ソフトウェアパターンに基づく体系的設計・検証手法の研究

金井 勇人 (410031)

北陸先端科学技術大学院大学 情報科学研究科

2006 年 2 月 9 日

キーワード: モデル検査,SPIN, 検証パターン, ソフトウェアパターン.

近年，色々なところで組み込みソフトウェアが使用されるようになってきており，その信頼性が社会的な問題となっている．組み込みソフトウェアが大規模化，かつ複雑化してきており，従来の開発・検証手法の限界が指摘されている．そこで，形式的検証手法に注目が集まっている．しかしながら，形式的検証手法は論理的な記述等があり，ソフトウェア開発に適用するには，ソフトウェア技術者に対して，大変な労力を必要とする．そのため，形式的検証手法を適用するための体系だった手法が求められている．

形式的検証手法の１つにモデル検査がある．この検証技術は，ソフトウェアの有限状態モデルが，論理で表現された性質を満たすかどうかを状態の網羅的な探索によって検証を行う技術のことである．モデル検査技術を UML 等で記述される設計モデルに適用することにより，ソフトウェアの信頼性を高めることが期待できる．しかし，検証するためには UML 等で記述されている内容をモデル検査ツールで，そのツールに依存した言語 (以下，仕様記述言語と呼ぶ) で記述しなければならない．また，モデル検査ではソフトウェアが満たしてほしい性質を確認するために，性質を時間的な概念を持たせた論理式 (以下，時相論理式と呼ぶ) で記述することも必要になる．この時相論理式は仕様記述言語に対応した形で記述する必要がある．こうした作業は仕様記述言語，時相論理式，それぞれの文法をよく理解し，ソフトウェア検証に対応したテクニック的な記述を考える必要があり，ソフトウェア技術者にとって，大変な作業となる．その上，検証したい性質が複雑になると，時相論理式を記述することが非常に困難になる．

ソフトウェアの性質の確認方法には，いくつかの定石がある．それをパターンとして体系だてて提示することが，ソフトウェア技術者の支援に有効であると考える．本研究では，対象となる設計の構造とその構造で確認したい性質を合わせてパターン化する手法を提案する．また，検証対象のシステムを記述する仕様記述言語と検証したい性質を記述する時相論理式は密接に関連しているので合わせて，記述手法を支援する必要がある．なお，本研究ではモデル検査ツールとして SPIN を対象にする．

本研究は UML をモデル検査で検証する際の以下の２つの問題点を扱う．

- UML 上の性質を時相論理式に変換するのは大変である．

- UML から仕様記述言語への変換は自明ではない.

1 つ目の問題点である，時相論理式で表現することが困難であるという問題に対しては、よく使われる時相論理式をパターンとして提示するという提案がなされている。しかし，この従来のパターンは時相論理式のみのパターンで，非常に汎用的で一般的である．これでは，UML 上の性質を記述する支援としては不十分である．そこで，UML 上の性質を使って具体的な構造を時相論理式と合わせて考えることによって，具体的なソフトウェアの性質をパターン化し，それを SPIN に適用することを 1 つ目の目的とする．

また，もう 1 つの問題点である，UML の仕様記述言語への変換に関する問題に対しては，時相論理式との密接な関係があるので，それを考慮した本研究の対象である PROMELA への変換規則を提案する．具体的には、メッセージの送受信などといった UML 特有の概念を、LTL 上で表現しやすいように、変換規則を工夫している。これを本研究の 2 つ目の目的とする．

本研究の特徴は UML で構造を持たせ，それに対して性質を定義し，LTL のパターン化を行った点にある．これにより，それぞれの UML 構造に関わる具体的な性質を検証するための LTL をパターン化することができる．また，UML のクラス図，ステートチャート図から PROMELA へ変換規則の提案も行った．これにより，UML から PROMELA への変換が手続き的に行えることができるようになる．

評価として，本研究で提案した UML の構造ごとに LTL をパターン化した検証パターンと UML から PROMELA への変換規則を使用して，企業から提供いただいた事例の設計モデルに適用し，実際に検証を行えることを確認できた．

本論文の構成は以下の通りである．2 章では，本研究の目的について述べ，3 章では形式的検証手法であるモデル検査技術とそのツールの概要について述べる．そして，4 章では本研究で提案した検証パターンと PROMELA への変換規則について述べる．5 章では事例の設計モデルに適用した評価を述べ，6 章では本研究のまとめと今後の課題，展望を述べる．