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

令和　５ 年　 ４ 月 １４ 日現在

機関番号：１３３０２
研究種目：基盤研究(B)（一般）
研究期間：2019～2022
課題番号：１９Ｈ０４０８２

研究課題名（和文）線形時相論理モデル検査の分割統治による並列化

研究課題名（英文）A divide and conquer approach to parallelization of LTL model checking

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）　　12,900,000円

研究成果の概要（和文）：各々の初期状態から作成される無限状態木を複数の層に分割し、複数の部分状態空間を生成し、各々の部分状態を個別にモデル検査することで、モデル検査における状態空間爆発問題を緩和した。複数の部分状態空間を並列にモデル検査することで、モデル検査の実行性能を改善した。leads-to性などの線形時相論理で記述可能な重要な性質のいくつかのクラスを扱うことができる。各々の性質のクラスごとに、逐次版と並列版の支援ツールを開発した。それらの支援ツールを用いた事例研究により提案技術と支援ツールの有効性を確認した。

研究成果の学術的意義や社会的意義
ソフトウェアは我々の生活に深く入り込んでいる。大変便利であるが、複雑であればあるほど潜在的不具合が存在する可能性は大きい。顕在化すると、財政的損失ばかりでなく人命にも危険が及ぶ可能性すらある。このため、潜在的不具合は可能な限り取り除いたほうが良い。そのための有望な技術にモデル検査がある。しかし、ソフトウェア産業界において日常業務での使用に耐えうるようにするには解決すべき課題がある。状態空間爆発の緩和と実行速度の改善だ。状態空間を複数の空間に分割することで状態空間爆発を緩和し、複数の部分状態空間を並列にモデル検査することで実行速度を改善した。ソフトウェア産業界での実用化に向けて前進できた。

研究成果の概要（英文）：By splitting an infinite state tree constructed from each initial state into multiple layers and tackling each sub-state space, the state space explosion in model checking can be alleviated. By handling multiple sub-state spaces simultaneously, the model checking running performance can be improved. Several important classes of linear temporal logic (LTL) properties, such as leads-to properties, can be dealt with. We built sequential and parallel versions of a support tool for each property class and conduct cases studies with such tools, demonstrating the usefulness of the techniques proposed and the support tools.

研究分野：計算機科学

キーワード：モデル検査　分割統治　並列化　leads-to性　eventual性　条件付安定性　until性　until安定性

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

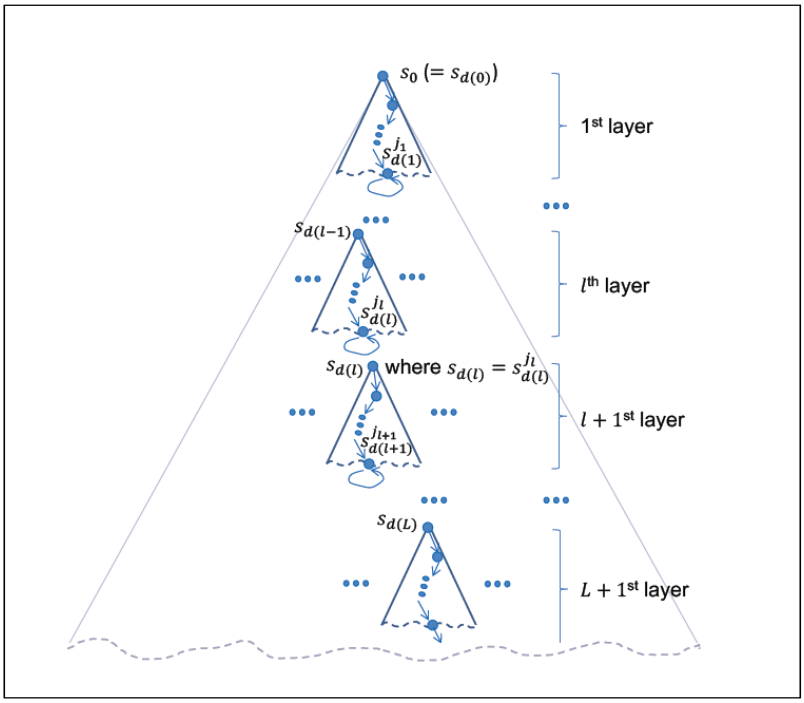
モデル検査は、システムの正しさ（システムが所望の性質を満たすこと）を確認する有望な技術である。ハードウェア産業界では日常業務で使われている。ソフトウェア産業界でも日常業務で使われるようにするには解決すべき問題が残っている。もっとも大きな問題のひとつは状態空間爆発である。探索空間が大きくなり過ぎるため、時間が掛かり過ぎたり、メモリに収まりきれなくなりモデル検査不能になったりする。実行性能の改善も実用化には不可欠である。Dijkstra のバイナリセマフォの抽象化版（Qlock）が leads-to 性で記述可能な非排斥性と呼ばれる性質（あるプロセスが際どい領域に入りたい場合、有限時間内に必ず入ることができること）をモデル検査すると、１０個のプロセスが Qlock に参加していれば、Spin では状態空間爆発のため状態空間がメモリに収まりきれなくなりモデル検査不能になり、Maude のモデル検査器では３７日以上の時間を要した。

２．研究の目的

モデル検査における状態空間爆発の緩和並びにモデル検査の実行性能改善である。

３．研究の方法

各初期状態から構成される無限状態木を複数の層に分割し、複数の部分状態空間を生成し、部分空間ごとにモデル検査をすることで状態空間爆発を緩和し、複数の部分空間を並列に処理することで実行性能を改善する（図参照）。線形時相論理で記述できる重要な性質の複数のクラスを扱うことを可能とする。具体的には、leads-to 性、eventual 性、条件付安定性、until 性、until 安定性である。これらの５つのクラスに対し、上述した方法でモデル検査する方法を考案し、提案方法の正しさを証明し、証明に基づくアルゴリズムを提案する。最初の３つのクラスに対し、逐次版と並列版の支援ツールを Maude で作成した。leads-to 性はもっともよく利用される性質のクラスであることが知られている。あることが起これば、別のあることが有限時間内に必ず起こる、といったことを記述できる。eventual 性は停止性などを記述できる。条件付安定性は、分散システムの分野で自己収束アルゴリズムと呼ばれる耐故障性を有すシステムの満たすべき生成を記述できる。



提案方法では、部分空間のモデル検査のときにある性質に対し、すべての反例を探す必要がある。Maude のモデル検査器は一度に１つの反例しか探すことができず実行性能面でのボトルネックになっていた。このため、グラフの強連結要素を効率良く探すことのできる Tarjan アルゴリズムをベースにすべての反例を一度に探すことのできるモデル検査器を、Maude のモデル検査器で使われているソフトウェアコンポネントを再利用することで実装し、支援ツールで使うことにした。

提案方法のモデル検査の実行性能は、無限状態木の分割方法（レイヤーコンフィグレーション）に大きく依存する。そこで、良いレイヤーコンフィグレーションをユーザが探すことを支援するツールを実装した。

４．研究成果

Spin では状態空間爆発のため状態空間がメモリに収まりきれなくなりモデル検査不能になり、Maude のモデル検査器では３７日以上の時間を要した事例に対し、開発した支援ツールでは６時間程度でモデル検査終了することができた。既存の並列化モデル検査器 LTSmin を用いた場合、Spin と同様にモデル検査不能となった。他の事例を用いた実験においても提案方法と支援ツールの有効性をしめすことができた。

すべて事例をうまく扱えるわけではないことも分かった。状態空間内に対称性をたくさん有すシステムの場合、同じ状態が複数の部分空間に現れるため、状態空間の分割の効果が小さかったり、ネガティブな影響を受けたりすることも分かった。状態空間内に長いループがある場合、無限状態木の層分割では、すべての部分空間の大きさをオリジナルの状態空間の大きさに比べ十分に小さくできなく、提案方法の効果が得られなかった。今後の研究でこれらの点を改善していく予定である。

５．主な発表論文等

〔雑誌論文〕　計15件（うち査読付論文　15件／うち国際共著　2件／うちオープンアクセス　6件）

１．著者名 Minh Do Canh、Ogata Kazuhiro	４．巻 10
２．論文標題 Parallel Specification-Based Testing for Concurrent Programs	５．発行年 2022年
３．雑誌名 IEEE Access	６．最初と最後の頁 24955～24975
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2022.3155629	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Do Canh Minh、Phyo Yati、Riesco Adrian、Ogata Kazuhiro	４．巻 0
２．論文標題 A Parallel Stratified Model Checking Technique/Tool for Leads-to Properties	５．発行年 2021年
３．雑誌名 7th International Symposium on System and Software Reliability	６．最初と最後の頁 155～166
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISSSR53171.2021.00011	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Phyo Yati、Do Canh Minh、Ogata Kazuhiro	４．巻 0
２．論文標題 A Divide & Conquer Approach to Conditional Stable Model Checking	５．発行年 2021年
３．雑誌名 18th International Colloquium on Theoretical Aspects of Computing	６．最初と最後の頁 105～111
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-85315-0_7	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Phyo Yati、Do Canh Minh、Ogata Kazuhiro	４．巻 0
２．論文標題 A support tool for the L + 1-layer divide & conquer approach to leads-to model checking	５．発行年 2021年
３．雑誌名 45th IEEE Computer Society Computers, Software, and Applications Conference	６．最初と最後の頁 854～863
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/COMPSAC51774.2021.00118	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Phyo Yati、Minh Do Canh、Ogata Kazuhiro	4．巻 -
2．論文標題 A Divide & Conquer Approach to Leads-to Model Checking	5．発行年 2021年
3．雑誌名 The Computer Journal	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1093/comjnl/bxaa183	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Aung Moe Nandi、Phyo Yati、Do Canh Minh、Ogata Kazuhiro	4．巻 9
2．論文標題 A Divide and Conquer Approach to Eventual Model Checking	5．発行年 2021年
3．雑誌名 Mathematics	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/math9040368	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Ogata Kazuhiro	4．巻 30
2．論文標題 A Generic Approach on How to Formally Specify and Model Check Path Finding Algorithms: Dijkstra, A* and LPA	5．発行年 2020年
3．雑誌名 International Journal of Software Engineering and Knowledge Engineering	6．最初と最後の頁 1481～1523
掲載論文のDOI（デジタルオブジェクト識別子） 10.1142/S0218194020400215	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Do Canh Minh、Ogata Kazuhiro	4．巻 -
2．論文標題 A divide & conquer approach to testing concurrent programs with JPF	5．発行年 2020年
3．雑誌名 27th Asia-Pacific Software Engineering Conference (27th APSEC)	6．最初と最後の頁 356～364
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/APSEC51365.2020.00044	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Do Canh Minh、Ogata Kazuhiro	4．巻 -
2．論文標題 Parallel stratified random testing for concurrent programs	5．発行年 2020年
3．雑誌名 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)	6．最初と最後の頁 79～86
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/QRS-C51114.2020.00024	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Phyo Yati、Do Canh Minh、Ogata Kazuhiro	4．巻 -
2．論文標題 Toward development of a tool supporting a 2-layer divide & conquer approach to leads-to model checking	5．発行年 2019年
3．雑誌名 Proc. of 2019 International Conference on Advanced Information Technologies	6．最初と最後の頁 250-255
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/AITC.2019.8920978	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Minh Do Canh、Ogata Kazuhiro	4．巻 -
2．論文標題 A Divide & Conquer Approach to Testing Concurrent Java Programs with JPF and Maude	5．発行年 2020年
3．雑誌名 Proc. of 9th International Workshop on SOFL+MSVL	6．最初と最後の頁 42～58
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-41418-4_4	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Aung Moe Nandi、Phyo Yati、Ogata Kazuhiro	4．巻 -
2．論文標題 Formal Specification and Model Checking of the Lim-Jeong-Park-Lee Autonomous Vehicle Intersection Control Protocol (S)	5．発行年 2019年
3．雑誌名 Proc. of 31st International Conference on Software Engineering and Knowledge Engineerin	6．最初と最後の頁 159-164
掲載論文のDOI（デジタルオブジェクト識別子） 10.18293/SEKE2019-021	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Do Canh Minh、Phyo Yati、Ogata Kazuhiro	4．巻 10
2．論文標題 Sequential and Parallel Tools for Model Checking Conditional Stable Properties in a Layered Way	5．発行年 2022年
3．雑誌名 IEEE Access	6．最初と最後の頁 133749～133765
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2022.3230844	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Do Canh Minh、Phyo Yati、Ogata Kazuhiro	4．巻 LNCS 13252
2．論文標題 A divide and conquer approach to until and until stable model checking	5．発行年 2022年
3．雑誌名 34th International Conference on Software Engineering & Knowledge Engineering (SEKE 2022)	6．最初と最後の頁 388～393
掲載論文のDOI（デジタルオブジェクト識別子） 10.18293/SEKE2022-058	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Minh Do Canh、Riesco Adrian、Escobar Santiago、Ogata Kazuhiro	4．巻 NA
2．論文標題 Parallel Maude-NPA for Cryptographic Protocol Analysis	5．発行年 2022年
3．雑誌名 14th International Workshop on Rewriting Logic and its Applications (WRLA 2022)	6．最初と最後の頁 253～273
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-12441-9_13	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計11件（うち招待講演　1件／うち国際学会　10件）

1．発表者名 Do Canh Minh
2．発表標題 A Parallel Stratified Model Checking Technique/Tool for Leads-to Properties
3．学会等名 7th International Symposium on System and Software Reliability（国際学会）
4．発表年 2021年

１．発表者名
Phyo Yati

２．発表標題
A Divide & Conquer Approach to Conditional Stable Model Checking

３．学会等名
18th International Colloquium on Theoretical Aspects of Computing（国際学会）

４．発表年
2021年

１．発表者名
Phyo Yati

２．発表標題
A support tool for the L + 1-layer divide & conquer approach to leads-to model checking

３．学会等名
45th IEEE Computer Society Computers, Software, and Applications Conference（国際学会）

４．発表年
2021年

１．発表者名
Do Canh Minh

２．発表標題
A divide & conquer approach to testing concurrent programs with JPF

３．学会等名
27th Asia-Pacific Software Engineering Conference (27th APSEC)（国際学会）

４．発表年
2020年

１．発表者名
Do Canh Minh

２．発表標題
Parallel stratified random testingfor concurrent programs

３．学会等名
IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)（国際学会）

４．発表年
2020年

１．発表者名
Kazuhiro Ogata

２．発表標題
A stratified way to mitigate the state space explosion in model checking

３．学会等名
The 12th IEEE International Conference on KNOWLEDGE AND SYSTEMS ENGINEERING (KSE 2020)（招待講演）（国際学会）

４．発表年
2020年

１．発表者名
Phyo Yati

２．発表標題
Toward development of a tool supporting a 2-layer divide & conquer approach to leads-to model checking

３．学会等名
2019 International Conference on Advanced Information Technologies（国際学会）

４．発表年
2019年

１．発表者名
Minh Do Canh

２．発表標題
A Divide & Conquer Approach to Testing Concurrent Java Programs with JPF and Maude

３．学会等名
9th International Workshop on SOFL+MSVL（国際学会）

４．発表年
2019年

１．発表者名
Phyo Yati

２．発表標題
Formal Specification and Model Checking of the Lim-Jeong-Park-Lee Autonomous Vehicle Intersection Control Protocol (S)

３．学会等名
31st International Conference on Software Engineering and Knowledge Engineerin（国際学会）

４．発表年
2019年

１．発表者名
Do Canh Minh

２．発表標題
A divide and conquer approach to until and until stable model checking

３．学会等名
34th International Conference on Software Engineering & Knowledge Engineering (SEKE 2022)（国際学会）

４．発表年
2022年

１．発表者名
Do Canh Minh

２．発表標題
Parallel Maude-NPA for Cryptographic Protocol Analysis

３．学会等名
14th International Workshop on Rewriting Logic and its Applications (WRLA 2022

４．発表年
2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	ど　かんみん (Do CanhMinh) (00981143)	北陸先端科学技術大学院大学・先端科学技術研究科・助教 (13302)	
研究協力者	りえすこ　あどりあん (Riesco Adrian)	マドリードコンプルテンセ大学・Facultad de Informatica・准教授	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
スペイン	Universidad Complutense de Madrid			