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　２ 年　 ７ 月 １３ 日現在

機関番号：１２６０８
研究種目：基盤研究(C)（一般）
研究期間：2016～2019
課題番号：１６Ｋ００００９３

研究課題名（和文）並行ソフトウェアの正確かつ高速な実行時検査

研究課題名（英文）Research on Efficient and Precise Runtime Checking of Concurrent Software

研究代表者
荒堀　喜貴（Arahori, Yoshitaka）

東京工業大学・情報理工学院・助教

研究者番号：５０６１３４６０

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本研究は、並行ソフトウェアを実行時に正確かつ高速に検査する方式の実現を目的とする。ソフトウェアの実行時検査とは、ソフトウェアの実行状態を観測して得られるデータからバグや脆弱性を検出する技術であり、ソフトウェアの信頼性やセキュリティの向上に役立つ。しかし，従来の実行時検査は並行ソフトウェアに対しバグや脆弱性を正確かつ高速に検査できないという問題点があった。本研究はこの問題を解決することを目指し、主な研究成果として（1）並行処理の複雑属性を正確に捕捉するメタデータ表現と（2）並行処理の複雑属性表現上での高効率な競合検査と（3）多様な並行処理モデルを対象とする正確かつ高効率な並行バグ検査を実現した。

研究成果の学術的意義や社会的意義
ソフトウェアの信頼性及びセキュリティの研究分野で有望な技術として実行時検査が活発に議論されている。その中で、本研究は並行処理の正確かつ高速な検査という重要な問題を部分的に解決する一連の技術を提案した。この提案は当該分野の他の研究と異なる特徴と新規性を有し学術的意義がある。計算機ハードウェアの並列化の進展に伴い、並行処理は今後益々普及する一方でその信頼性とセキュリティの確保は困難な課題である。本研究の成果は並行処理のバグ及び脆弱性の正確かつ高速な検査を可能にするため、当該の研究分野への技術的貢献と社会への実用的貢献を生む。

研究成果の概要（英文）：The goal of this research project is to design and implement efficient and precise runtime checking techniques for concurrent software. Runtime checking of software is a collection of techniques, which directly monitors the runtime behaviors of the target program for bugs or vulnerabilities, and is effective for achieving software reliability and security. However, existing runtime checking techniques are either imprecise or inefficient, when applied to concurrent software. In this research, we aim to address this problem and have achieved, as main contributions, (1) meta-data representation for precisely capturing complex attributes of concurrent processing, (2) efficient race-checking methods based on the precise meta-data representation, and (3) efficient and precise concurrency-bugs detectors for various domains including event-concurrency, distributed concurrency, as well as traditional local concurrency.

研究分野：プログラム解析

キーワード：並行処理　並行バグ　プログラム解析　動的解析　実行時検査

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

ソフトウェアの信頼性やセキュリティの研究分野ではこれまで、ソースコード検証やモデル検査など、不具合の完全なる検出を目指す手法が研究されてきた。これらの手法は、対象プログラムの構造から実行時に生じうる状態を全て調べあげ、全状態を対象にバグや脆弱性を網羅的に発見しようとする。しかし、近年の大規模かつ複雑なプログラムでは、考えられる状態の数が巨大であるため、全状態を検査することは現実的に不可能である。このため、検査対象の状態を減らす抽象化や簡約の技法が研究されているが、これらの技法は一般に検査の精度や手間とトレードオフの関係にあるため、大規模で複雑なプログラムを正確に効率良く検査することは未だ困難な課題である。

これに対し、実行時検査と呼ばれる手法は、対象プログラムに特定の入力を与えて実行し、実行状態を観測して得られるデータからバグや脆弱性を検出する。実行時検査は、実際に観測した状態に的を絞って検査を行う。このため、ソースコード検証やモデル検査に比べるとバグや脆弱性の検出漏れが起きやすいものの大規模なソフトウェアに対し誤検出の少ない正確な検査を効率良く実行できる。

検査の正確さと効率の良さは実用面での利益が大きいため、国内外の研究機関や企業で実行時検査に関する研究が進められている。これらの研究はプログラム解析の理論やシステムソフトウェア及び計算機アーキテクチャの要素技術に基づき優れた検査方式を提案している。

しかし、既存の代表的な実行時検査方式は、複数の処理が並行するソフトウェア（並行ソフトウェア）に対し十分な検査精度と効率を得るに至っていない。並列計算機が普及する一方で並行脆弱性や並行攻撃など並行処理のバグ（並行バグ）を突く新手の脅威が出現しており、これらに対する正確で高速な検査方式の確立は喫緊の課題である。

２．研究の目的

ソフトウェアの実行時検査とは、ソフトウェアの実行状態を観測して得られるデータからバグや脆弱性を検出する技術であり、ソフトウェアの信頼性やセキュリティの研究分野で活発に議論されている。しかし、従来の実行時検査は複数の処理が並行するソフトウェア（並行ソフトウェア）に対しバグや脆弱性を正確かつ高速に検査できないという問題を抱える。本研究はこの問題の解決を目的とする。具体的には、マルチスレッド処理やイベント処理や分散並行処理などの多様な形態の並行処理を対象に、並行処理の実行時の状態を正確に捕捉するメタデータ表現と、その表現上で並行バグや分散並行バグや非決定的性能バグや等価性違反などの様々な種類のバグの検査を効率的に実行するメタデータ処理方式を明らかにする。

３．研究の方法

並行ソフトウェアのバグ及び脆弱性を正確かつ高速に検出する実行時検査の確立という本研究の目的達成に向けて、研究期間中に以下の段階的実装と効果計測実験を行う。具体的には主に以下の方針で研究を進める。初年度はまず、並行処理の複雑属性を捕捉するメタデータ表現を設計する。次に、並行処理の複雑属性表現に基づく競合検査を実現し、この検査器を既知の競合を持つ並行ソフトウェアに適用し、従来の競合検査方式に対する精度向上を計測する。次年度は、この実装と実験の結果をふまえ、並行処理の複雑属性表現上で競合検査を並列化やサンプリング等に基づき効率的に実行するメタデータ処理方式を実現し、効率向上効果を計測する。次年度は、競合以外の並行バグ及び脆弱性としてイベント並行処理における等価性違反と分散並行処理における非決定的バグ等を扱えるよう検査器の検査方式を拡張する。得られた検査器のそれぞれについて検査精度・効率の向上効果を計測し、更なる最適化と限界の分析を加え成果をまとめる。

４．研究成果

主な研究成果を以下の 3 つのカテゴリに分けて説明する。

・並行処理の複雑属性を捕捉するメタデータ表現

複雑属性として共有データの共有範囲と所有権を追跡管理し、複数スレッドが共有するデータの共有範囲に絞って正確な競合解析を行う効率的な検査方式を設計・実装した。実験の結果から、HTTP クライアントや SMTP クライアントを含む中小規模の実用マルチスレッドプログラムを対象に、提案方式が従来手法に比べて誤検出を大幅に低減でき検査効率も有望であることが分かった。この成果の一部は国際会議 IEEE HASE 2019（1 件）で発表した。

・並行処理の複雑属性表現上での高効率な競合検査

複雑属性を持つメタデータの処理を記録と検査の二つのフェーズに分割し、各フェーズを個

別に並列化する方式を実現した。具体的には、記録フェーズで検査対象の各スレッドが各自のバッファにメタデータを記録し、検査フェーズにおいて共有データアクセスの範囲ごとに複数の検査スレッドが競合検査を並列実行する方式を設計した。更に、この競合検査の並列実行方式について。競合の並列検査の負荷分散も実現した。具体的には、検査対象領域ごとに負荷の偏りを正確かつ高速に計測し、効率的に分散させる方式を実現した。中小規模の実用マルチスレッドプログラム（機械学習ライブラリ）を対象にした実験の結果、提案する負荷分散方式が有効に機能することを確認した。この成果の一部は国内会議 IPSJ SIGSE 2018（1 件）および国際会議 IEEE SCAM 2018（1 件）で発表した。

・多様な並行処理モデルを対象とする正確かつ高効率な並行バグ検査

従来の単一ノード内でのマルチスレッド処理に加え、複数のノード上で稼働するマルチスレッド処理（分散並行処理）を対象に競合検査を正確かつ効率的に実行する方式として、ノード間通信の影響範囲内で競合の潜在的発生箇所を重点検査するサンプリング方式を検討し実現した。大規模分散並行システムを想定したシミュレーションにより、検査精度を維持した検査効率の向上効果を確認した。また、このサンプリングベースの分散並行バグ検査手法について、その評価を充実させる目的で大規模な分散並行システムにおける分散並行バグ検査器の性能シミュレータの検討とプロトタイプ実装を進めた。これらの成果の一部は国内会議 IPSJ SIGSE 2018（1 件）および JSSST PPL 2019（1 件）で発表した。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計17件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 冨永江奈，荒堀喜貴，権藤克彦
２．発表標題 イベント駆動コードの差分解析を可能にするパス探査経験則
３．学会等名 第22回プログラミングおよびプログラミング言語ワークショップ（PPL2020）
４．発表年 2020年

１．発表者名 春日涼太郎，荒堀喜貴，権藤克彦
２．発表標題 Typestate解析を応用した静的解析による分散並行システムのバグの検出
３．学会等名 第22回プログラミングおよびプログラミング言語ワークショップ（PPL2020）
４．発表年 2020年

１．発表者名 和田智優，荒堀喜貴，権藤克彦
２．発表標題 クラウドシステムの非決定的性能バグ検査器
３．学会等名 第12回データ工学と情報マネジメントに関するフォーラム （第18回日本データベース学会年次大会）
４．発表年 2020年

１．発表者名 星野シンジ，荒堀喜貴，権藤克彦
２．発表標題 並行バグの効率的な自動原因解析を可能にする静的解析
３．学会等名 第26回ソフトウェア工学の基礎ワークショップ（FOSE2019）
４．発表年 2019年

１．発表者名
和田智優，荒堀喜貴，権藤克彦

２．発表標題
ωCatch: クラウドシステムにおけるパフォーマンスバグの正確な自動検知に向けて

３．学会等名
第26回ソフトウェア工学の基礎ワークショップ（FOSE2019）

４．発表年
2019年

１．発表者名
石山泰地，荒堀喜貴，権藤克彦

２．発表標題
分散並行ファジング

３．学会等名
第26回ソフトウェア工学の基礎ワークショップ（FOSE2019）

４．発表年
2019年

１．発表者名
李兆亮，荒堀喜貴，権藤克彦

２．発表標題
強化学習に基づく並行バグ検知

３．学会等名
第26回ソフトウェア工学の基礎ワークショップ（FOSE2019）

４．発表年
2019年

１．発表者名
冨永江奈，荒堀喜貴，権藤克彦

２．発表標題
入力空間とイベント空間を探索するJavaScriptコードの等価性検証

３．学会等名
情報処理学会論文誌プログラミング（PRO）

４．発表年
2019年

１．発表者名
Ena Tominaga, Yoshitaka Arahori, Katsuhiko Gondow

２．発表標題
AwaitViz: A Visualizer of JavaScript's async/await Execution Order

３．学会等名
The 34th ACM/SIGAPP Symposium on Applied Computing（国際学会）

４．発表年
2019年

１．発表者名
Yoshitaka Arahori

２．発表標題
RangeLocker: Adaptive Range-Sensitive Lockset Analysis for Precise Dynamic Race Detection

３．学会等名
The 19th IEEE International Symposium on High Assurance Systems Engineering (HASE 2019)（国際学会）

４．発表年
2019年

１．発表者名
Yoshitaka Sakurai, Yoshitaka Arahori, Katsuhiko Gondow

２．発表標題
POI: Skew-Aware Parallel Race Detection

３．学会等名
The 18th IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM 2018)（国際学会）

４．発表年
2018年

１．発表者名
片平遥香，荒堀喜貴

２．発表標題
分散並行バグ動的検出の大規模性能シミュレータ

３．学会等名
第21回プログラミングおよびプログラミング言語ワークショップ（PPL2019）

４．発表年
2019年

１．発表者名
冨永江奈，荒堀喜貴，権藤克彦

２．発表標題
等価性検査のための入力×イベント空間の探査経験則の学習

３．学会等名
第21回プログラミングおよびプログラミング言語ワークショップ（PPL2019）

４．発表年
2019年

１．発表者名
冨永江奈，荒堀喜貴，権藤克彦

２．発表標題
実行順序に着目したasync/awaitの実行の可視化

３．学会等名
情報処理学会第198回ソフトウェア工学研究発表会

４．発表年
2018年

１．発表者名
高野健太，荒堀喜貴，権藤克彦

２．発表標題
イベント処理を考慮した正確かつ高速なデータフロー解析

３．学会等名
情報処理学会第198回ソフトウェア工学研究発表会

４．発表年
2018年

１．発表者名
櫻井義孝，荒堀喜貴，権藤克彦

２．発表標題
ハイブリッド競合検査の負荷分散を考慮した並列化

３．学会等名
情報処理学会第198回ソフトウェア工学研究発表会

４．発表年
2018年

１．発表者名 片平遥香，荒堀喜貴，権藤克彦
２．発表標題 サンプリングに基づく分散悪性競合のオンライン検出
３．学会等名 情報処理学会第198回ソフトウェア工学研究発表会
４．発表年 2018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