$ in a proof is derive from F which is the n-th element in the proof of ϕ, then by induction hypothesis, F has a $\mathtt{S4'}^{\Delta}$ proof of length a^n, and by the above lemma, $\Box F^{a^{n+1}}$ has an $\mathtt{S4'}^{\Delta}$ proof of length at most $a^{(n+1)}$. ⊣

Proposition 4.10. *(structural method) Every proof in $\mathtt{S4}^{\Delta}$ can be extended to a proof in $\mathtt{S4'}^{\Delta}$.*

Proof. We will lengthen the proof inductively by adding formulas $\Box F^i$ after the i-th non-conclusion formula F of the proof. We also only check the necessitation case. If the k-th non-conclusion formula $\Box F^i$ is derived from the i-th formula F, we add formulas $\Box F^i \to \Box(\Box F^i)^k$ and $\Box(\Box F^i)^k$, where the former is an axiom since $k > i$. Then the resulting sequence will be a proof in $\mathtt{S4}'^{\Delta}$. ⊣

The merit of the structural method over the inductive method is the complexity (this can be seen from the number labels). However, the strucutral method is not alwarys applicable when we consider to extend the realization procedure to other nomal modal logics, especially to those without the transitivity A2 axiom. Instead, the LP-style counterparts of these logics have the following *strong axiom necessitation* rule: "R2* $\vdash c\!:\!F$ for $c \in \mathcal{C}$, if $\vdash F$ and F is an axiom or is inferable using R2*". The Δ-style counterpart of this R2* rule is not difficult to figure out. With this rule, the inductive method will still work, where only A2 axiom $\Box A^i \to \Box(\Box A^i)^j$ of axiom A is used.

4.3 From $\mathtt{S4}'^{\Delta}$ to $\mathtt{S4}''^{\Delta}$

Now from a cut-free S4 proof, we can produce an $\mathtt{S4}'^{\Delta}$ proof, which is also an $\mathtt{S4}''^{\Delta}$ proof, whose proof realization will be an ELP proof. We need some more work to produce a *stable* $\mathtt{S4}''^{\Delta}$ proofs whose realization are exactly LP proofs. We first show that the realization of a stable proof is an LP proof, and provide an algorithm to produce one from a given $\mathtt{S4}''^{\Delta}$ proof.

Recall that if we say a formula in L_Δ is, for example, A1-stable, then it cannot be an A2-, A4-, or R2- formula. To extend this use, we will say, for a C in { A1, A2, A4, R2 }, a set of m-formulas is C-stable if every element of the set is so. A set is stable if it is C-stable for some C.

Given an equivalence relation on m-formulas in a $\mathtt{S4}''^{\Delta}$ proof, we say a sequence of equivalence classes $E_1, E_2, \ldots$ is a *superchain* if for every i there are m-formulas $F \in E_i$, $G \in E_{i+1}$ such that F is a predecessor of G.

Definition 4.11. *Let S be a set of m-formulas. $P_*(S)$ is the set of all $*$-predecessors of m-formulas in S for $* \in \{\alpha, \beta, \gamma, \delta\}$ (see Definition 3.12). Given a proof in $\mathtt{S4}''^{\Delta}$, we say an equivalence relation defined on the proof is stable if it satisfies the following conditions:*

1. *every induced equivalence class is stable,*
2. *for each $* \in \{\alpha, \beta, \gamma\}$, P_* will be in some equivalence class entirely, and P_δ is in the union of at most two equivalence classes, entirely.*
3. *there is no induced circular superchain.*

A proof is stable if we can find a stable equivalence relation on it.

Definition 4.12. *Given a stable proof in* $\mathtt{S4}''^{\Delta}$ *via an equivalence relation* $\sim$*, a characteristic proof assignment* p *is stable if it also satisfies equations* $p(F,i) = p(G,j)$ *for any* $\Box F^i \sim \Box G^j$*.*

Theorem 4.13. $\mathcal{H}$ *is a proof in* $\mathtt{LP}$ *if and only if there is a stable proof* $\mathcal{F}$ *in* $\mathtt{S4}''^{\Delta}$ *and a stable characteristic proof assignment* p *on* $\mathcal{F}$ *such that* $\mathcal{H} = \mathcal{F}^p$*.*

Proof. Suppose $\mathcal{F}$ is a stable proof via a stable equivalence relation, the construction of stable characteristic proof assignment p is just the procedure in Lemma 3.14, but additionally require that when an m-formula has no predecessors, we have to assign a term to the m-formula in a way that every m-formula in the same equivalence class will get the same term. Then it can be shown that $\mathcal{F}^p$ will be an $\mathtt{LP}$ proof. For the other direction, just as the proof in Theorem 3.15 shows, given a proof $\mathcal{H}$ in $\mathtt{LP}$, hence a proof in $\mathtt{ELP}$, we will have an $\mathtt{S4}''^{\Delta}$ proof $\mathcal{H}^\eta$ and a proof assignment p such that $(\mathcal{H}^\eta)^p = \mathcal{H}$. Then the equivalence relation on m-formulas in $\mathcal{H}^\eta$ such that $\Box F^i \sim \Box G^j$ if and only if $i = j$ will be stable. Hence $\mathcal{H}^\eta$ is a stable proof. ⊣

One observation is that in an $\mathtt{S4}''^{\Delta}$ proof if we enlarge all numbers larger than a fix number by a fix number, then the resulting sequence is still an $\mathtt{S4}''^{\Delta}$ proof. Hence in the following we will suppose the difference between two consecutive numbers are far enough to fit our need.

Proposition 4.14. *Every proof in* $\mathtt{S4}''^{\Delta}$ *can be extended to a stable proof.*

Proof. The purpose of this algorithm is to repeatedly use $\mathtt{S4}''^{\Delta}$A4 axioms to stablize every m-formula such that every A1-formula has at most one predecessor pair, every A2-formula has at most one γ-predecessor, and every A4-formula has at most two δ-predecessors, and for these formulas, there are no predecessors other than the ones described. Then the identity relation on m-formulas in the resulting proof is a stable equivalence relation. Now suppose, say, there are A1 axioms $\phi_1 \equiv \Box(F \to G)^i \to \Box F^j \to \Box G^k$, and $\phi_2 \equiv \Box(H \to G)^m \to \Box H^n \to \Box G^k$ in a proof, then $\Box G^k$ is an A1-formula with two predecessor pairs. We add axioms $\Box G^x \to \Box G^k$, $\Box G^y \to \Box G^k$, $\Box(F \to G)^i \to \Box F^j \to \Box G^x$, $\Box(F \to G)^i \to \Box F^j \to \Box G^y$ to the proof, where $\Box G^x$ and $\Box G^y$ are new, such that ϕ_1 and ϕ_2 become derived formulas. Also sometimes ϕ_1 will be applied by *axiom necessitation* to have formula $\Box \phi_1^i$. Then we add more formulas including $\Box(\Box G^x \to \Box G^k)^0$, $\Box(\Box(F \to G)^i \to \Box F^j \to \Box G^x)^0$ to have $\Box\phi_1^i$ derived. Repeat steps of this kind till we have a stable proof. ⊣

Now the overall procedure, starting from an $\mathtt{S4}G^-$ proof of an $\mathtt{S4}$ theorem, of our algorithm for the realization theorem can be concluded as:

$$\mathtt{S4}G^- \underset{4.4}{\hookrightarrow} \mathtt{S4}^{\Delta}G^- \underset{4.5}{\hookrightarrow} \mathtt{S4}^{\Delta} \underset{4.10}{\hookrightarrow} \mathtt{S4}'^{\Delta} \underset{4.14}{\hookrightarrow} (\mathtt{S4}''^{\Delta})^* \underset{3.15}{\hookrightarrow} \mathtt{LP},$$

where each logic name stands for its proofs, hookarrows mean proof transformations, the number under every arrow is the proposition or theorem where you can find the algorithm, and $(\mathtt{S4}''^{\Delta})^*$ denotes stable proofs in the logic.

Theorem 4.15. *A formula $\phi \in L_\Box$ is an* $\mathtt{S4}$ *theorem if and only if there is a realization r such that ϕ^r is an* $\mathtt{LP}$ *theorem.*

In Brezhnev and Kuznets [7], it is proved that the original realization procedure in [2] creates a proof of size exponential to the size of initial cut-free $\mathtt{S4}$. They improved the procedure to have a polynomial algorithm. Our procedure, though including several steps, should also be polynomial, if we use the structural method to convert an $\mathtt{S4}^{\Delta}$ proof to an $\mathtt{S4}'^{\Delta}$ proof, since the original procedure in [2] spiritually adopted the inductive method by repeating the lifting lemma[3].

5 Discussions

One of the consequences of this paper is that $\mathtt{LP}$-style logics, as well as Δ-style logics, can be taken as instruments for studies on the structure of modal logic proofs, especially non-circular proofs, which are detemined by $\mathtt{LP}$-style logics. We have shown that through the theorem realzation procedure every $\mathtt{S4}$ theorem has a non-circular proof suggested by $\mathtt{LP}$, and this procedure can be easily generalized as a way to prove that every theorem in a modal logic with a cut-free Gentzen proof system can be realized to a theorem in a given $\mathtt{LP}$-counterpart of the logic, and the realizability of theorems immediately leads to the completeness of non-circular proofs, i.e. every theorem has a non-circular proof suggested by the given $\mathtt{LP}$-style logic. To gereralize the procedure, all we need to do is provide a Δ-style cut-free Gentzen system with adequate Δ-modal rules corresponding to the $\mathtt{LP}$-counterpart given for the modal logic. Below we take $\mathtt{GL}$ and $\mathtt{S5}$ as examples.

Here we consider three versions of $\mathtt{LP}$-style of $\mathtt{GL}$ at once. Each is $\mathtt{LP}$ with the A3 axiom $t{:}F \to F$ being replaced by one of the following $\mathtt{LP}$-style

[3]Lifting Lemma [2, Lemma 5.4] for $\mathtt{LP}$: if $s_1{:}F_1, \ldots, s_n{:}F_n \vdash G$ then there is a proof term t such that $s_1{:}F_1, \ldots, s_n{:}F_n \vdash t{:}G$.

Löb axioms: $s : (t{:}F \to F) \to u{:}F$, with $u = *s$, $*t$, or $s * t$ for a functional symbol $*$. The Δ-style counterparts of these LP-style *Löb* axioms would be $\Box(\Box F^j \to F)^i \to \Box F^k$, where $k > f(i,j)$, for $f(i,j) = i$, j, or $\max(i,j)$, respectively. The Δ-modal rule of the cut-free Gentzen system for these $\mathtt{GL}^{\Delta}$ logics are

$$\frac{\Box\Gamma^{\iota}, \Gamma, \Box A^{j} \Longrightarrow A}{\Box\Gamma^{\iota} \Longrightarrow \Box A^{k}},$$

for any $k > f(k', j)$ with $k' = \max(\iota) + 2|\Gamma| + 1$. The soundness of these rules with respect to their corresponding $\mathtt{GL}^{\Delta}$ logics shows that every GL theorem can be realized to a $\mathtt{GL}^{\Delta}$ theorem and, by our proof realization algorithm, to a theorem in the corresponding LP-style GL logic. These imply that every GL theorem has a non-circular proof of the type determined by these LP-style GL logics.

The peculiarity of Fitting's cut-free Gentzen system for S5 is that in order to justify the theoremhood of a formula ϕ, one should establish a proof of $\Rightarrow \Box\phi$ instead of $\Rightarrow \phi$. But this makes no problem for us.[4] One of the LP-style *5* axiom is taken to be $\neg t{:}F \to ?t{:}t{:}F$ in the literature[5], and its Δ-counterpart is $\neg\Box F^i \to \Box(\neg\Box F^i)^j, j > i$. Here's the right Δ-modal rule (there is no numerical conditions for the left Δ-modal rule), where multisets $\Gamma' = \{C'_i\}$ and $\iota' = \{j'_i\}$:

$$\frac{\Box\Gamma^{\iota} \Rightarrow \Box\Gamma'^{\iota'}, A}{\Box\Gamma^{\iota} \Rightarrow \Box\Gamma'^{\iota''}, \Box A^{k}},$$

for any $k > \max(\iota, \iota') + (|\Gamma| + |\Gamma'|) + 1$, and for any $j''_i \in \iota''$, $j''_i \geq j'_i$. Notice that the principal label of the positive m-formula $\Box A^k$ relies on principal labels of other positve m-formulas.

Some LP-style counterparts of normal modal logics such as K, D, K4, D4, and KD4 have been introduced in the literature[6]. Our procedure can also be adapted to give another algorithmic proof of the *realization theorem* for these logics.

One thing to be noticed is that not all types of non-circular proofs are complete. Theoretically, there should be more incomplete sets of non-circular proofs than complete ones. But what is interesting is that those determined by the natural stamps, or to say the natural LP-style logics, like what we have just mentioned, are all complete. This makes us wonder what common factors they share. One guess would be that the stamp collects only direct edges from negative m-formulas to positive ones. But this is not the case. The LP-style *5* axiom that we have here is a counterexample. Thus

[4] Fitting [9] also gave an alogrithmic proof of the realization theorem for S5 based on this cut-free Gentzen system.

[5] See [16], and [17]

[6] See [5] and [6]

the problem remains open.

Acknowledgements

I would like to thank profefossor S. Artemov for encouraging this work in many aspects. Thank professor M. Fitting for reading several earlier drafts and providing many precious suggestions. Thank R. Kunzets for valuable comments and criticisms including catching an error. Also thank J.-Y. Teng for her assitance in editing the text, and T. Protopopescu for proofreading an earlier draft.

References

[1] S. Artemov. Operational modal logic. Technical Report MSI 95-29, Cornell University, 1995.

[2] S. Artemov. Explicit provability and constructive semantics. *Bulletin of Symbolic logic*, 7(1):1–36, 2001.

[3] S. Artemov. Justified common knowledge. In *Theoretical Computer Science*, volume 357(1-3), pages 4–22, 2006.

[4] S. Artemov. The logic of justification. *The Review of Symbolic Logic*, 1(4):477–513, 2008.

[5] V. Brezhnev. On explicit counterparts of modal logics. Technical report, Cornell University, 2000.

[6] V. Brezhnev. On the logic of proofs. In *13th European Summer School in Logic Language and Information, Proceedings of the 6th ESSLLI Student Session, 2001, Helsinki*, pages 35–46, 2001.

[7] V. Brezhnev and R. Kuznets. Making knowledge explicit: How hard it is. *Theoretical Computer Science*, 357:23–34, 2006.

[8] S. Feferman, editor. *Kurt Gödel Collect Works.* Oxford, 1986-2003. 5 volumes.

[9] M. C. Fitting. The realization theorem for S5 a simple, constructive proof. Manuscript.

[10] M. C. Fitting. A simple propositional S5 tableau system. *Annals of Pure and Applied Logic*, 96:107–115, 1999.

[11] M. C. Fitting. A logic of explicit knowledge. In *In L. Behounek and M. Bilkova (Eds.), Logica Yearbook 2004*, pages 11–22. Filosophia, 2005.

[12] M. C. Fitting. The logic of proofs, semantically. *Annals of Pure and Applied Logic*, 132:1–25, 2005.

[13] K. Gödel. Vortrag bei zisel. Translated as *Lecture at Zisel's* in [8] III, 62-113, 1938.

[14] K. Gödel. Eine interpretation des intuitionistischen aussagenkalkuls. *Ergebnisse eines Mathematischen Kolloquiums.*, 4:39–40, 1933. Translated as *An interpretation of the intuitionistic propositional calculus* in [8] I, 296-301.

[15] E. Goris. Explicit proofs in formal provability logic. In *LFCS*, pages 241–253, 2007.

[16] E. Pacuit. A note on some explicit modal logics. In *Proceedings of the Fifth Panhellenic Logic Symposium*, pages 117–125, 2005.

[17] N. Rubtsova. Evidence reconstruction of epistemic modal logic S5. In D. Grigoriev, J. Harrison, and E. A. Hirsch, editors, *CSR*, volume 3967 of *Lecture Notes in Computer Science*, pages 313–321. Springer, 2006.

[18] A. Troelstra and H. Schwichtenberg. *Basic Proof Teory.* Cambridge University Press, 1996.