様式 C-19

科学研究費補助金研究成果報告書

平成　21 年　4 月　23 日現在

研究種目：若手研究（B）
研究期間：2006～2008
課題番号：　18700024
研究課題名（和文）　モジュラーな項書き換えシステムに基づく仕様検証システムの開発

研究課題名（英文）　On a formal verification system based on modular term rewriting

研究代表者
中村 正樹（NAKAMURA MASAKI）
金沢大学・電子情報学系・助教
研究者番号：40345658

研究成果の概要：本研究では，モジュラーな項書換えシステムに基づく仕様検証システムの開発を行った．これにより，特に仕様作成，実行，検証時におけるデータ仕様の扱いが容易となり，形式仕様言語の幅広い利用を促す研究成果が得られた．また，仕様から実装を得るためのツールの開発，異なる検証技術の融合技術，検証エンジンの基礎理論など，ソフトウェア開発工程全体を取り扱うことが可能な形式仕様言語の構築へとつながる研究成果が得られた．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	1,200,000	0	1,200,000
2007 年度	1,100,000	0	1,100,000
2008 年度	1,100,000	330,000	1,430,000
年度			
年度			
総　計	3,400,000	330,000	3,730,000

研究分野：ソフトウェア工学
科研費の分科・細目：情報学・ソフトウェア
キーワード：形式手法，検証システム，項書換えシステム，代数仕様，モジュールシステム，仕様変換，ソフトウェアテスト

１．研究開始当初の背景

ソフトウェア技術が大衆化してきた現在，ソフトウェアの安全性の確保はますますその重要性を増している．形式手法は，ソフトウェアの設計段階で形式的に仕様を記述，検証する手法であり，数学的に安全が保証された高品質なソフトウェアの開発に適している．形式手法を広く社会に浸透させることは安全な情報社会の実現に重要な要件の一つである．本研究で対象とする代数仕様による形式手法は，洗練された論理体系，記述スタイルに比べ，検証面においていくつか問題がある．検証のコアとなる推論エンジンがその基礎理論である項書き換えシステム(TRS)の数々の有用な理論と結びついておらず，また大規模な検証のためには複数の推論を適切に組み合わせた証明スコアが用いられるが，その正しさは検証者自身が証明する必要が

ある．

２．研究の目的

本研究の目的は，高い専門的知識を必要としない検証システムを提供することで，ソフトウェア開発者が容易に利用可能な代数仕様による形式手法を得ることである．具体的には代数仕様の洗練されたモジュールシステムを反映したTRSの理論の再構築とそれに基づくモジュラーな推論エンジンの開発，および，証明スコアを形式的に扱うための理論の構築とそれを基にした証明スコア記述のためのガイドラインの策定および支援ツールの開発を行う．

３．研究の方法

平成18年度は，当初の計画に基づき，モジュラーな項書き換えシステム（MTRS）の理論に基づいて形式仕様言語CafeOBJ上に実装した仕様検証システムのプロトタイプを用い，仕様の記述，実験を行った．実験を通して得られた知見は以下の通りである．プロトタイプの適用範囲と実際に作成される仕様の差異を明らかにし，実用的な適用範囲を持つようにMTRSの理論を拡張する必要があることがわかった．特にMTRSに基づく局所等価述語の実装に対して明らかにする必要がある．ただし適用範囲は，周辺分野の研究の進歩にしたがい日々変わっていくものであるため，本研究で提案する推論エンジンでは，適用条件の判定機能をモジュール化し，当面はすでにわかっている簡単な条件を採用することとした．採用する条件であっても十分に実用的であり，既存の多くの仕様に適用可能であることがわかっている．証明スコアの調査分析では，所属する研究室のメンバらとの打ち合わせを通し，既存の仕様例をもとに，システマティックな証明スコアの作成手法がまとまりつつある．これらの成果は，既存のCafeOBJ検証システムに対するものであるが，本研究課題で提案する検証システムにおいてもほとんどそのままの形で適用可能である．

平成19年度は，モジュラーな項書換システムの研究を引き続き行い，より簡明な理論の構築と実装に向けての検討を行った．またモジュラーな検証システムと他の検証システムとの協調的な検証技術の構築のための基礎研究として，項書換システムによる等式推論を基礎とする証明スコアによる手法以外の代数仕様の検証技術に関する研究を行った．

平成20年度は，代数仕様言語CafeOBJ上で実現したモジュラーな項書換えシステムに基づく検証システムの事例研究を通し，その有効性を確かめた．また構築した検証システムの発展のため，効率的な検証エンジン，種々の検証システムの融合，仕様から実装への変換技術などを支援する基礎理論，方法論，ツール開発などの研究を行った．

４．研究成果

平成18年度の研究成果を以下に示す．上記の局所等価述語の適用条件のひとつである項書き換えシステムの停止性に関して，仕様変換による停止性証明手法を提案した．振舞仕様の自動検証技術に関する研究成果は，本提案の検証システムにも将来的に役立つ技術である．本研究課題の核となる理論が雑誌論文として採録された．また本提案の検証システムを実際に用いた研究成果も得られた．

平成19年度の研究成果を以下に示す．モジュラーな項書換システムの理論は，マカオで開催された国際会議 The 4th International Colloquium on Theoretical Aspects of

Computing で発表し，計算機科学のレクチャーノート（LNCS シリーズ）に掲載された．書換理論，仕様記述，検証技術を含む計算機科学の理論的な側面からの最新の研究発表が多くなされ，本研究課題の今後の方向性を考える上で重要な機会となった．他の検証ツールとの協調に関する研究として，不動点の概念を用いた振舞仕様の不変性自動検証ツール Crème の研究開発を行った．今後は Crème で扱いやすい問題の分析を行い，どのようにモジュラーな検証エンジンに取り込むかを検討する．振舞仕様から書換仕様への変換手法の提案も行い，振舞仕様へのモデル検査技術の適用を可能とした．また検証エンジンの振舞の分析のための研究として，代数仕様のための停止性判定手法の提案を行った．代数仕様記述者が扱いやすい停止性判定手法の提案は，モジュラーな検証エンジンに適切な代数仕様の作成方法へとつながる重要な基礎研究である．

平成 20 年度の研究成果を以下に示す．等式仕様の実行エンジンの基礎理論：項書換えに基づく等式推論エンジンの基礎となる項のマッチング技術を提案した．項の簡約の効率化には不必要な書き換えをできるだけ避け，必要に応じて（オンデマンドに）書き換えを行う必要がある．本提案のオンデマンドマッチングは，システムに応じてユーザがマッチング順序を切り替え可能なこと，すべての書き換え規則を同時に比較すること，などの特徴を持ち，既存の関連技術ではうまく扱えないシステムを扱うことが可能となった．検証システムの融合技術：システムを抽象度の高い振る舞いのレベルで捉えて仕様を記述する振舞仕様からより具体的に捉える書換仕様への変換手法を提案した．振舞仕様では証明譜に基づく対話的な検証手法が行われ，書換仕様では網羅探索やモデル検査による全自動検索が行われる．振舞仕様を制限する形で具体的な書換仕様に変換することで，検証したい性質に対する反例の発見など検証の手助けを得ることが可能になった．形式仕様からの実装を支援するツール開発：記号計算による仕様の形式検証では，設計レベルの安全性を数学的に保証できたとしても，最終成果物となる実装の安全性は保証されない．実装レベルの安全性には，ソフトウェアテストの技術が有効である．本研究では，検証済みの形式仕様から実装（スケルトン）への自動変換およびテスト自動生成を行うツールを開発した．検証結果を利用することで，安全性を保証するためのテストケース群を系統的に得ることが可能となった．

今後は，モジュラー項書換えシステムに基づく検証システムを中心に，検証システムの融合，実装への自動変換，テスト自動生成，検証エンジンの効率化など，研究期間中に得られた種々の技術を統合し，実際のソフトウェア開発に適用可能な，要求，設計から実装，保守までを支援するソフトウェア開発のための統合形式言語の構築に向けた研究を行っていく．

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 8 件）

①. Masaki Nakamura, Takahiro Seino, Generating test cases for invariant properties from proof scores in the OTS/CafeOBJ method, IEICE TRANSACTIONS on Information and Systems, 査読有, Vol.E92-D,No.5, 2009, in press.

②. Masaki Nakamura, Kazuhiro Ogata, Kokichi Futatsugi, User-defined on-demand matching, IEICE TRANSACTIONS on Information and Systems, 査読有, Vol.E92-D, No.7, 2009, in press.

③. Masaki Nakamura, Weiqiang Kong, Kazuhiro Ogata, Kokichi Futatsugi, A specification translation from behavioral specifications to rewrite specifications, IEICE TRANSACTIONS on Information and Systems, 査読有, Vol.E91-D, No.5, 2008, pp.492-1503.

④. Masahiro Nakano, Kazuhiro Ogata, Masaki Nakamura, and Kokichi Futatsugi, Crème: An Automatic Invariant Prover Of Behavioral Specifications, International Journal of Software Engineering and Knowledge Engineering (IJSEKE), 査読有, Vol.17, No. 6, 2007, pp.783-804.

⑤. 中村正樹, 二木厚吉, 実行可能な代数仕様の停止性証明について, 情報科学技術レターズ, 査読有, Vol. 6, 2007, pp.27-30.

⑥. K. Kusakari, M. Nakamura and Y. Toyama, Elimination Transformations for Associative-Commutative Rewriting Systems, Journal of Automated Reasoning, 査読有, Vol. 37, No. 3, 2006, pp.205-229.

⑦. M. Nakamura, M. Watanabe and K. Futatsugi, A Behavioral Specification of Imperative Programming Languages, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 査読有,Vol.E89-A, No.6, 2006, pp.1558 - 1565.

⑧. 中村正樹, 二木厚吉, モジュラーな代数仕様言語のための項書き換えシステム, コンピュータソフトウェア, 査読有, Vol. 23, No. 3, 2006, pp.35-50.

〔学会発表〕(計 4 件)

①. 中村正樹, 清野貴博, OTS/CafeOBJ 法における証明譜からのテスト生成,ソフトウェアサイエンス研究会(SS), 2007 年 12 月 17 日, 松江

②. Masaki Nakamura and Kokichi Futatsugi, On equality predicates in algebraic specification languages, the 4th International Colloquium on Theoretical Aspects of Computing, 2007. Sep. 26th, Macau.

③. 中村正樹, 二木厚吉, 実行可能な代数仕様の停止性証明について,第 6 回情報科学技術フォーラム(FIT), 2007 年 9 月 7 日, 豊田

④. Masaki Nakamura, Weiqiang Kong, Kazuhiro Ogata, Kokichi Futatsugi, A complete specification transformation from OTS/CafeOBJ to OTS/Maude, ソフトウェアサイエンス研究会(SS), 2006 年 6 月 22 日, 岡山

６．研究組織

(1)研究代表者

中村 正樹（NAKAMURA MASAKI）
金沢大学・電子情報学系・助教
研究者番号：40345658