氏　　名	海 津 智 宏		
学 位 の 種 類	博士(情報科学)		
学 位 記 番 号	博情第 303 号		
学位授与年月日	平成 26 年 6 月 24 日		
論 文 題 目	プロセス代数に基づく非決定的なシナリオ合成によるシーケンス図の検証		
論文審査委員	主査	鈴木 正人	北陸先端科学技術大学院大学　准教授
		青木 利晃	同　准教授
		緒方 和博	同　准教授
		磯部 祥尚	産業技術総合研究所　教授
		田原 康之	電気通信大学 大学院　准教授

論文の内容の要旨

In recent years, software development process is required to support for diversification and multi-platform by the shorter delivery time. In order to develop a system to efficiently respond to such requests, software development using component has spread. When defining the structure and behavior of software components, UML diagrams are often used. UML is a standardized modeling language developed by OMG. Especially in upstream development, UML sequence diagrams are frequently used to understand and verify the behavior of components.

However, the specification of sequence diagram is complicated and flexible. Also, in many cases, the detailed behavior has not been determined in early development stage. For example, developers can design login process as “return a success message if the user name and the password are correct, return a failure message if the user name and the password are invalid”. Here, if the way how passwords are stored and they are checked has not been designed yet, it cannot be described deterministically whether it should return a success message or a failure message. For these designs, it is important to verify designs leaving the nondeterminism like “return a success message or a failure message nondeterministically”. Using conventional methods, it was difficult to handle those nondeterminism. Therefore, it was difficult to verify sequence diagrams automatically. It has relied on manual review to find mistakes such as inconsistencies and insufficient refinements between sequence diagrams. If such mistakes are found in a late development stage, it may take a lot of time and cost to correct them.

In this paper, we define a subset of sequence diagrams with formal semantics and propose a method to verify consistency of the sequence diagrams. With this method, developers can clarify the specifications by using formal description and find bugs by using automatic verification.

In order to verify sequence diagrams, we propose a synthesis method of a formal expression called CSP (Communicating Sequential Processes) from sequence diagrams. This synthesis method consists of following steps: At first, an order of sending and receiving is extracted from each sequence diagram for each component and it is formally expressed as a CSP process. Next, two or more CSP processes extracted from a number of sequence diagrams for the component is combined to a CSP process which represents the whole behavior of the component. We define new CSP operators for synthesizing sequence diagrams. Finally, using expansion rules of the new CSP operators, the CSP process is converted into a standard CSP process without the new operators. The standard CSP process can be verified using existing CSP tools such as PAT and FDR2. In addition, counter examples found in the model checking can be translated back to sequence diagrams for supporting to correct their inconsistency.

Compared with the related works, the main advantage of this work is that nondeterminism can be considered. It means that our approach can handle abstract sequence diagrams. Sequence diagrams are often abstract in early development stage. Our approach can be applied to such diagrams.

We implemented a tool named SDVerifier, based on the proposed method, which can be used for verifying sequence diagrams. We also conducted experiments with real world case studies.

Keywords
Sequence Diagram, Process Algebra, CSP, Process Synthesis, Verification

論文審査の結果の要旨

当博士論文はソフトウェア開発で使用されるシーケンス図の検証を行うことを目的として、形式手法のひとつであるプロセス代数を用いた新しいシナリオ合成の手法の提案とツールの実装、評価について論じたものである。シーケンス図の意味論および検証に関しては Live Sequence Chart をはじめとしたいくつかの研究があるが、それらの多くは実際のシステム構築において頻繁に発生する非決定的なメッセージの選択を表現する機構が十分ではない。

特に複数のシナリオを合成することで発生する通信の非決定性に関しては、送信側が非決定的にメッセージを選択することを記述/検証可能なモデルが存在しなかった。本論文ではプロセス代数である CSP を用いてシーケンス図を数学的に記述し、そこで発生するメッセージの選択によっていわゆるデッドロックが発生しないことや、ある段階での振る舞いの記述を次の段階で詳細化した際に問題となる「一致性の保持」に関する検証を可能としている。最初に各シーケンス図をオブジェクトを単位として CSP のプロセスに変換し、次に複数のシーケンス図に記述されるシナリオの合成を表現するために CSP を拡張した記法と意味論として eCSP を導入する。これは標準 CSP に合成を表す o と,送信イベントを内部化する$の 2 つの演算子を CSP に導入し、トレース等価および失敗等価という 2 種類の等価性によってその意味を形式的に定義したものである。通常の CSP に用意されている演算子ではイベント発生後に分岐する場合の記述が不十分であるが、新しい演算子の導入により合成後の内部選択/外部選択を適切に記述することが可能になる。次に eCSP による記述を従来の検証ツール(PAT)で扱うことが可能なように変換のアルゴリズムを定義する。その際にオブジェクトの生成/消滅を記述できるように「準備状態」という概念を導入し、またオブジェクト間のパラメタ受け渡しなどを実現している。また事例研究として実際の企業内で使われているシステム(電子商取引)の一部を記述、検証し、意図的に誤りを混入した場合にそれを検出、反例解析による原因の特定にも成功している。また大規模システムへの適用の可能性について実験を行い、実用性も十分であることを示している。

以上、本論文は、ソフトウェアの仕様としてシーケンス図の合成と検証について新しい理論を構築し、数学的な証明と実践によりその有効性を示したものであり、学術的に貢献するところが大きい。よって博士（情報科学）の学位論文として十分価値あるものと認めた。