様式 Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年 6 月 5 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・大学院情報科学研究科・教授
研究者番号： 60111829

研究成果の概要（和文）：

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，プログラムの安全性などの性質を効率的に検証する技法の開発である．得られた成果は，車載 LAN プロトコルの検証，プログラムの等価性判定，プログラムのループ不変式の自動生成などの技法である．加えて，これらの検証技法の基盤となる技術に関して，項書き換え系の停止性検証，命題論理の充足可能性判定，等式理論を法とする充足可能性判定などの基礎的な成果を得た．

研究成果の概要（英文）：

The purpose of this project is to develop methods for verifying properties of programs by applying techniques of term rewriting and tree automata. The results are methods for verifying automotive LAN protocols and proving program equivalence, and automated generation of loop invariants of imperative programs. In addition, we have obtained several results which are basic to program verification: methods for proving termination of term rewriting systems, efficient SAT solvers for propositional logic and SMT solvers for equational logic.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	3,500,000	1,050,000	4,550,000
2009 年度	2,500,000	750,000	3,250,000
2010 年度	1,900,000	570,000	2,470,000
2011 年度	1,800,000	540,000	2,340,000
総　計	9,700,000	2,910,000	12,610,000

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. 研究開始当初の背景

申請時の状況として，以下のことが上げられる．

(1) 暗号プロトコルの形式的検証：暗号プロトコルの重要な性質は情報漏洩がないことであり，その問題を項書き換え系の到達可能性問題に帰着する研究が注目されていた．

(2) 型推論に基づくオブジェクト指向プログラムの安全性検証：安全型の適切な定式化により，プログラムから情報漏洩がないことを型推論の手法で検証する手法が開発されていたが，安全性の定式化の基礎として用いられる非干渉性が実用的な観点からは強すぎるという課題があった．

(3) 項書き換え系や木オートマトンの解析技術をプログラム検証の種々の問題に応用する研究が盛んになりつつあった．

2. 研究の目的

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．

3. 研究の方法

一般に，プログラムの性質は論理式として定式化され，その性質の検証は，論理式の恒真性を示すことに帰着される．論理式の恒真性を示すには，定理自動証明やモデル検査のツールが有用である．本研究では，次の２つの研究の方法を採用した．

(1) 具体的な検証課題に対して定理自動証明あるいは充足可能性判定のためのツールを用いて解決を図る．

(2) 定理自動証明や充足可能性判定のツールの開発，改良を行う．

4. 研究成果

具体的な検証課題の解決を行った研究として次の成果を得た．

(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検証するための基礎となる結果である．

(2) 新世代車載 LAN プロトコルの見逃し誤り関する研究：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．

上記の (1) および (2) の研究の結果は，新世代車載 LAN プロトコルの設計にフィードバックされ，プロトコルの設計誤りの除去に活用された．

定理自動証明および充足可能性判定のツールに関して，次のような成果を得た．

(3) 項書き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，実装した．また，本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．

(4) 等式理論を法とする充足可能性判定法の提案と実装：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，Knuth-Bendix 手続きにより自動的にその等式理論の決定手続きを生成し，等式理論を法とする論理式の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．また，Knuth-Bendix

手続きによらず，従来の合同閉包手続きを変数を含む等式に拡張した合同閉包アルゴリズムを開発した．後者の研究発表により，電子情報通信学会ソフトウェアサイエンス研究会奨励賞を受賞した．

(5) プログラムのループ不変式自動発見手法の開発：関数呼出しを含むプログラムに対して，非線形不等式（関数呼出項も含む）の形のループ不変式を発見する手法を開発し，実験により評価した．関数の仕様は，しばしば，等式理論として与えられることから着想を得たものである．従来のループ不変式自動生成の手法では扱えなかったプログラムを対象とすることができる．本成果は，ループ不変式自動生成の新たな研究方向を示唆するものと考えられる．

(6) 充足可能性判定法の効率的実現：基本対称節と節の連言からなる論理式の充足可能性判定にリテラル監視法を取り入れて効率化した充足可能性判定ツールを開発し，その有効性を評価した．SAT ソルバーの性能向上は目覚ましく，現実的な問題に応用され始めているが，まだまだ，性能の改善が必要である．本成果は，基本対称節という数を表現するのに適した命題論理式を扱えるように SAT ソルバーを改良する試みであり，SAT ソルバーの効率改善に有効であるだけでなく，問題の論理式としてのコーディングを容易にする．なお，本成果を取りまとめた論文等が電子情報通信学会の論文賞，同学会ソフトウェアサイエンス研究会奨励賞を受賞した．

(7) 項書き換え系と木オートマトン理論の展開：停止性および到達可能性のそれぞれについて，それが決定可能である項書き換え系のクラスで，これまでに分かっているクラスより広いクラスを発見した．その他，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成果を得た．

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 28 件）

(1) 鈴木英一, 坂部俊樹, 酒井正彦, 草刈圭一朗, 西田直樹：関数呼び出しを持つプログラムの非線形ループ不変式の自動生成，電子情報通信学会ソフトウェアサイエンス研究会，2012，SS2011-46，pp.39–44，査読無

(2) 坂井利光, 酒井正彦, 坂部俊樹, 西田直樹, 草刈圭一朗：語問題を基底等式集合の語問題に帰着可能な等式集合のクラスについて，電子情報通信学会ソフトウェアサイエンス研究会，2012，SS2011-47，pp.45–49，査読無

(3) SAKATA Tsubasa, NISHIDA Naoki, SAKABE Toshiki : On Proving Termination of Constrained Term Rewriting Systems by Eliminating Edges from Dependency Graphs，Proceedings of the 20th International Workshop on Functional and (Constraint) Logic Programming (WFLP 2011), LNCS，2011，6816，pp.138–155，査読有

(4) 高桑一也, 西田直樹, 酒井正彦, 坂部俊樹, 草刈圭一朗：制約付き項書換え系における木準同型写像を用いた関数等価性検証，日本ソフトウェア科学会第 28 回大会，2011，7B-1，pp.1–12，査読無

(5) Yoshiharu Kojima, Masahiko Sakai, Naoki Nishida, Keiichirou Kusakari, Toshiki Sakabe : Decidability of Reachability for Right-shallow Context-sensitive Term Rewriting Systems，IPSJ Transactions on Programming，2011，4，pp.12–35，査読有

(6) 日野善信, 酒井正彦, 坂部俊樹, 草刈圭一朗, 西田直樹：2 リテラル監視法で実装された SAT ソルバへの基本対称節処理機能の組み込み，電子情報通信学会ソフトウェアサイエンス研究会，2011，SS2011-38，pp.67–72，査読無

(7) NAGASHIMA Masanori, SAKAI Masahiko, SAKABE Toshiki : Determinization of Conditional Term Rewriting Systems for Program Generation，第 83 回情報処理学会・プログラミング研究会 配布資料，2011，，pp.1–16，査読無

(8) 倉橋克尚, 酒井正彦, 西田直樹, 坂部俊樹, 草刈圭一朗：制約付き木オートマトンとその閉包性，電子情報通信学会ソフトウェアサイエンス研究会，2011，SS2010-63，pp.61–66，査読無

(9) 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
(10) 服部達哉, 酒井正彦, 西田直樹, 草刈圭一朗, 坂部俊樹：順方向ナローイングに基づく右線形右シャロー項書換え系の非停止性証明について，電子情報通信学会ソフトウェアサイエンス研究会，2011，SS2010-44，pp.31–36，査読無
(11) 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
(12) 長島正憲, 酒井正彦, 坂部俊樹, 西田直樹, 草刈圭一朗：条件付き等式の変換に基づくプログラム生成，電子情報通信学会ソフトウェアサイエンス研究会，2010，SS2009-41，pp.37–42，査読無
(13) 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
(14) 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
(15) 大平崇博:次世代車載 LAN プロトコルにおける見逃し誤りの解析，名古屋大学大学院情報科学研究科修士論文，2010,，pp.1–30，査読無
(16) NISHIDA Naoki, SAKAI Masahiko:Completion after Program Inversion of Injective Functions，Postproceedings of the 8th International Workshop on Reduction Strategies in Rewriting and Programming (WRS'08), Electronic Notes in Theoretical Computer Science，2009，237，pp.39–56，査読有
(17) KOJIMA Yoshiharu, SAKAI Masahiko, NISHIDA Naoki, KUSAKARI Keiichirou, SAKABE Toshiki：Context-Sensitive Innermost Reachability is Decidable for Linear Right-Shallow Term Rewriting Systems，IPSJ Transactions on Programming，2009，2，pp.20–32，査読有
(18) 長島正憲, 酒井正彦, 坂部俊樹, 西田直樹, 草刈圭一朗:条件付き等式の変換に基づくプログラム生成，電子情報通信学会ソフトウェアサイエンス研究会, 信学技報 SS2009-41，2009，109-343，pp.37–42，査読無
(19) 御宿義勝, 酒井正彦, 坂部俊樹, 草刈圭一朗, 西田直樹：右線形右シャローな項書換え系における文脈依存停止性の決定可能性について，電子情報通信学会ソフトウェアサイエンス研究会, 信学技報 SS2009-41，2009，109，pp.31–36，査読無
(20) 鈴木翔, 草刈圭一朗, 坂部俊樹, 酒井正彦, 西田直樹:高階書換え系における引数切り落とし法と実効規則，電子情報通信学会ソフトウェアサイエンス研究会, 信学技報 SS2009-41，2009，109，pp.25–30，査読無
(21) 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，日本ソフトウェア科学会第 26 回大会講演論文集，2009，7B-2，pp.14–14，査読無
(22) 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
(23) UCHIYAMA Keita, SAKAI Masahiko, SAKABE Toshiki, KUSAKARI Keiichirou, ISHIDA Naoki：Decidability of Termination Properties for Term Rewriting Systems Consisting of Shallow Dependency Pairs，Tech. Rep. of IEICE (SS2008-45)，2008，108，pp.37–42，査読無
(24) 馬野洋平，酒井正彦，西田直樹，坂部俊樹，草刈圭一朗:基本対称関数を付加した CNF 論理式の充足可能性判定，電子情報通信学会ソフトウェアサイエンス研究会（SS2008-44），2008，108，pp.31–36，査読無
(25) 古市祐樹，西田直樹，酒井正彦，草刈圭一朗，坂部俊樹：制約付き項書換え系の潜在帰納法を利用した手続き型プログラム検証の試み，情報処理学会論文誌プログラミング，2008，1，pp.100–121，査読有
(26) 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

(27) 西田直樹，坂田翼，酒井正彦，草刈圭一朗，坂部俊樹:制約付き項書換え系の定理自動証明における等式の方向付けのための簡約化順序，電子情報通信学会技術研究報告 (SS2008-20)，2008，108，pp.43–48，査読無
(28) 坂田翼，西田直樹，酒井正彦，草刈圭一朗，坂部俊樹:プレスブルガー文付き項書換え系における書換え帰納法について，電子情報通信学会技術研究報告 (SS2008-1)，2008，108，pp.1–6，査読無

6. 研究組織

(1) 研究代表者
坂部 俊樹（SAKABE TOSHIKI）
名古屋大学・大学院情報科学研究科・教授
研究者番号：60111829
(2) 研究分担者
酒井 正彦（SAKAI MASAHIKO）
名古屋大学・大学院情報科学研究科・教授
研究者番号：50215597