様式 C-19

科学研究費補助金研究成果報告書

平成２２年　６月１０日現在

研究種目： 若手研究(スタートアップ)
研究期間： 2008　～ 2009
課題番号： 20800082
研究課題名（和文）　テストに基づく補題発見を用いた安全性自動検証器の開発

研究課題名（英文）　Development of an automatic safety property prover with lemma discovery based on test

研究代表者
中野　昌弘（NAKANO MASAHIRO）
独立行政法人産業技術総合研究所・システム検証研究センター・産総研特別研究員
研究者番号： 90470046

研究成果の概要（和文）：
本研究では、不動点帰納法による検証能力の向上、適用可能規模の向上のため、テストに基づく発見的手法により帰納法の仮定を求め(補題発見)、従来手法では自動検証できなかった問題に対しても、自動的な検証を行えるようにすることを目的とする。SMT ソルバとして CVC3 を利用して最弱事前条件計算を実装し、補題発見機能と不動点帰納法による不変性自動検証器を実装した。SMT を用いたことや補題の発見、各種手続きの効率化を図ることで、証明力の向上と数十倍程度の高速化を実現し、より規模の大きな問題であっても、自動で証明できるようになった。

研究成果の概要（英文）：
In this research, we developed an automatic invariant prover based on fixed-point induction with lemma discovery. To improve features of automatic verification and efficiencies, we implemented the weakest precondition computation with an SMT solver: CVC3, then implemented functions of fixed-point induction and lemma discovery with the computation. Using an SMT solver and lemma discovery, it could speed up more than ten times and prove a large scale problem.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	980,000	294,000	1,274,000
2009 年度	980,000	294,000	1,274,000
年度			
年度			
年度			
総　計	1,960,000	588,000	2,548,000

研究分野：仕様記述・仕様検証, 数理論理学, 並列分散処理
科研費の分科・細目：
キーワード：

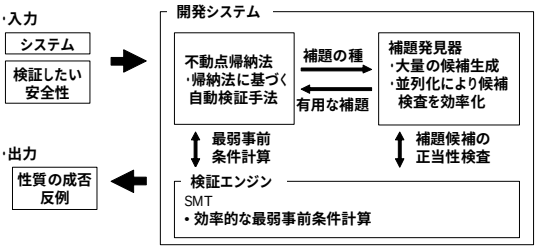
１．研究開始当初の背景

高度に情報化された現代社会では、情報システム・組込みシステムに潜む誤りが社会や企業に大きな影響を与えている。様々なシステムにおいて、簡便に正しさや安全性を確保する技術の開発が強く求められている。

比較的大規模なシステムに対しても適用可能である有界モデル検査 (Bounded Model Checking, BMC)、その検証エンジンとして利用されている SAT (Satisfiability) は、命題論理に基づく充足可能性判定器である。SMT(Satisfiability Modulo Theory)は、SAT に整数等の述語論理を扱えるよう拡張したものであり、次世代のモデル検査の基礎技術として期待されている。これらの技術に基づく有界モデル検査は、現実の問題に適用できる性能を有しながらも、システムの有限長のパスに関して検査するのみで、システムを網羅的に検査するわけではない。このため有界モデル検査はバグ発見に効果を発揮するが、システムの正しさや安全性を保証することができない。

２．研究の目的

本研究では、SMT を用いて大規模システムに適用可能な、システムの正しさ・安全性を保証できる検証手法の開発を目的とし、提案する検証手法の有用性を示すため検証器を試作する。図に試作器の概略を示す。具体的には、不動点帰納法に基づいて、安全性を自動で検証する技法の開発を行う。帰納法の基底・帰納ステップの証明に SMT を用いる。これらの計算では、SMT に実装された様々な決定手続きを利用し、また Incremental SAT 技術により効率的に最弱事前条件の計算を行う。不動点帰納法は、証明の成否の鍵である「帰納法の仮定」を、最弱事前条件計算により段階的に求めていくが、不動点への収束性が低いため、自動検証可能な問題は限られている。本研究では、テストに基づく発見的手法により帰納法の仮定を求め(補題発見)、従来の不動点帰納法では自動検証できなかった問題に対しても、自動的な検証を目指す。



３．研究の方法

初めに、SMT による帰納法の実装に役立つ細かな技術の調査と、利用可能な SMT について調査を行う。また SMT やその並列化、自動検証に関して研究協力者からの意見を頂く。これらの調査に基づき、SMT の入力言語にあわせた仕様記述言語を設計する。試作器の開発は、最弱事前条件計算、不動点帰納法、並列化インタフェースの実装、各種補題候補の生成機能の実装と、段階的に開発を行う。不動点帰納法の実現以降は、各段階に応じた問題による実験が可能である。このため、テストによる問題の早期発見と原因の絞込みが容易であり、研究・開発を効果的に進めるのに役立つ。また実行可能な本体に機能を追加することで開発が進められることから、試作器の開発が計画通りに行われなかったとしても、常に一定の成果が得ることができる。さらに試作器の開発進捗状況を計ることも容易になる。

４．研究成果

SMT の実装のひとつである cvc3 を利用し、最弱事前条件計算を実装した。現状他の SMT では、充足可能であるとき、具体的な１つのモデルを得ることができるのみで、全ての充足可能な場合を得るためのインタフェースが提供されていない。したがって、ソースコードが公開され利用法の自由度が高い cvc3 を利用した。

最弱事前条件計算を用いて、不動点帰納法と補題発見器を実装し、述語間の導出関係をチェックする機能も SMT を利用して実装した。補題発見器では、補題候補として元となる述語の部分論理式から自動的に生成する。より有用な候補から順に調べチェックすることで、補題発見に成功したときに残りの多くの候補を検査しなくともよくなる様にした。

こうして、補題発見器を備えた最小構成の不変性自動検証器を実装したものの、単に SMT を使用して実装しただけでは、プロセス間通信を多用したこれまでの実装と比べても、実行速度ではほとんど改善が見られなかった。そこで、・最弱事前条件を計算する述語に応じて、不要な述語を省き、述語数を抑えた。

・述語間の導出関係の検査は、SMT に計算させると非常に時間がかかるため、2 段チェックにし、多くの場合 SMT を使用しなくともチェックできるようにした。

・補題候補チェックは、アルゴリズム上重複が発生しやすいので、結果をキャッシュするようにした。

・その他、述語を簡単化するようにし、各処理の効率化を図った。

以上により、全体として 3 倍～数十倍程度の高速化を実現した。

分散化については、設計から考慮に入れてはいるが、シングルスレッド性能の改善のために時間を費やしたため、現状は分散化できていない。30 コントロールロケーション程度の規模の例題で、20 分ほどで証明できた。よ

り大規模になれば、分散化は必須であるので、今後も継続して開発し、分散化したい。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 0 件）

〔学会発表〕（計 1 件）
① 中野昌弘、高井利憲、安全性・余安全性に対する反例集合の獲得、第 5 回システム検証の科学技術シンポジウム、2008

〔図書〕（計 0 件）
〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
中野　昌弘（NAKANO MASAHIRO）
独立行政法人産業技術総合研究所・システム検証研究センター・産総研特別研究員
研究者番号： 90470046

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：