Annals of Pure and Applied Logic 165 (2014) 1318–1338

Contents lists available at ScienceDirect

Annals of Pure and Applied Logic

www.elsevier.com/locate/apal

Non-circular proofs and proof realization in modal logic ☆

Ren-June Wang

Department of Philosophy, National Chung-Cheng University, No.168, Sec. 1, University Rd., Min-Hsiung Township, Chia-yi County 621, Taiwan

ARTICLE INFO

Article history:
Received 22 December 2012
Received in revised form 13 July 2013
Accepted 15 July 2013
Available online 29 April 2014

MSC:
03B42
03B45
03B60
03F07

Keywords:
Justification logic
Timed modal epistemic logic
Modal logic
Realization theorem
Hilbert-style proofs

ABSTRACT

In this paper a complete proper subclass of Hilbert-style S4 proofs, named non-circular, will be determined. This study originates from an investigation into the formal connection between S4, as Logic of Provability and Logic of Knowledge, and Artemov's innovative Logic of Proofs, LP, which later developed into Logic of Justification. The main result concerning the formal connection is the *realization theorem*, which states that S4 theorems are precisely the formulas which can be converted to LP theorems with proper justificational objects substituting for modal knowledge operators. We extend this result by showing that on the proof level, non-circular proofs are exactly the class of S4 proofs which can be realized to LP proofs. In turn, this study provides an alternative algorithm to achieve the realization theorem, and a novel logical system, called $S4^{\Delta}$, is introduced, which, under an adequate interpretation, is worth studying for its own sake.

1. Introduction

One of many applications of modal logic in computer science is to serve as logic of knowledge, for reasoning about the information transmissions in distributed systems (e.g. [16,8,14]), or about the intentional level of multiagent systems in general ([7,22]). Artemov's Logic of Proofs, LP ([1,2]), later developing into Justification Logic ([10,9,3,4]), enhances the expressivity of modal epistemic logic by introducing justification into the language. Formulas of the like $t{:}F$ are introduced with the intended meaning that "*t is a proof of F*" or "*t is a justification of F*", where t is a structural object, called *proof term* or *proof polynomial*, to stand for an explicit proof in formal arithmetic, or a justificational object. One of the main theorems concerning LP is about its formal relation with the modal logic S4. The *realization theorem* says that S4 theorems

☆ This article is a part of a special issue and it should have appeared in Annals of Pure and Applied Logic, Volume 165 Issue 1, but was omitted in error.

E-mail address: wrenjune@gmail.com.

http://dx.doi.org/10.1016/j.apal.2014.04.004

are exactly the formulas which can be turned into LP theorems by substituting suitable proof terms for the modal occurrences. Interpreted epistemically, the theorem shows that there is indeed a justification structure embedded in S4, as logic of knowledge, which can only be explicitly disclosed in the formalism of LP. The realization theorem is also the motivation for the introduction of Logic of Proofs. As a long standing question concerning the arithmetic foundation of intuitionistic logic, Gödel took the first step to embed intuitionistic logic into S4, as logic of provability ([12]), and Artemov furnished LP with a formal arithmetic semantics and then proved the realization theorem to complete the project.

Accordingly, a constructive syntactical proof for the realization theorem is offering an algorithmic procedure to extract the reasoning processes, the justification objects, from the logic of knowledge S4, and hence worth further attention. However, we find it is interesting and also puzzling in the original procedure given in [1,2] and later improved in [5], that a detour to analyze cut-free Gentzen-style S4 proofs is made, even though originally LP is introduced in Hilbert-style and presented in a way that it is almost a realized counterpart of the standard Hilbert-style S4 system; and proof terms, which are also suggested to be regarded as combinators in some general way ([2]), are best understood as encoding proofs in Hilbert-style. So naturally, questions are raised: What happens to the Hilbert-style S4 proofs? What is the formal relation between S4 proofs and LP proofs, if both in the style of Hilbert? Can we extend the result of the realization theorem to concern S4 proofs, instead just of theorems? Thus although the realization theorem is introduced with significance in application, it seems to suggest a deeper insight of the proof structure of modal logic. One of the contributions of this paper is to determine a complete proper subclass of Hilbert-style proofs of S4, called *non-circular*, and show that this is exactly the class of proofs which can be realized to LP proofs.[1]

In the present paper, we will first give a characterization of non-circular S4 proofs and then endeavor to show that the class is complete in the sense that every S4 theorem has a non-circular proof. It is our long-term goal to find an algorithm that can directly turn circular proofs into non-circular, but, partly because a proof-theoretical tool like cut elimination and normalization which can generate a normal form of a Hilbert-style proofs, no matter what it is, does not exist yet, we adopt an alternative procedure in the following. For, as we know, there is a natural way of translating proofs in Gentzen-style to Hilbert-style, we will show that, following the translation, the Hilbert-style proofs obtained from cut-free proofs are non-circular. This result, which in turn justifies the completeness of non-circular proofs, in a way explains why the detour in the original proof of the realization theorem takes place and why the proof works well.

In the course of our discussions, a novel logical system called $S4^{\Delta}$, with numerical labels for each modal occurrence, will be introduced. The purpose of this introduction is to help to investigate the non-circularity of S4 proofs. We will show, on the one hand, that non-circular S4 proofs are precisely those which can turn into $S4^{\Delta}$ proofs by getting suitable numerical labels, and, on the other hand, we will prove that there is an efficient algorithm which can convert $S4^{\Delta}$ proofs into LP proofs, and vice versa. Putting these two algorithms together, the desired proof realization procedure connecting non-circular S4 proofs and LP proofs is then established, and, furthermore, the overall process, including the translation of a cut-free Gentzen-style proof to a non-circular S4 proof, provides an alternative algorithm for the realization between theorems of S4 and LP.

$S4^{\Delta}$ as demonstrated here is an immediate logic between S4 and LP. It should serve well as a technical tool for the future study on the proof-theoretical structures of the both sides of the logic. But it is also an interesting logic worth studying for its own sake, depending on the interpretation of the numerical labels in the language of $S4^{\Delta}$. For example, with a direct connection with the interpretation of proof terms in LP as standing for explicit proofs, these labels could be understood as the lengths of proofs, and hence $S4^{\Delta}$ is a system of studying the syntactical property of proofs. And on the other hand, these labels can be understood as representing the time that the modeled reasoners take to perform inferences to increase

[1] A non-constructive proof for the realization theorem based on a possible-world style of semantics for LP can be found in [10], and a recent constructive realization algorithm is developed based on analyzing proofs in systems of nested sequents ([13]).