様式 C-7-2

自己評価報告書

平成 23 年 4 月 1 日現在

機関番号：13901
研究種目：基盤研究 (B)
研究機関：2008 ～ 2011
課題番号：20300010
研究課題名 (和文) 項書換え系と木オートマトンに基づくプログラム安全性検証に関する研究

研究課題名 (英文) Study of Verification of Security of Programs based on Term Rewriting Systems and Tree Automata

研究代表者
坂部 俊樹 (SAKABE, Toshiki)
名古屋大学・情報科学研究科・教授
研究者番号： 60111829

研究分野： 総合領域
科研費の分科・細目： 情報学・ソフトウェア
キーワード：仕様記述・仕様検証

1. 研究計画の概要

本研究の目的は，項書換え系や木オートマトンの解析技法を応用し，通信プロトコルを始めとするネットワークソフトウエアを含む並行プログラム一般の安全性について，効率的かつ適用範囲の広い検証技法を確立するとともに，検証システムを実装，評価することである．

本課題では，以下の項目を研究する計画である．

(1) 応用 pi 計算における弱い非干渉性の定式化
(2) 応用 pi 計算における安全型の定式化
(3) 安全型と弱い非干渉性の関係の解明
(4) 項書換え系と木オートマトンに基づいた安全型の近似型推論システムの開発
(5) 近似型推論システムへの応用に特化された項書換え系と木オートマトンの解析技法の開発
(6) 近似型推論システムに基づく安全性検証システムの実装と実験による評価

2. 研究の進捗状況

本課題で行った主な研究は以下のとおりである．

(1) ビットエラー環境下での新世代車載 LAN プロトコルの動作解析に関する研究：通信路でビットエラーが発生した場合のプロトコルの振る舞いをモデル検査ツールを用いて網羅的に解析する手法を明らかにした．この結果は，新世代車載 LAN プロトコルが安全に振る舞うことを検証するための基礎となる結果である．

(2) 項書換え系を応用した手続き型プログラム検証に関する研究：プログラムを等価な振る舞いをする制約付き項書換え系に変換し，得られた制約付き項書換え系の性質の証明技法を応用してプログラムの性質を検証する手法を開発した．

(3) 新世代車載 LAN プロトコルの見逃し誤りに関する研究：この研究では，充足可能性判定ツールを用いて新世代車載 LAN プロトコルのエラー検出機構をすり抜ける通信路上のビットエラーを解析する手法を明かにした．実験の結果，設計時には想定していなかった見逃し誤りが存在することが示された．

(4) 項書換え系を応用した命令型プログラム検証に関する研究：命令型プログラムを等価な制約付き項書換え系に変換し，得られた制約付き項書換え系の性質を検証することでプログラムの性質を検証するという手法にお

いて重要な役割を果たす書換え帰納法のための自動補題生成法を開発した．

(5) 抽象データ型の非干渉性に関する研究：従来の情報流解析によるプログラムの安全性は，メモリーの非干渉性に依存している．本研究では，メモリーを一般化した抽象データ型の非干渉性を定式化し，その検証法を考察した．

(6) 等式理論を法とする DPLL 遷移系の提案と実装：プログラム検証の問題は，与えられた等式理論の下での論理式の充足可能性問題に帰着されることが多い．本研究では，与えられた等式理論と論理式に対して，自動的にその等式理論の決定手続きを生成し，論理式の等式理論を法とする充足可能性を判定する枠組みを提案し，その実装，評価を行った．

その他に，項書換え系の停止性に関する研究，充足可能性判定に関する研究，木オートマトンが認識する言語の閉包性の研究，制約付き項書換え系の性質の自動証明に関する研究を行なった．

3. 現在までの達成度

達成度は，「② おおむね順調に進展している．」である．

計画段階から想定していた研究成果は次のものである．

(1) 制約付き項書換え系の帰納的定理証明のための補題生成手法
(2) 項書換え系の最内書換えの下での停止性が決定可能であるクラスの発見
(3) モデル検査手法を用いた車載 LAN プロトコルの安全性検証

計画時には想定していなかった研究成果として次のものがある．

(4) 抽象データ型を用いるプログラムの安全性検証の土台としての抽象データ型の非干渉性の定式化
(5) 等式理論を法とする充足可能性の判定手続きの開発

一方，計画していた応用 pi 計算の安全性の研究は，残念ながら成果を得るに到らなかった．

4. 今後の研究の推進方策

プログラムの安全性検証や命令型プログラムの不変式の自動発見などの研究を通じて，等式で表現される性質が証明されているプログラムモジュールを利用するプログラムの検証技法のベースとして，等式理論を法とする充足可能性の判定ツールが有用であることが明かになった．今後の研究推進方策としては，項書換え系の理論的成果に基づいた等式理論を法とする充足可能性判定ツールとその応用の研究をさらに発展させることが上げられる．

5. 代表的な研究成果

[雑誌論文]（計 19 件）

(1) 中林直生，西田直樹，草刈圭一朗，坂部俊樹，酒井正彦：制約付き項書換え系の書換え帰納法における補題等式の自動生成法，コンピュータソフトウェア，2011，28，pp.173–189，査読有
(2) 馬場達也，坂部俊樹，西田直樹，草刈圭一朗，酒井正彦：等式理論を法とする DPLL 遷移系について，電子情報通信学会ソフトウェアサイエンス研究会，2010，SS2010-36，pp.49–54，査読無
(3) 馬野洋平，酒井正彦，西田直樹，坂部俊樹，草刈圭一朗：基本対称関数に基づく節をもつ CNF 論理式の充足可能性判定，電子情報通信学会論文誌 D，2010，J93-D，pp.1–9，査読有
(4) Keita Uchiyam, Masahiko Sakai, Toshiki Sakabe：Decidability of Termination and Innermost Termination for Term Rewriting S ystems with Right-Shallow Dependency Pairs，IEICE Trans. on Information and Systems，2010，E93-D，pp.953–962，査読有
(5) 坂田翼，西田直樹，坂部俊樹，酒井 正彦，草刈圭一郎：制約付き項書換え系における書換え帰納法，情報処理学会論文誌プログラミング，2009，2，pp.80–96，査読有
(6) 鵜飼謙児，坂部俊樹，高田広章，倉地亮，酒井正彦，草刈圭一朗，西田直樹：ビットエラー通信路におけるスケーラブル CAN の動作解析，電子情報通信学会技術研究報告 (SS2008-37)，2008，108，pp.61–66，査読無

[学会発表]（計 0 件）

[図書]（計 0 件）

[産業財産権]（計 0 件）

[その他]（計 0 件）