様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年 6 月 17 日現在

機関番号：23201
研究種目：若手研究(B)
研究期間：2010～2012
課題番号：22700027
研究課題名（和文）
モジュラー書換え理論に基づく代数型ソフトウェア開発言語の構築
研究課題名（英文）
On algebraic specification languages based on modular rewriting systems
研究代表者
中村　正樹（NAKAMURA MASAKI）
富山県立大学・工学部・講師
研究者番号：40345658

研究成果の概要（和文）：
モジュールシステムを備えた代数仕様言語に適した項書換えシステムによる仕様実行に関する基礎的研究を行い，モジュール構造に基づく効率的な停止性判定手法を提案した．停止性は，項書換えシステムの最も重要な性質の１つで，任意の実行の有限時間内の停止性を保証する．本手法を用いることで，大規模複雑な代数仕様に対して，効率的に停止性を示すことが可能となり，モジュラーな代数型言語の開発の重要な基礎を与えた．

研究成果の概要（英文）：
We studied about term rewriting systems to give an operational semantics of specification execution for algebraic specification languages with sophisticated module systems. Our main result is a termination proving methods based on module structures. Termination is one of the most important properties of term rewriting, which guarantees any specification execution terminates in finite time. By our results, we can prove termination of large and complex algebraic specifications with conditional equations efficiently.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1100	330	1430
2011 年度	900	270	1170
2012 年度	900	270	1170
年度			
年度			
総　計	2900	870	3770

研究分野：ソフトウェア
科研費の分科・細目：仕様記述・仕様検証
キーワード：項書換えシステム

１．研究開始当初の背景

セキュリティに関する国際規格 ISO/IEC 15408,機能安全に関する国際規格 ISO/IEC 61508 でソフトウェアの安全性を確保する技術として形式手法・形式的検証の適用が推奨されている．そのような社会情勢において，形式手法は徐々に社会に浸透してきているが,単なる仕様記述,テスト実行以上の,形式的検証まで踏み込んだ技術は未だ十分に社会に浸透していると言えない.このような問題を解決するため,これまで主に専門家のみが行えた形式的検証技術を,実際にソフトウェア開発を行う一般の開発者にも利用可能なように大衆化する必要がある．

形式手法では，形式仕様言語が中心的な役割を演じる．特に，本研究が対象とする代数仕様言語は，書換えによる実行を特徴とし，多くの検証技術・検証事例が報告されているが，ソフトウェア開発全体に適用した事例やそのための支援環境は少ない．

２．研究の目的

本研究の位置づけは，代数仕様に基づく形式的検証技術を含んだ実用的なソフトウェア開発環境を整備することであり，ソフトウェア開発において益々必要性が増す形式手法・形式的検証の大衆化を目指し，ソフトウェア開発工程の全体を一貫して取り扱うことが可能な言語を構築し，研究者ではない一般ソフトウェア開発者にも利用可能な支援ツールを開発することを目的とする．

応募者の専門分野である項書き換えシステムは，記号処理，プログラム変換，プログラミング言語の操作的意味などの基礎を与える汎用性の高い計算モデルであり，代数仕様およびプログラミング言語の操作的意味や仕様間の変換，仕様からの実装・テスト生成など，ソフトウェア開発全体を取り扱う言語の実行モデルを与えるのに妥当であると考えられる．

応募者が提案したモジュラー項書換えシステム（MTRS）は，モジュール構造をもった代数仕様言語に適切な操作的意味を与え，モジュールごとに個別の実行モデルを付与可能であり，他の検証ツールとの融合や基本ライブラリの扱いに適していることが，これまでの研究で分かっている．ここで代数仕様言語の基本ライブラリとは，基本データ型の仕様（シグネチャ）と実装の組を指す．このことから，MTRS 理論が仕様と実装の融合を取り扱うのに適していると考え，仕様から実装までをシームレスに取り扱う言語の開発を着想した．

３．研究の方法

大規模・複雑なシステムの仕様を，効率的に，かつ理解しやすい形で作成するのに適したモジュールシステムを備えた代数仕様言語（CafeOBJ, Maude など）の操作的意味を与える項書換えシステムに関する基礎研究を元に，モジュール構造に適したソフトウェア開発支援環境を構築する．

形式仕様言語を用いたソフトウェア開発における設計段階では，形式仕様言語に基づいたシステムの形式的な仕様記述を行うが，実行可能性を特徴とする代数仕様言語においては，仕様の意味するモデルを考慮するだけでなく，仕様作成後に行う項書換えシステムに基づく仕様実行および形式的仕様検証も考慮しなくてはならない．仕様実行を考慮した仕様作成手法を，特にモジュールシステムに適した形で整理し，大規模・複雑なシステムの仕様作成を支援する．

また，本研究で主に研究対象としている代数仕様言語 CafeOBJ の振舞仕様では，仕様検証は項書換えエンジンを用いた対話的な証明手法に基づき行われる．一方で，代数仕様言語 Maude の書換仕様では，より具体的に仕様を記述する必要があるが，モデル検査器により，全自動網羅探索が可能である．振舞仕様から書換仕様へ仕様変換し，モデル検査により部分問題を自動証明する仕組みを与えることで，振舞仕様における問題の対話的証明の支援ツールを与える．

実装段階では，記号処理により数学的に正しさを確かめられた代数仕様をもとに，プログラミング言語で実装する．仕様検証で得られた数学的・体系的な証明結果をもとに，実装の正しさを確かめるためのソフトウェアテストのためのテスト集合を得る技術を与える．

４．研究成果

モジュールシステムを備えた代数仕様言語に適した項書換えシステムによる仕様実行に関する基礎的研究を行い，モジュール構造に基づく効率的な停止性判定手法を提案した[雑誌論文①,学会発表①,②,③].停止性は，項書換えシステムの最も重要な性質の１つで，任意の実行の有限時間内の停止性を保証する．発表論文[雑誌論文 1,学会発表 1,2]では，現在項書換えシステムの分野で最も強力な停止性証明手法である依存対法を，特に条件付き等式を含む代数仕様の実行モデルとなる条件付き項書換えシステムに対して適用し，(操作的) 停止性の十分条件を与えた．さらに，モジュール構造に基づく効果的な停止性証明手法である段階的的停止性証明手法を，同じく条件付き項書換えシステムに対して拡張し，実用的な代数仕様に適用可能な停止性手法手法を与えた．本手法を用いることで，大規模複雑な代数仕様に対して，効率的に停止性を示すことが可能となり，今後のモジュラーな代数型言語の開発の重要な基礎を与えた．発表論文[学会発表③]では，代数モデルに基づく停止性証明手法を提案した．停止性の研究は，停止性自動証明ツールが主要な研究分野となっているが,本研究では,停止性を持つ代数仕様の作成支援を目的とした停止性研究を行った．具体的には，作成しようとしている代数仕様が表す代数モデルに着目し,代数モデルを拡張する形で,モデルの存在が直接，代数仕様の停止性の証明となるような停止性のための代数仕様の生成手法を提案した．本成果により，代

数仕様作成者に理解しやすい停止性証明手法を与えることができ，仕様実行に適した仕様作成の枠組みを与えることが可能となった．

停止性と並ぶ項書換えシステムの重要な性質である十分完全性について，演算子の可簡約性に関する研究成果を発表した[雑誌論文③]．可簡約性は，仕様における演算子が矛盾無く定義されているかどうかを確かめる際に重要な概念であり，特に本研究では，振舞仕様などに現れる loose なデータ型と tight なデータ型が混在するような代数仕様を取り扱えるという特徴を持つ．具体的には,演算子の引数に対して,active か非 active を設定できる文脈依存書き換えと呼ばれる概念を元に，演算子の loose な引数を非 active，tight な引数を active と設定した文脈依存書き換え上での項の可簡約性により，振舞仕様における演算子の可簡約性を定式化した．一般に，停止性とパターンの基底インスタンス項の可簡約性を組み合わせることで代数仕様の十分完全性を示すことできるが，本成果により文脈依存書き換えとしての停止性と本提案の演算子可簡約性により，振舞仕様の十分完全性を示すことが可能となった．

仕様変換手法における研究成果では，代数仕様言語 Maude 上で，仕様変換による仕様検証支援ツールを開発した[雑誌論文②,学会発表⑥]．抽象的な代数仕様である CafeOBJ の振舞仕様で，書換エンジンを用いた対話的検証を支援するため，振舞仕様を具体的な仕様に変換（詳細化）し，それと等価な書換仕様を得る．書換仕様に対しては，Maude 言語のモデル検査器が適用可能であり，変換と組み合わせることで，元々の仕様の詳細化仕様に対する全自動網羅探索による検証が可能となる．特に，変換後の詳細化仕様に対するネガティブな検証結果が得られた場合，元々の振舞仕様においてもその検証したい性質が成り立たないことがわかるため，モデル検査器が示す反例を元に，仕様の見直す必要がある．また，詳細化仕様に対するモデル検査器によるポジティブな結果は，必ずしも元々の仕様上でその検証したい性質が成り立つことを保証しないが，具体的なひとつの事例に対して性質が成り立つことを足がかりに，対話的証明を組み立てる支援を得ることが可能である．

仕様からの実装技術では，代数仕様の証明結果からのテスト自動生成手法を提案した[学会発表④,⑤]．与えられた振舞仕様と検証したい性質に対して，場合分けや帰納法などの証明技術を用いて検証された結果には，実装上でその性質が成り立つかどうかをテストに確かめる際にも，同じ場合分けが有効であるという仮定のもと，検証結果から体系的にテストケース集合を生成する手法を提案した．

以上により，代数仕様に基づく仕様作成，検証，実装に対して，有用な成果を得ることができた．今後は，応募者の研究成果であるモジュラー項書換えシステムを基礎に，上記で示した仕様変換やテスト生成で得られた代数仕様を対象とした各種支援ツールの知見をもとに，これらの成果を有機的に結びつけ，設計から検証，実装までを支援する代数的ソフトウェア開発支援環境を構築する．具体的には，代数仕様をそのままの形で取り扱うのに適していることがわかった Maude 言語のリフレクション機能を用いて，振舞仕様を中心とした仕様検証，変換支援ツール，実装のためのテスト生成ツールを構築する．さらに，代数仕様言語 CafeOBJ でこれまで数多く発表されている実用的なシステムの仕様，および，応募者の研究室で行われているユビキタスセンサを対象としたセンサソフトウェアなどの事例に対して，構築した支援環境が有効に働くかどうかを確かめ，評価する．

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 3 件）

① Masaki Nakamura, Kazuhiro Ogata, and Kokichi Futatsugi, On Proving Operational Termination Incrementally with Modular Conditional Dependency Pairs, IAENG International Journal of Computer Science, Vol.40, Issue 2, pp117-123, 2013.（査読あり）
URL:
http://www.iaeng.org/IJCS/issues_v40/issue_2/index.html

② Min Zhang, Kazuhiro Ogata, Masaki Nakamura, Translation of State Machines from Equational Theories into Rewrite Theories with Tool Support, IEICE Transactions 94-D(5), pp.976-988, 2011.5
DOI:
http://dx.doi.org/10.1587/transinf.E94.D.976

③ Masaki Nakamura, Kazuhiro Ogata, Kokichi Futatsugi, Reducibility of operation symbols in term rewriting systems and its application to behavioral specifications, Journal

of Symbolic Computation, Vol.45, pp.551-573, 2010.
DOI: http://dx.doi.org/10.1016/j.jsc.2010.01.008

〔学会発表〕（計 6 件）（発表者に下線）

① Masaki Nakamura, Kazuhiro Ogata, Kokichi Futatsugi, Incremental Proofs of Operational Termination with Modular Conditional Dependency Pairs, Proceedings of the International MultiConference of Engineers and Computer Scientists 2013 Vol.I, IMECS 2013, pp.516-521, 2013.3, Hong Kong, China.

② Masaki Nakamura, Kazuhiro Ogata, Kokichi Futatsugi, A Hierarchical Approach to Operational Termination of Algebraic Specifications, Proceedings of the International Conference on Electronics, Information and Communication, ICEIC 2013, pp.144-145, 2013.2, Bali, Indonesia.

③ Masaki Nakamura, Kazuhiro Ogata, Kokichi Futatsugi, On Describing Terminating Algebraic Specifications Based on Their Models, Proceedings of the International MultiConference of Engineers and Computer Scientists 2012, IMECS 2012, pp.269-274, 2012.3, Hong Kong, China.

④ 清野貴博, 中村正樹, OTS/CafeOBJ 法に基づく並行システムの実装とテスト生成, 電子情報通信学会技術研究報告, 信学技報, vol.110, no.161, CST2010-33, pp.7-12, 2010.

⑤ 中村正樹, OTS/CafeOBJ 法における証明譜からのテスト生成, 第 20 回形式手法研究会, 専修大学神田校舎, 2010.11

⑥ Min Zhang, Kazuhiro Ogata and Masaki Nakamura, Specification Translation of State Machines from Equational Theories into Rewrite Theories, 12th International Conference on Formal Engineering Methods (ICFEM2010), Lecture Notes in Computer Science 6447, pp.678-693, Oct.2010, Shanghai, China.

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）
○取得状況（計 0 件）

〔その他〕なし

６．研究組織
(1) 研究代表者
中村正樹（NAKAMURA MASAKI）
富山県立大学・工学部・講師
研究者番号：40345658