JAIST Repository
https://dspace.jaist.ac.jp/

Title	分散システムを計算の対象とする分散アルゴリズムのモデル検査に関する研究
Author(s)	緒方，和博
Citation	科学研究費助成事業研究成果報告書: 1-4
Issue Date	2017-06-02
Type	Research Paper
Text version	publisher
URL	http://hdl.handle.net/10119/14331
Rights	
Description	挑戦的萌芽研究，研究期間：2014～2016，課題番号：26540024，研究者番号：30272991，研究分野：計算機科学、ソフトウェア工学、形式手法

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　　２　日現在

機関番号：　１３３０２
研究種目：　挑戦的萌芽研究
研究期間：　2014～2016
課題番号：　２６５４００２４

研究課題名（和文）分散システムを計算の対象とする分散アルゴリズムのモデル検査に関する研究

研究課題名（英文）A study on model checking of distributed algorithms whose computational targets are distributed systems

研究代表者

緒方　和博（OGATA, KAZUHIRO）

北陸先端科学技術大学院大学・先端科学技術研究科・教授

研究者番号：３０２７２９９１

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：分散スナップショットアルゴリズム（DSA）を書換え論理に基づく計算機言語Maudeのメタプログラム（MP）として記述する方法と分散スナップショット到達可能性（DSR）を直接モデル検査する方法を考案し、実験により有効性を確認した。従来法では、分散システム（DS）ごとにDSAも含め毎回記述する必要があったのに対し、提案方法では、MPを１回記述しさえすれば、DSのみの記述で十分であるという利点がある。また、DSRを直接モデル検査可能になったため、より高速にモデル検査可能になり、性質を満たさない場合反例を提示できるようにもなった。提案方法は、DSを計算の対象とする分散アルゴリズムに適用可能である。

研究成果の概要（英文）：We came up with how to specify a distributed snapshot algorithm (DSA) as a meta-program (MP) in Maude, a computer language based on rewriting logic, and how to directly model check the distributed snapshot reachability (DSR) property, and confirmed the usefulness by conducting several case studies. An existing approach makes it necessary to specify a DSA for each distributed system (DS), while the proposed approach does not. It suffices to specify DSA once as an MP and specify each DS only as the DS is taken into account. Since the DSR property can be directly model checked, the proposed approach performs model checking faster than the existing approach and generates a counterexample when the property is not satisfied. The proposed approach can also be applied to distributed algorithms whose computational targets are DSs.

研究分野：　計算機科学、ソフトウェア工学、形式手法

キーワード：　分散スナップショット　メタプログラム　モデル検査　Maude

１．研究開始当初の背景

モデル検査技術ならびにコンピュータの高速化等が相まって、分散システムを含む様々なシステムへのモデル検査の適用が盛んに行われていたが、分散スナップショットへアルゴリズムへの適用はほとんど見られなかった。主な理由は、分散スナップショットは、スナップショットを取る対象である分散システムに重ね合わせて使用されるために他のシステムとは異なる方法で形式化・仕様記述をする必要があることと満たすべき性質を既存の時相論理で記述することが容易ではないことであると思われた。スナップショットを取り始める状態を s0、スナップショットを取り終える状態を s1、スナップショットを s*とする。満たすべき性質は、スナップショットを取り終えたときにはいつでも s*は s0 から到達可能であり、s1 は s*から到達可能である、というものである。この性質を分散スナップショット到達性と呼ぶことにする。

既存研究に、分散スナップショットアルゴリズムを分散システムに重ね合わせて得られるシステムを書換え論理に基づく計算機言語 Maude で技術する方法ならびに Maude のサーチ機能を２回用いる事でこのシステムが分散スナップショット到達性を満たすことを示すモデル検査の方法について提案しているものがあった。この方法では、分散システムごとに分散スナップショットアルゴリズムも毎回記述し直す必要があること、モデル検査に Maude のサーチ機能を２回用いる必要があること、性質を満たさない場合の反例を提示できないこととといった改善すべき個所があった。

２．研究の目的

具体的には上述した既存研究の改善すべき個所の改善方法を提案することである。分散スナップショットアルゴリズムは、分散システムを計算の対象とする分散アルゴリズムである。高信頼の分散システムの構築には、分散スナップショットアルゴリズムに加え、コンセンサスアルゴリズム、リーダエレクションアルゴリズム、等々の分散システムを計算の対象とする分散アルゴリズムをいくつも用いる必要がある。分散スナップショットアルゴリズムを具体例として取り上げ、分散システムを計算の対象とする分散アルゴリズムの効果的な形式化・仕様記述・モデル検査の方法を提案することである。更に、これらの提案方法が、分散スナップショット以外の「分散システムを計算の対象とする分散アルゴリズム」（たとえば、コンセンサスアルゴリズムやリーダエレクションアルゴリズム）にも適用できる程度に一般化されていることも目的とする。

３．研究の方法

分散システム等は、状態機械と呼ばれる数学モデルで形式化する。状態機械 M = <S,I,T> は、初期状態の集合 I を部分集合として含む状態の集合 S と状態間の２項関係 T ⊆ S×S から構成される。要素(s,s') ∈ T を状態遷移と呼ぶ。２つの状態 s0 と sn に対し、各 i に対し(si,s(i+1)) ∈ T を満たす状態列 s0, s1, …, sn が存在するとき sn は s0 から到達可能であるという。分散スナップショットを取る機能を分散システムに重ね合わせて得られる分散システムも状態機械として形式化できることがわかっている。

状態機械の記述は書換え論理に基づく計算機言語 Maude を用いる。Maude は、Joseph A. Goguen 等により設計・開発された代数仕様言語 OBJ3 の流れをくむ。メタプログラムを記述するための機能、モデル検査を行うための機能を備え、本研究遂行のために適している。

分散スナップショットの仕様記述であるメタプログラムは、分散システムを形式化する状態機械の仕様を入力として取り、分散スナップショットを取る機能を分散システムに重ね合わせて得られる分散システムを形式化する状態機械の仕様を出力とするものである。

４．研究成果

既存研究を精査することで、分散スナップショット到達性は２つの状態機械に依存していることがわかった。１つは対象である分散システムの形式化である状態機械 M_{S}で、もう１つは分散スナップショットアルゴリズムを状態機械に重ね合わせることで得られるシステムの形式化である状態機械 M_{CL}である。分散スナップショット到達性は、「M_{CL}においてスナップショットを取り終えたときにはいつでも、s*は M_{S}において s0 から到達可能で、s1 は M_{S}において s*から到達可能である」、と記述されることが分かった[6]。既存研究でのモデル検査では２つの状態機械を用いずに M_{CL}のみを用いていた。しかし、M_{S}における到達可能性は M_{CL}においても保存されることから、既存のモデル検査方法でも分散スナップショット到達性をモデル検査できていることが確認できた[1]。

分散スナップショットアルゴリズムは、分散システムを入力として取り、分散スナップショットを取る機能を分散システムに重ね合わせた別の分散システムを出力するものとみなすことができる。このようなものはメタプログラムとして記述可能である。そこで、分散システムの形式化である状態機械 M_{S}の Maude による記述（仕様書）を入力として受け取り、分散スナップショットをとる機能を M_{S}に重ね合わせることにより作成される別の状態機械 M_{CL}を生成する Maude のメ

タプログラムを作成した[3]。この Maude のメタプログラムは、分散スナップショットアルゴリズムの仕様書とみなすことができる。分散スナップショットのみならず、分散システムを計算の対象とする分散アルゴリズムは Maude のメタプログラムとして仕様記述できることを示している。加えて、２つの状態機械 M_{S}と M_{CL}に依存する分散スナップショット到達可能性を直接モデル検査する方法を考案した[3]。メタプログラムでは、M_{S}と M_{CL}を自由に参照可能であるためにこのことが可能になった。この方法でのモデル検査は、Maude のサーチ機能を１回だけ用いれば十分であるという利点もある。このため、いつかの例題に対するモデル検査の実験から、既存のモデル検査の方法と比べより高速にモデル検査できることがわかった[3]。更に、新たに考案したモデル検査方法では、分散スナップショット到達可能性を満たさない場合、反例を提示することもできる[4]。

これまでに数々のメタプログラムが Maude で開発されてきたが、分散スナップショットアルゴリズム等の分散システムを計算の対象とする分散アルゴリズムの仕様として開発されたのは本研究が初めてである。メタプログラムは主にツールの開発に使われてきたが、本研究は、分散アルゴリズムの仕様記述やモデル検査にも利用できることを実証した。

上述したとおり、既存研究の改善すべき個所を改善することができた。本研究では、分散スナップショットアルゴリズムを具体例として用いたが、研究成果は、コンセンサスアルゴリズム、リーダエレクションアルゴリズム、等々の分散システムを計算の対象とする分散アルゴリズムの形式化・仕様記述・モデル検査にも適用可能である。

関連研究として、時間ならびに資源にセンシティブなビジネスプロセスとモーバイルロボットアルゴリズムの形式化・仕様記述・モデル検査に関する研究も行った[2,4,5]。いずれも分散システムのモデル検査に関する研究である。モーバイルロボットアルゴリズムの形式化・仕様記述・モデル検査に関する研究では、Maude を用いた。

５．主な発表論文等
（研究代表者は下線）

〔雑誌論文〕（計５件）

(1) Ha Thi Thu Doan, Francois Bonnet, Kazuhiro Ogata: Specifying a Distributed Snapshot Algorithm as a Meta-program and Model Checking it as Meta-level, Proc. of the 37th IEEE International Conference on Distributed Computing and Systems (ICDCS 2017), IEEE, 2017. (to appear) 査読有

(2) Kazuhiro Ogata, Thapana Chaimanont, Min Zhang: Formal Modeling and Analysis of Time- and Resource-sensitive Simple Business Processes, Journal of Information Security and Applications (JISA), 31: 23-40, Elsevier, 2016. 査読有

(3) Ha Thi Thu Doan, Francois Bonnet, Kazuhiro Ogata: Model Checking of a Mobile Robots Perpetual Exploration Algorithm, Prof. of 7th International Workshop on SOFL+MSVL (7th SOFL+MSVL), LNCS 10189, Springer, pp.201-219, 2016. 査読有

(4) Ha Thi Thu Doan, Wenjie Zhang, Kazuhiro Ogata, Min Zhang: Model Checking Chandy-Lamport Distributed Snapshot Algorithm Revisited, Proc. of the Second International Symposium on Dependable Computing and Internet of Things (DCIT 2015), IEEE, pp.30-39, 2015. 査読有

(5) Kazuhiro Ogata, Thapana Chaimanont, Min Zhang: Formal Modeling and Analysis of Time- and Resource-sensitive Simple Business Processes, Proc. of the Second International Symposium on Dependable Computing and Internet of Things (DCIT 2015), IEEE, pp.1-10, 2015. 査読有

〔学会発表〕（計１件）

(1) Wenjie Zhang, Kazuhiro Ogata, Min Zhang: A Consideration on How to Model Check Distributed Snapshot Reachability Property, 信学技報 114: 49-54, 2015. 査読無. 会場：プランナールみささ（鳥取県東伯郡三朝町）. 発表年月日：2015 年 1 月 26 日(月)

〔図書〕（計０件）

〔産業財産権〕

○出願状況（計０件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計０件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：

取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
緒方　和博（OGATA KAZUHIRO）
北陸先端科学技術大学院大学
・先端科学技術研究科・教授
研究者番号：30272991