

永続メモリシステム固有のバグの高精度な超並列検出

Massively Parallel and Accurate Detection of Persistent Memory Bugs

荒堀喜貴

東京科学大学（申請時: 東京工業大学）

1. 研究目的

- ・背景: 永続メモリシステム固有のバグを対象とする既存の解析技術とその限界

永続メモリは計算機システムのレイテンシ削減と障害耐性の向上を実現する強力な手段となる一方で、これらの利点を実現するためのプログラミングは永続メモリ命令/API 固有の複雑な動作シナリオを正しく理解して記述する必要があるため、従来の揮発性メモリ上のプログラミングに比べ難易度が格段に高い。近年、永続メモリのプログラミングに固有のバグ（永続メモリバグ）が問題視され、永続メモリバグを対象とする解析の技術が国際的に活発に研究されている。しかし、永続メモリバグの発現機序は複雑であり、特に永続性と一貫性の記述不備に起因する微妙なシナリオを漏れなく誤りなく解析するコストは非常に高い。結果として、従来の技術は解析対象の永続メモリバグの種類を限定するか、解析結果に多量の漏れ/誤りを起こす制限を抱える。

- ・目的: 永続メモリバグの高精度かつ超高速な解析の実現

本研究の目的は、既存技術の制限事項を克服し、種類を極力限定せず多様な永続メモリバグを高精度かつ高速に解析する技術の開発である。この目的を実現するアプローチとして、既存研究による逐次的な解析技術と異なり、多様な永続メモリバグの複雑な発現シナリオを効率的に並列検査する技術を開発することを目指す。特に、永続メモリ処理に固有の非決定的な動作ないしデータフローを静的および動的に追跡するプログラム解析を CPU および GPU で並列実行する方式の開発を目指す。

2. 研究成果の内容

本研究では、永続メモリシステム固有の複雑なバグ、特にその非決定的な動作に起因する問題の高精度かつ高速な検出を目的とする。永続メモリにおけるバグは、データの永続性、一貫性、および操作の不可分性といった特性が複雑に絡み合うため、その発現機序の特定と再現が困難であり、従来技術は解析対象の永続メモリバグの種類が限定的であるか、解析精度が十分でなかった。これらの問題を克服するという本研究の課題に対し、今年度はまず、永続メモリアクセスにおける特有の事象（イベント）や実行状態遷移を正確に捉えるためのメタデータ表現の設計を行った。このメタデータは永続メモリプログラムの振舞いを静的（コンパイル時）または動的（実行時）に追跡する際の実行状態の特徴を表現するものであり、具体的には、個々の永続

メモリアクセス操作の属性（例：アクセス種別、対象メモリアドレス、実行スレッド）に加え、各々の永続メモリアクセス操作に至る文脈、複数の操作間に跨る永続性保証の有無、更新順序の依存関係、さらにはクラッシュ発生時の復旧可能性といった、永続メモリアクセス操作に固有の実行状態の遷移や履歴を正確に特徴づける。これにより、多様な永続メモリバグの根本原因となりうる微妙なデータフローや実行状態の不整合を静的データフロー解析および動的トレース検査の連携により高精度に追跡することを可能にした。一方、高精度な静的/動的解析に伴う解析コストの増加、特に大量のテスト入力に伴う大量の実行トレースの解析コスト増加に対処する手段として、今年度は特に実行トレース解析の工程を従来技術のように逐次的に行うのではなくマルチコア CPU でのデータ並列処理、さらには GPU アーキテクチャを活用した超並列処理によって高速に検査するアルゴリズムを設計した。この並列検査機構により、従来技術では時間的制約から解析が困難であった規模の永続メモリプログラムやファジング等のブルートフォース型のバグ検査技術との組み合わせによる長時間かつ大容量の実行トレースに対し、実用的な時間内でのバグ/脆弱性の検出を期待できる。

3. 学際共同利用プログラムが果たした役割と意義

本研究の遂行において学際共同利用プログラムは重要な役割を果たしている。特に、提案する永続メモリバグ検出技術の設計およびプロトタイプ実装において、本プログラムを通じて提供される永続メモリ（Intel Optane Persistent Memory）を搭載した実機環境の利用は不可欠である。永続メモリシステム固有のバグおよびその解析器は、その特性上、エミュレータ環境だけでは再現および有効性検証が難しいケースが多く存在する。本プログラムによる実機環境の提供は、我々が設計した静的/動的解析手法のプロトタイプ実装および評価実験を進める上で大きな助けとなっている。2024 年度内においては、開発した解析器プロトタイプを実機上で大規模永続メモリプログラムに適用する網羅的かつ定量的な評価実験までは完了していないが、本年度に設計した解析器のプロトタイプは 2025 年度以降の研究課題（継続）においても重要な基盤となる。本プログラムによる永続メモリシステム実機環境の提供がなければ、このような実践的なアプローチによる研究開発は困難であるため、本プログラムの果たす意義は非常に大きい。

4. 今後の展望

今年度の提案方式のプロトタイプ設計/実装を現実の大規模永続メモリプログラムに適用して有効性を計る評価実験を引き続き継続するとともに、次年度（以降）の研究課題（継続）における情報流解析技術との融合により、大規模実用永続メモリプログラムに対する信頼性・セキュリティ検査基盤の確立を目指す。

5. 成果発表

- (1) 学術論文: なし (2025 年度に予定 (成果の一部を論文誌に投稿中))
- (2) 学会発表: なし (2025 年度に予定)
- (3) その他

使用計算機	使用計算機に ○	配分リソース※		
		当初配分	移行*	追加配分
Cygnus				
Pegasus	○	3640		
Wisteria/BDEC-01				
	※配分リソースについてはノード時間積をご記入ください。 *バジェット移行を行った場合、「+2000」「-1000」のように記入			