様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月１０日現在

機関番号：８２６２６
研究種目：若手研究（Ｂ）
研究期間：2009～2010
課題番号：２１７０００２２
研究課題名（和文）　等式付ツリーオートマトンの算術制約翻訳可能性と自動検証技術への応用に関する研究
研究課題名（英文）　Equational Tree Automata: Arithmetic Constraint Definability and the Application Towards Automated Verification
研究代表者
大崎　人士（OHSAKI HITOSHI）
独立行政法人産業技術総合研究所・産学官連携推進部門・連携研究体副体長
研究者番号：００３５６６２７

研究成果の概要（和文）：正則ACツリーオートマトン(regular AC-tree automata)の葉言語(leaf-languages)を表現する正則可換文法(commutative regular grammar)は、線形算術制約および正数ベクトル加算系(non-negative vector-addition systems)と等価な表現力を持つ(Parikh1966他)。本研究では、正数ベクトル加算系の定義を、整数（正値、零、負値）から成る座標系上に拡張した場合、それに対応する可換文法が満たすべき代数的性質を解明する。本研究の主な成果は、可換クリーニ代数の公理系に新たな演算子iと６つの公理を導入し（i-可換クリーニ代数と呼ぶ）、i-可換正規文法は、整数ベクトル加算系と等価な表現力を持つこと、正則可換文法、線形算術制約、正数ベクトル加算系の同形関係は、整数制約上へ自然に拡張可能であることが示せたことである。

研究成果の概要（英文）：Equational tree automata and the applications have been developed since 2001 when Ohsaki proposed this theory. The automated verification based on equational tree automata, ACTAS (http://staff.aist.go.jp/hitoshi.ohsaki/actas/), can be applied to the analysis of cryptographic protocols, XML schema and programming languages. The leaf-languages of regular AC tree automata are known as expressive as non-negative linear arithmetic constrains and semi-linear sets. We studied in this research program a new class of commutative grammar which can be the counterpart of “integer” linear arithmetic constraints, and thus of vector-addition systems. First we introduce the notion of “inverse” over (commutative) languages, more precisely, we define “commutative i-Kleene algebra” by introducing new operator i and 6 new axioms. The algebra admits Boolean operations together with inverse operation. This result is obtained from the observation that Hopkins and Kozen approach (1999) can be naturally extended to the commutative i-Kleene algebra. This implies that (1) commutative i-regular grammar is as expressive as commutative i-context-free grammar, and thus (2) commutative i-regular grammar is the counterpart of integer linear arithmetic.
In addition to the above-mentioned research activity, we contributed for familiarizing our equational tree automata to young researchers in Japan and overseas.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	1,900,000	570,000	2,470,000
２０１０年度	1,200,000	360,000	1,560,000
総　計	3,100,000	930,000	4,030,000

研究分野：計算論
科研費の分科・細目：情報学・情報学基礎

キーワード：ツリーオートマトン、書換系(rewriting systems)、可換文法、算術制約

１．研究開始当初の背景

「等式付ツリーオートマトン」の研究は、理論提唱した 2001 年以来、研究に賛同する研究者を国内外に獲得しつつ、基礎研究の成熟と研究の応用化の両方が進められていた。José Meseguer 教授を中心とするイリノイ大学アーバナシャンペン校の Formal Method Group は、同大学計算機科学科を拠点として、書換論理(rewriting logic)にもとづく仕様記述言語 Maude の設計とその理論研究を行っている。大崎と共同開発したソフトウェアライブラリ CETA は、等式付ツリーオートマトンの受理言語に関する判定問題を解消する機能をもつ。仕様記述に交換律・結合律を含む場合は、半線形集合(semi-linear sets)上の問題に帰着して Ginsburg のアルゴリズムを適用する。同様に、結合律のみを含む場合は、Anglins のアルゴリズムを適用して、本来決定不可能な判定問題を機械学習の要領で問題解消を図る。CETA に実装された機能により、例えば、Maude 記述の仕様が充分完全性(sufficient completeness)を満たすかという静的解析を自動的に行う。プロトコル検証の研究では、Ralf Treinen 教授（現在パリ第７大学、前 ENS Cachan 助教授）らとともに、通信プロトコルの仕様記述から検証用コードを自動生成し、生成された検証用コードから安全性を自動判定する検証法の研究を進めた。Treinen 教授は、プロトコル仕様記述言語 PROUVÉ の設計開発責任者である。また、大崎は、書換系とツリーオートマトンを組み合わせた自動検証法を提案し、さきがけ研究プロジェクト(2002.10～2006.3、JST「機能と構成」領域・片山卓也領域総括）を通じて無限状態モデル検査ツール ACTAS を開発した。ACTAS の計算機構で、国内特許、米国特許、EU 特許を取得している。

理論面では、Sophie Tison 教授らリール（仏）の研究者らとの共同研究を契機に、理論の成熟度が増し、その後、国内研究者らとの研究交流の機会も増えた。国内でも、関浩之教授（奈良先端大）と弱構造化文書処理への応用を見据えた等式付ツリーオートマトンの理論的拡張を行った。小林直樹教授（東北大）とは、非線形算術制約と等式付ツリーオートマトンの表現力の関連に着目して、充足可能性の判定可能な算術制約のクラス、等式付ツリーオートマトンへ翻訳可能なクラスの切り出しを行った。小林教授との研究成果を纏めた論文は、書換系分野の国際会議（RTA; International Conference on Rewriting Techniques and Applications）で最優秀論文賞（Best Paper Award）を受賞している。

２．研究の目的

本研究では、算術制約の解集合を等式付ツリーオートマトンで表現（エンコード）する研究で得られた成果を核にして、非線形算術制約を伴う遷移システムの自動検証法を提案することが目的である。非線形な算術制約をもつ遷移システムをモデル化できる数理的な枠組みとしては、ハイブリット・オートマトンが代表的である。しかし、ハイブリット・オートマトンはほとんどの判定問題が決定不可能であるなど、自動検証技術を開発するための基盤的枠組みには不向きである。一方、単調 AC ツリーオートマトン(monotone AC tree automata)と呼ばれる等式付ツリーオートマトンは、空判定が決定可能であること、合併集合や共通集合の演算について閉じていることなど、特定の自動検証に必要な性質を備えている。実際に、単調指数ディオファントス算術（monotone exponential Diophantine arithmetic)と名付けた算術制約のクラスは充足可能性の判定が決定可能なこと、その部分クラスで正の解集合を受理する単調 AC ツリーオートマトンを構成可能なことを昨年小林とともに解明し、非線形算術制約付きの遷移システムを対象とする自動検証の可能性を示した。本研究では、この研究をさらに一歩進めて、1.算術制約付きの遷移システムを等式付ツリーオートマトンと書換系でいかに翻訳(モデル化)するか、2.等式付ツリーオートマトンと書換系を入力として、その書換閉包（rewrite descendants）をいかに構成的に計算するか
の 2 つのテーマに取り組み、それぞれのテーマに対して具体的な方法を解明するための基礎研究を行う。

３．研究の方法

単調 AC ツリーオートマトンは、表現力がありすぎて実利用には向かないという実験的考察があり、本研究では、単調 AC ツリーオートマトンの部分クラスである「正則 AC ツリーオートマトン」の再考から着手した。正則 AC ツリーオートマトン(regular AC-tree automata)の葉言語(leaf-languages)を表現する正則可換文法(commutative regular

grammar)は、線形算術制約および正数ベクトル加算系(non-negative vector-addition systems)と等価な表現力を持つことが知られており、自動検証技術の有力な要素技術である。Hopkins と Kozen(1999)によって、30年を経て新事実が発見されて、言語方程式（language equations）にも連続関数の特徴が存在することが示された。Hopkins と Kozen は、Parikh の定理の一般化となっており、正則可換文法から、等価な表現の正数ベクトル加算系を多項式時間で算出することが実際に可能である。しかし、従来のツリーオートマトンの枠組みでは、葉(leaf)記号の数でベクトル要素を表現する手法を用いており、負数を自然に扱うことができない。したがって、整数(integer)ベクトル加算系に対応する可換文法が自然に定義可能であるかは、長らく議論されずにいた。本研究では、Hopkins と Kozen の研究で用いられた「Kleene 代数」を拡張して、負数を扱える代数系を定義し、その理論的帰結として得られる可換文法の特徴付け、整数ベクトル加算系との対応を考察する。

４．研究成果

すでに本報告書の概要の述べた通り、正則 AC ツリーオートマトン(regular AC-tree automata)の葉言語(leaf-languages)を表現する正則可換文法(commutative regular grammar)は、線形算術制約および正数ベクトル加算系(non-negative vector-addition systems)と等価な表現力を持つ(Parikh1966 他)。本研究では、正数ベクトル加算系の定義を、整数（正値、零、負値）から成る座標系上に拡張した場合、それに対応する可換文法が満たすべき代数的性質を解明する。本研究では始めに、可換クリーニ代数の上に割り算の概念を導入するため、単項演算子 i を導入して、可換クリーニ代数の公理系に i に関する６つの新たな公理を加えた(i-可換クリーニ代数と呼ぶ)。次に、i-可換クリーニ代数の具体例である i-可換正規文法に着目して、Hopkins と Kozen(1999)による「Parikh の定理の一般化」の中で用いられた言語多項式のテイラー展開の手法が、i-可換正規文法に適用可能であることを示した。その結果、(1) i-可換正規文法は、i-可換文脈自由文法と等価な表現力を持つこと、(2) i-可換正規文法は、整数ベクトル加算系と等価な表現力を持つことが示せた。以上により、正則可換文法、線形算術制約、正数ベクトル加算系の同形関係は、整数制約上へ自然に拡張可能であることが判明した。

以上の成果とともに、本研究では、大崎(2001)が提唱する等式付ツリーオートマトン理論の普及活動を行った。研究期間中には、国際サマースクール(ISR'09)や、複数の国内大学(大阪大学、北海道大学他)にて等式付オートマトンの講義を行い、計算機科学分野の若い研究者らに広める機会を創出した。

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１件）

①著者名：Nguyen Van Tang, 大崎人士
論文標題：Checking On-The-Fly Universality And Inclusion Problems Of Visibility Pushdown Automata
雑誌名: IEICE Transactions of Fundamentals
査読：有

〔学会発表〕（計７件）

① 発表者名：大崎人士
発表標題：ツリーオートマトンと計算論基礎
学会等名：複合情報学特別講義講義第二発表年月日：2010 年 12 月 16, 17 日
発表場所：北海道大学大学院情報科学研究科（札幌市）

② 発表者：大崎人士
発表標題:Introduction to Tree Automata, Track A (Introductory Course)
学会等名：4th International School on Rewriting (ISR2009), RTA
発表年月日：2009 年 6 月 23 日
発表場所：Brasilia (Brazil)

③ 発表者：大崎人士
発表標題：Equational Tree Automata, Track B (Advanced Course)
学会等名：4th International School on Rewriting (ISR2009), RTA
発表年月日：2010 年 6 月 24 日
発表場所：Brasilia (Brazil)

④ 発表者：大崎人士
発表標題:可換文法－Commutative Grammar
学会等名：記号論理と情報科学研究集会(SLACS2009)
発表年月日：2010 年 9 月 1 日
発表場所：京都大学（京都府右京区）

⑤ 発表者：大崎人士(登壇者) 他4名
発表標題：Collaborative Facilities for Verification: SATSUKI
学会等名：Workshop on Simulation Based Depelopment of Certified Embedded Systems
(AIST/CVS-INRIA/LIAMA workshop)
発表年月日：2009年10月6日

発表場所：淡路夢舞台国際会議場（兵庫県淡路市）

⑥発表者：大崎人士
発表標題：システム検証技術を社会へ一組み込みシステム産業の検証技術高度化支援，基調講演
学会等名：ソフトウエアの安全性・信頼性確保のための形式手法普及セミナー（主催三菱総合研究所・経済産業省）
発表年月日：2010 年 2 月 14 日
発表場所：三菱総合研究所（千代田区）

⑦発表者：大崎人士
発表標題：システム検証技術を社会へ一組み込みシステム産業の検証技術高度化―，招待講演
学会等名：第８回カーエレクトロニクス研究会（主催(財)九州先端科学技術研究所）
発表年月日：2011 年 5 月 20 日
発表場所：日本自動車会館（港区）

〔産業財産権〕
○取得状況（計２件）

名称：Reactive System Safety Verification Device, Method, Program and Recording Medium Containing the Program.
発明者：大崎人士、高井利憲
権利者：独立行政法人産業技術総合研究所（大崎人士、高井利憲）
種類：特許
番号：No. US7503060B2
取得年月日：2009 年 3 月 10 日
国内外の別：国外(米国)

名称：リアクティブ・システムの安全性検証装置、方法、プログラム及びそのプログラムを記録した記憶媒体
発明者：大崎人士、高井利憲
権利者：独立行政法人産業技術総合研究所（大崎人士、高井利憲）
種類：特許
番号：第 4406726 号
取得年月日：2009 年 11 月 20 日
国内外の別：国内

〔その他〕
ホームページ等
http://staff.asit.go.jp/hitoshi.ohsaki/

６．研究組織
(1)研究代表者
大崎　人士（OHSAKI HITOSHI）
独立行政法人産業技術総合研究所・産学官連携推進部門・連携研究体副体長
研究者番号：00356627