九州大学学術情報リポジトリ
Kyushu University Institutional Repository

Acceleration of Bounded Model Checking based on Satisfiability-Modulo-Theories for Embedded Software Designs

劉, 楽源

https://doi.org/10.15017/1470601

出版情報：九州大学, 2014, 博士（工学）, 課程博士
バージョン：
権利関係：全文ファイル公表済

KYUSHU UNIVERSITY

（別紙様式２）

氏　　名　：劉　楽源

論 文 名　：Acceleration of Bounded Model Checking based on
Satisfiability-Modulo-Theories for Embedded Software Designs
（組込みソフトウェア設計のためのSMT有限モデル検査の加速技術）

区　　分　：甲

論　文　内　容　の　要　旨

ソフトウェアは，我々の日常生活における必要不可欠なものとなっている．クルマ，原子炉，航空機の制御部，人工心臓ペースメーカーなどのシステムに多用されているセーフティクリティカルなソフトウェアは，社会的なセキュリティーの維持から我々の健康管理までに影響を及ぼす．それにより，我々の生活はこれらのシステムによって提供されているサービスにますます依存するようになった．上記のソフトウェアは，組込みソフトウェアと呼ばれているものである．組み込みソフトウェアの実行エラーは，通常致命的な場合もよくあり，その修正にも多大なコストがかかる．また，組込みソフトウェアはますます複雑化・高度化・並行化しているため，高信頼性を確保する技術の提案はチャレンジングな課題である．

組込みソフトウェアの信頼性を向上させるための形式検証技術の提案は，この論文のトピックである．特に，ソースコード自体ではなく，組み込みソフトウェアの設計の正しさの検証に本研究の焦点を置く．ソースコードと比べ，設計を検証する利点としては，ソフトウェア開発プロセスの早い段階で不具合が早期に発見でき，後戻りの修正コストも軽減できることである．

既存の様々な形式検証技術の中で，充足性モジュロ理論（Satisfiability Modulo Theories, SMT）に基づいた有限モデル検査（Bounded Model Checking, BMC）を本研究で採用する．明示的（Explicit）モデル検査とBDD（Binary Decision Diagram）に基づいたシンボリック（Symbolic）モデル検査を代表とする他の自動検査技術と比べ，BMCの方は悪名の高い状態空間爆発問題が起こりにくいという利点を持つ．組込みソフトウェア設計に関しては，日本の組込みソフトウェア業界で普及している階層化状態遷移表（Hierarchical State Transition Matrix, HSTM）モデリング言語で作成した設計が本研究の中心になる．

本研究の主な成果を下記にまとめる．（１）階層化状態遷移表で作成した組込みソフトウェア設計のBMC検査アルゴリズムを提案した．対象となる設計には，組込みソフトウェア設計でよく用いられる共通変数や非同期メッセージ送受信で通信する複数の並行プロセスから構成されている．（２）提案アルゴリズムは，大規模な設計に対する検査スピードが遅いため，BMC処理の加速技術を提案した．鍵となるアイディアは，明示的状態空間の探索技術を利活用し，設計の実行パスを記録しエンコードすることによって，BMCの論理式のサイズを縮小することである．その上，明示的に状態空間を探索する際に，Bounded Context Switch（BCS）といった状態空間の抽象技術を応用

し，設計の不具合を見つけるために不必要な実行パスを削除する．（３）検索する実行パスを分類するヒューリスティックな方法を提案し，さらに，マルチコアでそれぞれの分割された実行パスを並列に検証する手法を提案した．（４）前述の提案した技術を既存のモデル検査の形式検証ツール「Garakabu2」に追加実装した．その結果，「Garakabu2」本来の処理速度と米国SRI社が開発した最新式のSAL有限モデル検査器と比べて，本研究で遂行した加速技術を実装したものが，約１００倍速くなり，検証速度が大幅に改善されたことを実証した，

本論文は次の構成をとる．第２章では，主にモデル検査の基本的な技術を紹介する．第３章では，階層化状態遷移表で記述した組込みソフトウェア設計を量化子のない論理式にエンコードする手法を提案する．エンコードした論理式はBMC問題を表現し，その真偽がSMTソルバーで解明できる．第４章では，明示的モデル検査技術を予備処理として活用し，BMCの加速技術を提案する．検査対象の設計の状態空間を縮小するため，第５章では，有界コンテキスト・スイッチ（Bounded Context Switch，BCS）技術を明示的状態空間の探索手法に統合するアルゴリズムを提案する．その後，検索する実行パスを分割する技術を述べる．第６章では，分散的SMTのフレームワークを提案する．第７章では，前章に提案した加速技術および分散フレームワークを既存のモデル検査ツール「Garakabu2」に実装し，評価する．その結果，本研究で提案した高速技術により，検証速度が大幅に改善されたことを示す．第８章では，本研究の主な成果をまとめ，今後の課題を述べる．