学位論文内容の要約

博士の専攻分野の名称: 博士(文学)　　　　　　　　　　氏名: 蘇有安

学位論文題名

Proof-Theoretic Study of Epistemic Logic from an Intuitionistic Viewpoint

(直観主義的観点からの認識論理の証明論的研究)

The main purpose of this thesis is to provide a proof-theoretic study on epistemic logic from an intuitionistic viewpoint.

In the study of logic, the proof-theoretic method and the semantic method can be thought of two sides of a coin. The semantic method concentrates on studying the truth values of logical statements via mathematical models. The proof-theoretic method concentrates on studying proofs of statements via the validity of deduction based on axioms and inference rules. These two sides are both indispensable in the study of logic. Furthermore, by the well-known results of soundness theorem (which states that a provable sentence is always true) and completeness theorem (which states that a sentence that is always true is provable), we can show that these two sides coincide with each other.

Epistemic logic aims to capture concepts like knowledge and belief by a formalized method developed from modal logic. The work of von Wright (1952) and Hintikka (1962) gave birth to epistemic logic. Hintikka established the formalization of knowledge and belief. A formula KaA can be read as agent "a" knows that A is the case. Then, for example, the formula KaA → A states that "if A is the knowledge, then it is the case" and formula KaA → KaKaA states that " if A is known, then this is also known. " These formulas are generally accepted in the classical epistemic logic for the knowledge in Hintikka. Let us introduce the Kripke model or relational model of epistemic logic, where we have W denoting the set of states or possible worlds and a binary relation R denoting the indistinguishable relation between two states, V denoting the valuation function from the set of propositional variables to the power set of W. In this setting, we say that KaA holds in the state w if and only if for any state v which are connected to w by Ra, A is true in v. That is to say, if agent a looks at every indistinguishable state from where he or she stands and finds that A is true in any state, then we say that a knows that A is the case.
It is worth mentioning that group knowledge is also studied in the development of epistemic logic. There are three kinds of group knowledge which are studied most: The first can be described as "it is known by everyone"; the second is common knowledge which states that "it is commonly known to be the case "; the third is "distributed knowledge ", which states that after combining the knowledge from everyone, "it is distributively known to be the case ". In this thesis, we only concentrate on distributed knowledge. This topic is inspired by the situation

in which a group of agents obtain new knowledge by putting their knowledge together; more specifically, new knowledge is obtained by someone outside the group. For example, suppose we get KaA i.e., A is known by agent a, and Kb(A → B) i.e., A → B is known by agent b. Then, after combining the knowledge together, we have D{a,b}B, where B is known to be the case. In the Kripke model, distributed knowledge among a group G can be captured by taking the intersection of the indistinguishable relations of every agent in the group G. If A is true in any states which are considered to be possible by both a and b (taking the intersection of Ra and Rb), then we say that D{a,b}A is true.

For a long time, the study of epistemic logic has mainly focused on the semantic side. The proof theoretic studies are mainly concentrated on the Hilbert system. However, the Hilbert system is not a well-behaved tool. When we want to prove the consistency of a system, or to prove that some formulas are not provable by proof-theoretic methods, it is difficult to use the Hilbert system. Instead, studies using sequent calculi can overcome these problems. A sequent is a pair of logical formulas in the form of $\Gamma \Rightarrow \Delta$, which aims to capture the inference in the form "if all formulas in Γ hold, then some formulas in Δ hold."

Sequent calculus, which was established by Gentzen (1935), provides us the following merits in the proof-theoretic approach. First, the cut-elimination theorem in sequent calculi enables us to prove consistency and unprovability directly via the method of proof-search. Second, in sequent calculus, most logical axioms can be captured in the form of logical inference rules. As a result, we can look into the details and structures in a proof. Later, this feature makes a study on the derivation of the knowability paradox much easier.

There have been studies on the epistemic logic using sequent calculi, for example using the methods of hypersequents (Poggiolesi 2013), where a hypersequent is a finite multiset of sequents, or labeled-sequents, where the Kripke semantics can be reflected in syntax and then internalized into sequent calculi (Negri 2005). Compared to these studies, we want to concentrate on the ordinary notion of Gentzen's original sequent calculus, which is a cornerstone of the development of sequent calculi. By investigating this direction, our study can be a basis for the further development of other proof-theoretic studies on the topic of epistemic logic. Furthermore, in the original Gentzen sequent calculi, the intuitionistic sequent calculi can be obtained by restricting the setting of classical sequent calculi. This makes a study on a possible relationship between classical epistemic logic and intuitionistic epistemic logic much more straightforward and easier.

Since the work of von Wright and Hintikka, the development of epistemic logic has been often based on the classical logic, in which the Principle of the excluded middle (PEM) $A \vee \neg A$ is always true. That is to say, in the classical epistemic logic, for any proposition A, either it is true or its negation is true. Compared to classical logic, intuitionistic logic, which is developed from intuitionism, has fewer axioms and is more close to humans' ability of inference. Intuitionism was introduced by L. E. J. Brouwer. From its birth, the goal of intuitionism has been to rebuild the validity of mathematical truth on the basis of human activity. It is most known for its objection to the principle of bivalence, which claims the truth value of any proposition must be true or false. As a consequence, intuitionistic logic does not suggest the validity of the (PEM) $A \vee \neg A$.

One remarkable step in the development of intuitionism is the famous Brouwer-Heyting-Kolmogorov interpretation (BHK interpretation) of the logical connectives. The BHK interpretation provides a way to escape from understanding the validity of a proposition only by its truth value. Instead, we can now hold the validity of a proposition by an analysis of its proof; that is to say, we can say that a proposition is valid if we can always find a proof for it. This proof consists of subproofs which are arranged on the basis of the complexity of the proposition. By taking the BHK interpretation, we can reject the principle bivalence and the principle of the excluded middle. Furthermore, it also opens the gate to studying the validity of intuitionistic truth via a proof -theoretic method.

In the classical epistemic logic, $Ka(A \vee \neg A)$ is true for any agent a, and for any proposition A. This is not always the case. By taking intuitionistic logic as the basis in the study of epistemic logic, we can block this problem. In other words, compared to the classical epistemic logic, the intuitionistic epistemic logic provides an approach to studying the information changes in agents who do not accept (PEM). In what follows, we concentrate on the well-known knowability paradox, which is a touchstone in the study of the difference between the intuitionistic epistemic logic and the classical epistemic logic. The knowability paradox, also known as the Fitch-Church paradox, states that, if we claim that every truth is knowable $A \to \langle\rangle KA$ (the formula $\langle\rangle B$ denotes that B is possible), then we are forced to accept its consequence that every truth is known $A \to KA$. This paradox is commonly recognized as a threat to Dummett's semantic anti-realism. That is because that the semantic anti-realists claim the knowability principle (KP), i,e., every truth is knowable, but they do not accept the omniscience principle (OP) , i.e., every truth is known. Since Dummett (1963) admitted he had taken some of the basic intuitionistic features as a model for the anti-realist view, the method of switching an underlying logical system to the intuitionistic one to avoid the paradox has attracted much attention. However, a relation between the classical epistemic logic and intuitionistic epistemic logic has not been clarified for the knowability paradox.

Question 1. What is a relationship between intuitionistic epistemic logic and classical epistemic logic in the knowability paradox?

We answer this question in Chapter 3. Glivenko translation and Kuroda translation can provide a method to embed the classical logic in the intuitionistic logic, which allows us to study the classical validity in the intuitionistic logic. We provide a similar translation in the context of the knowability paradox to study a relationship of inferences in classical epistemic logic and inferences in intuitionistic epistemic logic. To prove this result, we provide sequent calculi in both classical and intuitionistic logic to analyze the knowability paradox. We also show that the omniscience principle is not valid in the intuitionistic logic for the knowability paradox.

The second and third questions focus on the intuitionistic epistemic logic IEL from Artemov and Protopopescu (2014). As we have mentioned, in the knowability paradox, the formula $A \rightarrow KA$ is generally considered as the omniscience principle (OP). However, Artemov and Protopopescu suggest that the formula of the form $A \rightarrow KA$ should be accepted as a cornerstone of intuitionistic epistemic logic based on the BHK-interpretation. They proposed the following BHK interpretation for KA: a proof of a formula KA (it is known that A) is the conclusive verification of the existence of a proof of A. According to Artemov and Protopopescu, a conclusive piece of evidence that verifies the existence of a proof can be given by zero-knowledge protocols (for example, an encrypted message), testimony of an authority, classified sources, and existential generalization (we may know that some elements exist for sure; however, we cannot provide such an example). Basically, a proof of $A \rightarrow B$ is a construction such that given a proof of A, the construction gives us a proof of B. Then, a proof of A itself can be regarded as the verification of the existence of the proof of A. In this sense, we always have such a proof of $A \rightarrow KA$, i.e., $A \rightarrow KA$ is valid. Then, the propositional intuitionistic epistemic logic IEL accepts $A \rightarrow KA$ as an axiom. Hintikka had given arguments for first-order epistemic logic. He mentioned that if we want to deal with the locutions like "knows who", "knows when", and "knows where", we can translate these expressions into a language with quantifiers and equality symbols. Since the study of Artemov and Protopopescu (2016) concentrates only on the propositional part, it raises the second question.

Question 2. Can we give a suitable first-order expansion with a sequent calculus for intuitionistic epistemic logic IEL ?

To answer this question positively, in Chapter 4, we add the equality, function symbols and quantifiers into the IEL. We also give the sequent calculi for both propositional IEL and first-order IEL. We also check that the BHK-interpretation of the quantifiers fits the BHK-interpretation of the knowledge operator well. Next, we move to our final question. As we have mentioned above, intuitionism is a movement to found the mathematical truth on human creative activities. Then, it is very natural to consider a distributed intuitionistic knowledge to capture the idea that some knowledge is known by a group of agents, for example, a community consisting of professional mathematicians. Meanwhile, as we have mentioned above, in Artemov and Protopopescu, a conclusive verification can be based on many different sources, for example, zero-knowledge protocols and classified sources. Then, the following scenario can be taken into consideration: in the community of professional researchers, there are some knowledge $D\{a,b\}A$ that can be considered as the results of combining the contributions K_aB, $K_b(B \rightarrow A)$ of other researchers a,b by citing their works. In this case, we may not be able to check every detail of the proof of B and $B \rightarrow A$. However, we can still verify the existence of the proof B, $B \rightarrow A$

based on zero-knowledge protocols or classified sources. In this respect, it is very natural to regard that verification obtained by multiple agents can also generate a conclusive verification.

Question 3. Can we develop the intuitionistic epistemic logic IEL to cover the distributed knowledge?

To answer this question positively, in Chapter 5 a distributed knowledge is added into the IEL. The new system is studied by the semantic and proof-theoretic methods. A new BHK-interpretation for the distributed knowledge is also proposed to be coordinated with that from Artemov and Protopopescu.