氏名(本籍・生年月日)Pratima Kumari Shah (Nepal 1981年10月8日)
学位の種類　博　士（工学）
学位記番号　甲 第 616 号
学位授与の日付　平成２６年９月３０日
学位授与の要件　信州大学学位規程　第５条第１項該当
学位論文題目　**On the Formal Verification of Petri Net Properties using a Mechanized Proof Checker Approach**
(プルーフチェッカーシステムを用いたペトリネットの性質の形式的検証について)
論文審査委員　主査　准教授　Pauline N. Kawamoto
教　授　Yasunari Shidama
教　授　Minoru Maruyama
教　授　Jun Kawabe
准教授　Artur Kornilowicz (University of Bialystok 大学)

論 文 内 容 の 要 旨

In this work, we use a theorem checking system called Mizar to formalize token boundedness property of a subclass of Petri nets. The rigorous Mizar formalization and mechanical theorem verification presented in this work uncovers a common example of how information omitted from natural language descriptions of mathematical concepts and proof can lead to areas of ambiguity.

Both natural language and formal language descriptions of hardware and software systems and their properties are widely used in the area of computer science. Petri nets are often used to mathematically model and examine concurrent behaviors of hardware and software systems. However, when definitions and proofs of Petri net properties are expressed in natural language, details (trivial proof) that appear obvious for expert mathematicians or are repeated often are sometimes omitted from these descriptions, leaving the reader to fill in the gaps in order to understand. This kind of problem can occur because definitions in natural language are not always precise. Some missing information can cause errors or ambiguity in interpretation when developers try to apply these concepts to tools for system modeling and analysis.

Such errors may have catastrophic consequence in terms of money and time. In general an earlier an error is detected, the cheaper it is to fix, which eventually produces reliable hardware and software systems with high quality.

In this work, the Mizar system is used for the formal verification of token boundedness property of a subclass of Petri nets called decision free Petri nets, which has the characteristics that every place in the net has exactly one input transition and one output transition, and mechanically verify that this formalization is semantically and logically correct. The Mizar language descriptions are more complete because every statement in this language must be fully justified with no jumps in the chain of logic. Using a number of basic Petri nets constructs already verified by the Mizar system and accepted to its repository of mathematical information, we built an extension for the decision free Petri nets and proved the token boundedness property of their circuits. While formalizing, we found clear examples of how gaps available in natural language descriptions of mathematical concepts and proofs in literature can lead to areas of ambiguity and highlight the value of using mechanical systems proof checking mechanisms to formalize such notions and archive all details of the corrected materials in the open digital library of Mizar for reuse. This type of archiving of mechanically verified Petri net knowledge can serve as a reliable source for system modeling tool developers who rely on a common and clear understanding of the concept definitions and proofs, and also for the beginner reader.

The motivation of this research is to demonstrate the power of formalization techniques and its application to the formal verification of theorems concerning mathematically rich Petri net models with high reliability. In the future, the formal proofs of decision free Petri nets in the database of the theorem checking system can be used to analyze the liveness and safeness properties in directed circuits of Petri nets.