氏　　名	Jingcheng Yuan
学位の種類	博士（情報科学）
学位記番号	博情第 583 号
学位授与年月日	令和 8 年 3 月 25 日
論文題目	Verification of Flash File System Crash Consistency Based on Model Checking
論文審査委員	青木 利晃　北陸先端科学技術大学院大学　教授
	田中 清史　同　教授
	冨田 尭　同　准教授
	鵜川 始陽　東京大学　准教授
	高野 祐輝　株式会社ティアフォー　プリンシパル

論文の内容の要旨

File systems are fundamental to computing, managing data on storage devices, yet they face the persistent challenge of maintaining crash consistency, ensuring data integrity after an unexpected system failure. Operations like file creation or modification require updating multiple, non-adjacent on-disk data structures, and a crash during this process can leave the file system in an inconsistent state, leading to data corruption or loss. While techniques such as journaling improve robustness, verifying crash consistency remains difficult due to system complexity and the vast number of potential failure scenarios. Existing testing methods, including black-box tools like CrashMonkey, suffer from limited coverage and efficiency, often missing subtle corner-case errors. Formal verification with model checking offers exhaustive exploration but has been hampered by state-space explosion and the impracticality of modeling full-stack file systems in languages such as Promela. This thesis introduces a comprehensive methodology and a practical tool, MC^3 (Model Checking for Crash Consistency), for the automated, exhaustive verification of file system crash consistency. Our approach employs a state space search that exhaustively explores file system states while checking correctness properties on-the-fly. To overcome state explosion, we developed two key innovations: an object-based workload generation algorithm that systematically produces all valid file system operations, and a novel directory tree isomorphism detection technique that encodes and eliminates redundant states, drastically reducing the search space. We first applied this methodology to block-based file systems (e.g., FAT, ext2), identified the root causes of consistency violations and the non-atomicity of multi-block metadata updates, and proposed a write-ordering mechanism to prevent critical errors. We then implemented MC^3 to verify file system models written in C/C++. Applying MC^3 to a model of the

Flash-Friendly File System (F2FS), a complex log-structured file system (LFS), revealed a previously unknown crash consistency bug where metadata rollback combined with block reuse during garbage collection causes silent file data loss, a vulnerability likely common to many LFS designs. Our evaluation shows that MC^3 significantly outperforms CrashMonkey in testing efficiency and coverage, enabling the discovery of deep design-level bugs on a standard desktop PC within a practical time frame, thereby providing a powerful and scalable verification framework to enhance the reliability of future storage systems.

Keywords: Model Checking, File System, Crash Consistency, SPIN, F2FS

論文審査の結果の要旨

本論文は，ファイルシステムのクラッシュ一貫性検証を対象として，モデル検査を用いた体系的な検証手法および検証フレームワークを提案するものである．近年，ストレージシステムの大規模化，高性能化に伴い，ファイルシステムの内部構造は高度に複雑化している．特にクラッシュ発生時には，データのみならずメタデータ更新の非原子的な振る舞いなどに起因して整合性違反が生じる可能性があり，その検出は極めて困難である．また，このような整合性違反はデータの損失につながる．IoT 機器が広く利用されている現状を考えると，喫緊に解決すべき問題である．一方，そのような検証はブラックボックステストに基づく手法が主流であるが，再現性，網羅性，テスト効率の観点で限界があった．

そこで，本研究では，これらの課題に対して，ファイルシステムの状態を観測し，それらの状態を網羅的に探索するモデル検査手法を用いて問題解決を図っている．この際，適切に状態を抽象化しなければ状態爆発問題に直面する．そこで，本研究では，状態の抽象化およびファイルシステムのモデル化手法を提案している．まず，既存のモデル検査ツールを用いたファイルシステム構成要素の検証可能性を示し，モデル検査がクラッシュ一貫性検証に有効であることを示している．次に，フルスタックのファイルシステムを対象とした検証を可能とするため，新たに MC3（Model Checking for Crash Consistency）フレームワークを提案している．MC3 では，C/C++によるモデル記述により実システムに近い構造を扱うことを可能とし，オブジェクトベースのワークロード生成，ディレクトリ構造の同型性に基づく状態削減などの技術を導入することにより，大規模状態空間に対する網羅的探索を実用的な計算資源で実現している．既存モデル検査手法および MC3 のそれぞれにおいて，ファイルシステムに特化した抽象化，状態表現，最適化手法を提案している．これらの提案により，現実的なファイルシステムに対する効率的なモデル検査が可能となっており，本論文における中核的提案であり，新規性および有効性を有する点である．

本論文では，提案手法を実システムに近いモデルを用いて評価している．ログ構造型ファイルシステムに対する検証を通じて，従来のブラックボックステストでは発見が困難であったクラッシュ一貫性に関する潜在的不具合を発見しており，モデル検査の有効性を実証的に示している．また，既存ツールとの比較を通じて，提案手法が高い探索効率と広い検証カバレッジを有することを示している．これらの結果は，モデル検査をファイルシステム設計段階に適用することの有用性を示すものであり，システムソフトウェアの信頼性向上に対する重要な知見を与えている．

以上，本論文は，ファイルシステムのクラッシュ一貫性検証について，モデル検査に基づく体系的手法および検証フレームワークを提案し，その有効性を実験的に示したものであり，学術的に貢献するところが大きい．よって博士（情報科学）の学位論文として十分価値あるものと認めた．