様式 C-19

科学研究費補助金研究成果報告書

平成２１年　５月２９日現在

研究種目：基盤研究(C)
研究期間：２００７～２００８
課題番号：19500035
研究課題名（和文）　モデル検査による設計モデル検証プロセスの研究

研究課題名（英文）　Research on Design Verification Process Using Model Checking

研究代表者
田原 康之（TAHARA YASUYUKI）
電気通信大学・大学院情報システム学研究科・准教授
研究者番号：30390602

研究成果の概要：近年、ソフトウェアは大規模化、複雑化が進んでいることから、高信頼でかつ安全なソフトウェア設計を実施するために、モデル検査技術が有望視されている。本研究では、開発者に分かりやすい設計と、モデル検査に必要な抽象的数学理論のギャップを縮めるために、既存技術である Template Semantics をベースとした、形式モデルの意味論を参照・変更可能な設計モデル検証プロセスを考案し、そのプロセスに基づく開発支援ツールのプロトタイプを開発した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,700,000	510,000	2,210,000
２００８年度	1,500,000	450,000	1,950,000
年度			
年度			
年度			
総　計	3,200,000	960,000	4,160,000

研究分野：総合領域
科研費の分科・細目：情報学・ソフトウェア
キーワード：計算機システム、情報システム、ソフトウェア開発効率化・安定化、ソフトウェア学、ソフトウェア検証

１．研究開始当初の背景

近年、ソフトウェアは大規模化、複雑化が進んでいることから、高信頼でかつ安全なソフトウェア設計を実施するために、モデル検査技術が有望視されている。しかし、モデル検査手法は、抽象的数学理論の理解が必要であるという問題があった。

そこで、設計モデルとして、最も普及しているソフトウェアモデリング言語である UML で記述したものを検証対象とすることにより、設計モデル記述の労力を軽減する、という方向の研究があるが、UML による設計と抽象理論とのギャップは依然として存在していた。

そこで本研究は、形式モデルの厳密さと、開発者が扱う設計モデルや要求仕様といった非形式的記述のあいまいさとのギャップが、このような真の難しさの要因の１つと考え、そのギャップを縮めるという、これまでにない方向で研究を進めるものである。

２．研究の目的

モデル検査手法による設計モデル検証プロセスにおいて、形式モデルの厳密さと、非形式的記述のあいまいさとのギャップを縮め、検証作業を容易にする技術を確立し、技術を適用するための支援ツールを開発する。上記のギャップの重要な原因の１つが、意味論の有無である。形式モデルは、意味論によって数学的対象にマッピングされるため、厳密に扱えるのに対し、非形式的記述はそうではない。そこで、開発者が、容易に意味論を理解し、また必要に応じて意味論をカスタマイズすることにより、結果的に形式モデルの扱いを容易に可能とする。詳しくは、形式モデルの記述、モデル検査ツールの出力の分析、および形式モデルや設計モデルへの反映といった作業の効率と正確さを向上させる。

３．研究の方法

本研究のアプローチの概略は次の通りである。まず、現状の設計モデル検証プロセスでは、意味論が既存の情報として固定的なものが与えられており、容易に変更できないため、次のような問題点がある。

(1)

非形式的記述の中に、使用している形式モデルでは容易に記述できない要素があった場合、開発者が自らの経験とノウハウにより、それらしい記述を行うことになる。しかし、実際には元の意図を正しく反映した記述が困難なことが多く、最悪の場合は別の形式モデルやモデル検査ツールに切り替える必要が生じる。

(2)

検証の結果として、振舞いモデルが性質記述を満たさない場合、反例が出力される。この場合に、意味論に問題があるため、修正した方がよいことも多い。しかし、意味論は変更できないため、設計モデルや振舞いモデルを不自然に修正しなければならず、不適切な設計モデルを作成してしまう場合がある。一方本研究では、図１のような検証プロセスを確立することにより、上記の問題点を解決する。

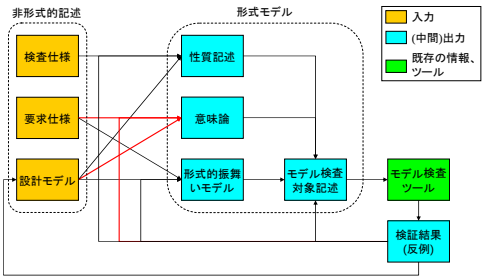

図１ 本研究で確立する検証プロセス

すなわち、従来のプロセスに対して、図 ３において赤い矢印で示した、次の２種類のステップを新たに追加している。

(1)

要求仕様と設計モデルから、意味論を導出するステップ

(2)

検証結果として反例が出力された場合に、意味論の修正として反映するステップ

これらを実現するために、意味論を記述する枠組みを用意し、意味論の導出や修正を支援する技術とツールを構築する。

なお、上述の計画通りに研究が進まない場合は次のように対応する。まず、検証プロセス、およびその要素技術である意味論の導出や修正を支援する技術の確立が予定通りに進まない場合は、検証プロセスのうち一部のステップにのみ注力することにより、部分的にでも検証プロセスの確立を進める。

また、ツールの開発が予定通りに進まない場合は、やはり一部の機能の実装に注力することにより、部分的にでも検証プロセスの支援を可能とする。

４．研究成果

平成 19 年度は、(1)既存技術である Template Semantics をベースとした、形式モデルの意味論を参照・変更する枠組みの理論を確立した。具体的には、開発者が非形式的記述による要求仕様と設計モデルに対し、形式モデルがそれらの意図を正確に反映するように、Template Parameter と呼ばれるデータを策定することにより、意味論を変更する方法を確立した。

また、(2)その枠組みを適用した検証プロセスを支援するツールのプロトタイプ第1版として、Template Semantics に基づく枠組みに基づき、形式的振舞いモデルと性質記述から、モデル検査対象記述を自動生成するツールの仮想設計を行い、(3)ネットワーク家電の例題に適用してその有用性を評価した。
平成 20 年度は、(1)平成 19 年度に確立した検証プロセスを、実際の検証作業に適用するために必要な、詳細なノウハウを抽出し、検証プロセスに沿って整理することにより、開発者がノウハウを容易に利用可能とした。たとえば、ネットワーク家電の制御ソフトウェアにおける、タイムアウト処理の厳密な振舞いの定義について、単純なモデルから始めて、検証・修正の繰り返しを行い、より正確な定義に近づける、といったノウハウを確立した。
また、(2)検証プロセスを支援するツールの第2版として、意味論、形式モデル、および非形式的記述の記述・デバッグ支援ツールの仮想設計を行い、(3)ツールをネットワーク家電の例題に適用し、その有用性を評価した。
本研究で仮想設計を行ったツールを実装・公開し、多くの開発者の試用・評価を通じて、モデル検査技術の普及を促進し、その結果高信頼なソフトウェアの開発効率向上に寄与することが期待できる。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　０件）

〔学会発表〕（計　２件）
① Yasuyuki Tahara, Nobukazu Yoshioka, Kenji Taguchi, Toshiaki Aoki, Shinichi Honiden, “Education Course of Practical Model Checking”, First International Workshop on Formal Methods Education and Training, 2008 年 10 月 28 日, 北九州市（日本）

② 田原 康之, 吉岡 信和, 田口 研治, 海谷 治彦, 本位田 真一、「開発プロセスにおけるセキュリティ関心事の分離に向けて」、ウインターワークショップ 2008 ・イン・道後、2008 年 1 月 24 日、松山市（日本）

〔図書〕（計　２件）

① 吉岡 信和、青木 利晃、田原 康之（著）、萩谷 昌己（監修）、本位田 真一（シリーズ監修）、近代科学社、「SPIN による設計モデル検証」、2008 年、pp. 165-186

② 磯部 祥尚、粂野 文洋、櫻庭 健年、田口 研治、田原 康之（著）、田中 譲（監修）、本位田 真一（シリーズ監修）、近代科学社、「ソフトウェア科学基礎」、2008 年、pp. 125-144、267-296

〔産業財産権〕
○出願状況（計　０件）

○取得状況（計　０件）

〔その他〕

６．研究組織

(1)研究代表者

田原 康之
電気通信大学・
大学院情報システム学研究科・ 准教授
研究者番号：30390602

(2)研究分担者

本位田 真一
国立情報学研究所・
アーキテクチャ科学研究系・教授
研究者番号：70332153

(3)連携研究者