様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

令和　５ 年　 ５ 月 １９ 日現在

機関番号：１３９０１
研究種目：基盤研究(B)（一般）
研究期間：2019～2022
課題番号：１９Ｈ０４０８３

研究課題名（和文）ソフトウェアモデルへの量的尺度の導入とプログラム解析への応用

研究課題名（英文）Quantitative extension of formal models and its application to software analysis

研究代表者
関　浩之（Seki, Hiroyuki）

名古屋大学・情報学研究科・教授

研究者番号：８０１９６９４８

交付決定額（研究期間全体）：（直接経費）　　10,380,000円

研究成果の概要（和文）：ソフトウェアの信頼性を保証する手法として，量的情報流の動的解析，データ値を扱う計算モデル，重み付き計算モデルの３つの課題について研究を行った．動的情報流の２つの定義を提案し，その計算量解析を行うとともに，モデル計数ツールを用いた実装を行った．レジスタ計算モデルについて，レジスタ付きCFGの基本問題の計算量を明らかにするとともに，比較演算子に着目したRCFGの一般化，RCFGに対応するレジスタ付きPDSのLTLモデル検査アルゴリズム，レジスタオートマトンと能力等価な凍結演算子付きmu-計算の部分クラスを提案した．重み付きレジスタオートマトンの最小重み実行問題の計算量を明らかにした．

研究成果の学術的意義や社会的意義
ソフトウェアの信頼性を保証する方法論を確立することは現代社会の喫緊の課題である．本研究の成果は，長年にわたり蓄積されたソフトウェア検証の理論的成果をさらに現実の問題に応用可能とするため，情報漏洩量，データ値および重みといった量的概念を組み込んだ数理モデルに対して，ソフトウェアの信頼性を保証する手法を与えたことに学術的および社会的意義がある．例えば，有限状態モデルにデータ値を扱う能力を加えると容易に基本問題が判定不能となってしまうが，本手法におけるレジスタモデルではデータ値の操作に合理的制約を加えることにより，重要な基本問題の判定可能性を失うことなく拡張が可能となっている．

研究成果の概要（英文）：We studied on the following three research topics. First, we proposed two notions on dynamic quantitative information flow (QIF), analyzed the complexity for computing these QIFs and implemented a tool for computing these QIFs based on model counting tools. Second, we investigated the complexity of basic problems on register context-free grammar (RCFG). We then proposed generalized RCFG and provided a sufficient condition for an RCFG to have decidability property on basic problems. As an application of register models to software verification, we studied LTL (linear-time temporal logic) model checking for register pushdown systems. We also proposed a subclass of mu-calculus with the freeze quantifiers which are equivalent to register automata. Furthermore, we investigated the reactive synthesis from visibly register pushdown automata. Third, we introduced the optimal run problem for weighted register automata and analyzed its complexity.

研究分野：ソフトウェア基礎理論

キーワード：ソフトウェア検証　モデル検査　プログラム自動合成　レジスタオートマトン　形式言語理論　量的情報流　線形時相論理　セキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

ソフトウェアの信頼性を担保する本質的な手法はその正しさを数理的に保証することであり，モデル検査や定理自動証明の技法として方法論が追究されてきた．これらの成果を実用システムに適用可能とするためには，量的概念を考慮した数理的モデルに拡張する必要がある．例えば，実時間システムの安全性には時間の概念が欠かせないし，ソフトウェアのセキュリティ保全に数理的検証技術を応用する場合，機密情報の漏洩量を閾値以下に抑えられることの量的保証が必要である．このような観点から，量的概念をもつ数理モデルを設定し，モデルの性質を理論・実践両面から究明することが本課題の学術的「問い」である．量的概念は多様であることから単なる拡張ではいわゆる「次元の呪い」のため応用可能な手法は得られない．例えば，データ値の無限集合に対しては，その構造について現実性を失わない範囲である種の対称性を仮定し，系の振舞いを有限空間内に埋め込むことができるかどうかに，問題の理論的面白さと同時に応用可能性が集約されているといえる．

２．研究の目的

本研究では，量的概念をもつ数理モデルに基づくソフトウェアの解析法および検証法を開発することを目的とする．その学術的独自性・創造性は以下の通りである．

**複眼的アプローチ：**本研究課題では特にセキュリティ・プライバシの定量化に着目する．これらの情報の漏洩量について論じるには，プログラム理論（どのような手順で計算や記号的推論が行われるのかという意味論的解析）と情報理論（系あるいは通信路のどの入力がどの出力にどの程度影響を及ぼすのかという確率論的解析）の双方が必要である．情報理論では通常，系自体はブラックボックスと見なし送受信データの意味は解釈せず系の確率的振舞いのみに着目する．したがって，プログラムを通信路と見立てて情報理論を適用する際には，プログラムの意味論を組合せることにより精密な解析を行うことが可能となる．本研究ではこれに加え，次項でも述べるように形式言語理論，計算複雑さの理論を援用して複眼的な立場から系の性質を論じる点に独自性がある．

**理論的考察と実証的研究：**本研究前半では，後に具体的に述べる量の概念の数理モデルに対して，モデルの表現能力（認識または生成する言語のクラスの同定や比較），重要な判定問題の可解性や計算複雑さの上下界を究明する．研究期間の後半ではより実践的な課題に移行する．特に数値計算が関連する問題に対しては，理論的にしばしば大きな計算量下界が導かれる．これらを単に悲観的にとらえるのではなく，実用上効率良く解析の行えるクラスを見出すとともに，実践を通じて有効な解析法を見出す．具体的に，近年多くの成功をもたらしている SAT（充足可能性問題）／SMT（背景理論付き SAT）に関連するツール，特に，確率や情報量の計算の本質は事象の数え上げであることから，制約式の解を計数する#SAT ソルバや，解を列挙する ALLSAT ソルバを利用した解析手法に重点を置いて実装を行う．

**数理的手法におけるセキュリティの位置づけ：**一般的な安全性とは，系の状態集合が「望ましい状態」と「望ましくない状態」に分割されているとき，系が望ましくない状態に到達しないことを意味する．セキュリティについて論じる場合はこれに加えて，情報がどのように系の内部を流れるか，例えば，着目した変数の内容がどの変数に代入されるか，あるいは，どの条件判定に影響を及ぼすかが重要であり，このような意味で「望ましくない情報の流れ」がある閾値以下しか生じないことが本質的である．この特性を意識して数理的手法のセキュリティ検証への適用を考察する．

３．研究の方法

本研究課題では以下の３つのテーマを設定する．

**量的情報流の動的解析：**前述したように，機密情報やプライバシ情報が，それらにアクセスする権限のないユーザやプロセスに漏洩しないようにデータの流れを制御することが情報セキュリティ技術の基本的な目的といえる．入力データに機密度に基づくレベル(セキュリティレベル)，変数やチャネル（合わせて単に出力とよぶ）にクリアランス（どのセキュリティレベルのデータを流せるか）を設定し，出力にそのクリアランスに反するセキュリティレベルの入力データが流れ込まないかの観点からデータ流解析を行うことを情報流解析とよぶ．またこの観点から望ましくない情報流が一切発生しないことを非干渉性と呼び，ソフトウェアがセキュリティ面で満たすべき性質とみなされてきた．しかし，非干渉性は実システムに対しては制約が強すぎることが指摘され，機密度の高い入力（機密入力と略）に関する情報がどの程度，クリアランスの低い出力（公開出力と略）に流れるかを定量的に分析する，いわゆる量的情報流（quantitative information flow，QIF）解析が注目されている．QIF に関して，情報流を一種の型と見なして伝統的な型システムの手法を拡張した解析法が初期の頃から研究されてきた．型に基づく手法は比較的解析の効率が良いが解析精度が劣るという欠点がある．また，プログラムへの例入力に

対する振舞いを統計的に解析して漏洩量の近似計算を行う方式も提案されているが十分な精度は得られていない．これらに対し，プログラムをその入出力関係を表す論理式に近似変換し，漏洩量の計算を，論理式を満たす解の個数の計算（解の計数とよぶ）に帰着する手法が注目されている．これは，充足可能性問題(SAT)および背景理論付 SAT 問題(SMT)を解くツールが飛躍的に発展したことによる．本課題においても，解の計数を行えるように拡張された#SAT ツールや解を列挙する ALLSAT ツールを用いた解析法に重点をおく．

研究期間の前半ではまず，動的 QIF についての理論的考察を行う．QIF は機密入力に関するエントロピー（曖昧さ）が出力値の観測によって平均的にどの程度減少するか，すなわち，機密入力と公開出力の間の相互情報量によって定義されることが多い．しかし，漏洩量は個別の実行に依存して変化する．漏洩量の平均値が小さくてもある実行では漏洩量が大きい場合そのような実行は中断（もしくは無効化）すべきである．そこで，個々の実行における観測出力値に基づいて QIF を導入する必要がある．これを動的 QIF とよぶ．動的側面を考慮したセキュリティ尺度が提案されているものの，確率的動作を行うプログラムについては，漏洩量が負値を取る場合があり直観に反する．そこで本研究ではまず，動的 QIF が満たすべき条件を整理しそれらを満たす動的 QIF の定義を提案する．引き続き，動的 QIF を求める計算複雑さの分析を行う．研究期間の後半では，動的 QIF を計算する具体的な手法やアルゴリズムを開発する．次いでツールの実装を行い，提案手法の有効性を評価する．

**データ値を扱う計算モデル：**XML に代表される構造化文書への問合せや更新のための言語がいくつか開発されている（例えば，XPath，XQuery）．構造化文書はユーザが定義するタグによって階層化され，木構造によって表現することができる．これら木構造（以下，木と略）に対する問合せは，木上の経路に基づく照合を行う場合は有限オートマトン，部分木の照合を行う場合は木オートマトンを用いてモデル化でき，多くの研究がなされてきた．一方，構造化文書はタグ名の他にデータ値（XML における属性値や PCDATA 等）をもつ．従って，有限状態遷移系に基づく数理モデルを，データ値を扱えるように拡張する必要がある．しかしながら，有限状態遷移系に整数等のデータ値を扱う能力を加えると，ごく単純な操作のみしか許さなくてもチューリング万能となり所属問題や空問題など基本問題が判定不能となることはよく知られている．そこで，データ値に対する操作を，入力データ値の記憶（レジスタへのロード）と値の比較のみに限定し，有限オートマトンおよび文脈自由文法(CFG)を拡張したモデルとして，レジスタオートマトン(RA)，レジスタ CFG（RCFG）が提案され，その諸性質を考察した研究も存在する．しかし，RA や RCFG におけるデータ比較演算は等号判定のみであり，制約が強すぎる．

本研究ではまず，RCFG の基本的表現能力を解明するため，ε-規則の有無，単記号規則の有無などが表現能力に与える影響，文法のサイズパラメータ（レジスタ数など）が生成能力に与える影響を考察し，影響のある場合は部分クラスの表現階層を同定する．次に，データ値に対する比較演算を一般化することを試みる．任意の二項関係を許せば自明でない問題はほとんど判定不能となってしまうため，原始命題に用いることのできる二項関係として，有理数等の稠密集合上の全順序（数の大小比較等）を含み，基本問題の判定可解性を失わない二項関係のクラスを設定する．並行プロセス計算における模倣関係に対応する性質を満たすような二項関係がその候補である．データ値に対する比較演算が等号判定のみの場合に系の挙動が解析しやすいのは，レジスタの状態を，その内容である具体的なデータ値の代わりに，同じデータ値をもつレジスタ部分集合へ同値類分割すれば十分だからである．例えばレジスタ数が 4 個の場合，{{1,3}, {2,4}}で第 1 レジスタと第 3 レジスタ，第 2 レジスタと第 4 レジスタの値が等しいことを表しておけば，具体的なデータ値は不要となる．一般の二項関係をデータ値の比較に用いることができる場合はこの同値類分割を一般化した一種の型を導入することにより，系の振舞いに関する基本問題の判定可解性を示す．これらの理論的検討に高田喜朗氏（高知工科大准教授）が研究協力者として参加する．また，時間オートマトン，時間プッシュダウンオートマトン（TPDA）は，現在時刻を外部からの入力値とみなせば RA，RCFG の特殊なケースとみなせる．

**重みをもつ計算モデル：**データ値は計算モデル（オートマトンなど）が直接扱う量的概念であるのに対し，量的情報流は計算モデルの振舞いに付随して生じる情報の流れを定量化した概念である．ここでの「重み」も量的情報流と同様，計算モデルが直接扱う量ではなく，確率，コストなど，モデルの操作的意味に付随して発生する，外部から与えられる量を表現するものである．有限オートマトンの遷移に重みを与えたものを重み付きオートマトン（weighted automata，WA）とよび，レジスタ付きオートマトン（RA），プッシュダウンオートマトン（PDA）に対して同様に重みを導入したものを WRA，WPDA とよぶ．重みは具体的に確率やコスト等を表すことができる．WRA や WPDA は形式言語理論分野で認識可能級数および代数的級数の操作モデルとして長く研究されてきた．

本研究ではこれらの蓄積を踏まえ，特にソフトウェア解析の観点から，重み最小実行問題の計算複雑さの解析とアルゴリズムの開発を行う．最小化問題はグラフの最短経路問題の一般化ともとらえることができ，特に WRA の重み最小実行問題を解くアルゴリズムは，データ値を扱うシステムのコスト最適スケジューリング等に応用可能である．

## ４．研究成果

### (1) 量的情報流の動的解析

量的情報流(QIF)はプログラムの出力値を観測することによって知りうる機密入力値に関する情

報の定量的尺度であり，プログラムの機密入力値と観測可能な出力値との相互情報量として定義されることが多い．これは実行前（コンパイル時）における機密情報の漏洩量の期待値といえる．これに対して，動的情報流とはプログラム実行時，すなわち特定の実行に対する漏洩量の尺度である．動的情報流の定義に対して求められる条件として，(R1) 負値をとらないこと，(R2) 個々の機密入力値と独立に定義されること，(R3) 従来の QIF の定義と互換性をもつことが挙げられる．すでに動的情報流の定義が提案されているが(R1)-(R3)をすべて満たすものは存在しなかった．本研究では，動的情報流の定量的尺度として，出力値観測後の機密入力値の自己情報量に基づく指標（QIF1）と，機密入力値と出力値の同時情報量に基づく指標（QIF2）の２つを提案し，それらの定義の妥当性と特性を議論した．理論的考察として，ブールプログラムの３つのクラス（ループなし，while 型，再帰型）に対して，QIF1 と QIF2 の計算問題に付随する判定問題の計算量を明らかにした．例えば，while 型プログラムに対する QIF2 問題は PSPACE 完全であることを証明した．

以上は理論的考察であるが，さらに，既存のモデル計数ツールを活用してこれらの動的 QIF を計算するツールを実装し，ベンチマークプログラムを用いて計算実験を行った．具体的に，C プログラムを有界モデル検査器 CBMC によってブール式に変換し，これを観測出力値とともに投射モデル計数ツールに与えることによって QIF1, QIF2 を計算する．モデル計数ツールとして，aZ3, SharpCDCL，DSharp-p，GPMC を用いた．先行研究で用いられている 14 個のベンチマークに対して実験を行った結果，小規模プログラムに対する提案計測手法の有効性が確認できたが，大規模プログラムへの適用についてはさらなる改善が必要であることも分かった．以上の結果は論文誌 IEICE Transactions on Information and Systems に採択された．

以上を踏まえ，動的 QIF をより効率良く計算する手法についての研究を行った．動的 QIF への入力は解析対象のプログラムと観測出力値の２つである．上で説明したように，観測出力値が異なると，動的 QIF も一般に異なる．計算に先立って，与えられたプログラムは CBMC によりブール式$\varphi$に変換される．この後の計算方式に次の２つの方法がある．Compute-on-Demand 方式(CoD)：出力値$o$が与えられるたびに$\varphi$に$o$の情報を組み込んだブール式$\varphi'$を作りこれに対してモデル計数を行う．Construct-in-Advance 方式(CiA)：$\varphi$を効率的な計数が可能な内部表現（BDD または d-DNNNF）に変換し$o$が与えられたらこの内部表現に基づいてモデル計数を行う．CoD では後段，CiA では前段の計算コストが大きい．よって，同一のプログラムに対し，多くの出力値について動的 QIF を計算したい場合は CiA のほうが適していると予想される．本研究では，CiA においてさらに，与えられたプログラムをより規模の小さいプログラムに分解し，分解された部分プログラムの QIF の計算結果からもとのプログラムの QIF を得る手法を２つ考案した．プログラムの入出力値集合を分割する手法（Value Domain decomposition，ValDo）と，プログラム構造を直列分解する手法（Sequential composition，Seq）である．Seq においては，幅優先探索を用いて正確な動的 QIF を計算する方法の他に，動的 QIF の上下界を計算する近似計算法も考案した．下界については深さ優先探索を閾値で打ち切る手法，上界については Max#SAT 問題に帰着して計算する手法を用いる．以上の手法に基づく動的 QIF の計算ツールを実装した．ベンチマークを用いた実験を行った結果，ValDo は QIF 計算の並列化に適し，Seq はプログラムがいくつかの直列フェーズに分解可能な場合に効果が大きいことが示された．この成果は国際会議 SECURWARE 2019 に採択された．

（2）レジスタ計算モデル

文脈自由文法(Context-Free Grammar，CFG)にデータ値を扱う能力を加えたレジスタ CFG (Register CFG，RCFG)が知られている．本研究では，RCFG とそれに関連する計算モデルについて，所属問題と空問題の計算複雑さを明らかにした．特に，RCFG に対する所属問題および空問題はいずれも一般に EXPTIME 完全であること，所属問題については，ε-規則なし RCFG および成長的 RCFG に対してそれぞれ，PSPACE 完全，NP 完全となること，一方，空問題については，これら２つの部分クラスに対しても，EXPTIME 完全に留まることを示した．RCFG に対応する言語認識モデルであるレジスタプッシュダウンオートマトンおよびレジスタ木オートマトンについても，その言語表現能力ならびに基本問題の計算複雑さを明らかにした．この研究成果は，理論計算機科学分野の著名誌 Theoretical Computer Science に採録された．

RCFG においてはデータ値に対する比較演算として等号判定のみが許されている．そこで本研究では，データ値に対する任意の比較演算を許すように拡張した一般化 RCFG（Generalized RCFG，GRCFG）を提案した．そして，稠密集合（有理数の集合など）上の大小関係を扱う実用上重要な GRCFG の部分クラスでは所属問題や空問題が判定可能である一方，一般にはこれらの問題は判定不能となることを証明した．さらに前者の結果を一般化し，これらの問題が判定可能となる簡潔で見通しのよい十分条件（模倣性と進行性）を提案した．

再帰プログラムのための簡潔な計算モデルとしてプッシュダウンシステム(Pushdown System，PDS と略)が知られている．本研究では PDS をレジスタ付きに拡張したレジスタ PDS（Register PDS，RPDS）を導入し，その高信頼ソフトウェア開発への応用に取り組んだ．そのためにまず，RPDS の正則保存性について理論的な考察を行った．任意の正則言語$R$に対して変換 T を適用して得られる言語$T(R)$が正則であるとき，$T$は正則保存性をもつという．仕様$S$と検証対象のプログラムのモデル$T$が与えられたとき，$T$の任意の実行が$S$を満たすかどうかを判定するモデル検査問題すなわち，$T(I) \subseteq S$が成り立つかどうかを判定する問題を考える（ここで$I$はプログラムの初期

状態の集合)．もし$S$の補集合$\overline{S}$が正則言語であり，かつ，$T$が正則保存性をもつならば，モデル検査問題は判定可能となる．なぜならば，$T(I) \subseteq S$ は $T(I) \cap \overline{S} = \emptyset$と等価であり，正則言語のクラスは積集合演算について閉じており，かつ，空問題が判定可能であるからである．この正則保存性に基づくモデル検査法は，通常の文字列言語や木言語に対しては多くの研究がなされてきたが，データ値を扱う場合についての研究は十分でなかった．そこで本研究ではデータ値を扱う再帰プログラムを RPDS でモデル化し，RPDS に対するモデル検査法の自動化を目指して次のような研究を行った．まず，データ値を扱えるようにするため，データ言語が正則であることをレジスタオートマトンによって認識されることであると定義する．本研究ではまず，RPDS が正則保存性をもつこと，厳密には，「与えられた RPDS $P$に対し，任意の正則データ言語の$P$による順方向閉包が常に正則データ言語となること」を証明した．次に，仕様として線形時相論理式（LTL 式）$\psi$，モデルとして RPDS $P$が与えられたとき，モデル検査問題（$P$が$\psi$を満たすかどうか）が判定可能であること，およびその計算量を明らかにした．さらにフレッシュ性と呼ばれる条件を満たす RPDS の LTL モデル検査問題を通常の PDS の同問題に還元する手法を提案した．これらはいずれも論文誌 IEICE Transactions on Information and Systems に掲載された．

本研究での終盤では上記のアプローチに基づき，①仕様(検証性質)を表現する論理のクラス，および，②プログラムのモデルを表す変換系のクラスの双方に対して次のように拡張を行った．まず，①について，上のモデル検査問題ではプログラムのモデルはデータ値を扱えるが仕様（検証項目）を記述する LTL 式ではデータ値を直接記述できない．そこで，レジスタオートマトンに変換可能な凍結演算子付き LTL の部分クラスを見出した．さらにこれを進展させ，RA と能力等価な凍結演算子付き mu-計算の部分クラスを見出した．後者の研究発表に対しては，電子情報通信学会ソフトウェアサイエンス研究会研究奨励賞および電子情報通信学会ディペンダブルコンピューティング研究会若手優秀講演賞を同時受賞した．②については，RPDS を拡張してデータ語書換え系を定義しその正則保存性およびセキュリティ検証への応用について考察した．

以上はソフトウェア検証，すなわち，人手で実装したプログラムが仕様を満たすかどうかを判定する問題を扱っている．一方，仕様が与えられたとき，それを満たすプログラムを自動生成できればさらに望ましい．そのような動機付けから，「時系列に沿って順次与えられる入力に対してどのような出力列で反応すべきか」を表す仕様が与えられたとき，仕様を満たして動作するプログラム（実現プログラム）が存在するかどうかを判定し，もし存在するならばそのようなプログラムを自動生成する問題を，リアクティブ合成問題(reactive synthesis problem)とよぶ．特に，仕様がω-オートマトンや LTL 式で与えられたとき，仕様を満たす有限状態のリアクティブプログラムを（存在するならば）合成する問題は 1960 年代からの長い研究の歴史がある．このような過去の研究を踏まえ，本研究ではまず，プッシュダウンオートマトン(PDA)，実現プログラムがプッシュダウン変換器(PDT)の場合のリアクティブ合成問題の判定可能性について論じた後，仕様がレジスタ PDA（RPDA），実現プログラムがレジスタ PDT の場合についてリアクティブ合成問題の判定可能性を考察し，仕様が決定性可視 RPDA で与えられる場合は本問題が二重指数時間可解であることを示した．この成果は国際会議 18th International Colloquium on Theoretical Aspects of Computing (ICTAC 2021)に採択となった．

以上の問題設定はゲーム理論的に言えば，２人プレイヤー（システムと，システムに対して入力を与える環境)の間のいわゆるゼロ和ゲームであり，その意味で悲観的すぎる問題設定である．また環境は必ずしも単一のオブジェクトとは限らない．そこで，0〜$k$の($k$ + 1)人（システムをプレイヤー0とする）がそれぞれ個別の勝利目的をもつ多プレイヤー非ゼロ和ゲームを考える．このような問題設定においては必勝戦略に代わり，全プレイヤーの戦略の組の平衡性（ナッシュ均衡 NE はその典型例）を考える．本研究での終盤においては，このような考え方に基づく合理的自動生成問題（ただしデータ値は扱わない）に取り組み，確率的ゲームにおける種々のω-正則目的に対して，この問題の計算複雑さについて考察を行った．

上の応用研究と並行し，レジスタをもつ計算モデルに対する理論研究の深化として以下の成果を得た．レジスタオートマトン，レジスタ文脈自由文法，ボトムアップ型レジスタ木オートマトンの表現する言語クラスのそれぞれに対して，いわゆるポンプの補題を証明した．レジスタモデルを群論的に抽象化したノミナルモデルを用い，決定性上昇型ノミナル木オートマトンを定義し，それに対するアクティブ学習アルゴリズムを提案した．

（3）重み付き計算モデル

重み付きレジスタオートマトン（WRA）はレジスタオートマトンに重みを導入して拡張した計算モデルであり，重みによって遷移やレジスタ操作のコストを表現できる．また WRA は重み付き時間オートマトン（WTA）の拡張になっている．本研究では，WRA に対する最小重み実行問題を定義し，この問題の計算複雑さの解析とこの問題を解くアルゴリズムの開発を行った．その成果をまとめた論文は，国際会議 ICTAC 2019 にて Best Paper Award を受賞した．さらにその拡張版は海外論文誌 Theoretical Computer Science に採録された．

文脈自由文法の拡張である多重文脈自由文法に重みを導入した重み付き多重文脈自由文法(WMCFG)を提案し，WMCFG に関する基本問題の判定可能性や WMCFG の生成する重み付き言語クラスの閉包性についても考察した．この研究発表に対して，電子情報通信学会ソフトウェアサイエンス研究会研究奨励賞を受賞した．さらに，重み付き文脈自由文法における曖昧さの度合いに基づく表現能力の変化や階層性について考察した．

５．主な発表論文等

〔雑誌論文〕　計14件（うち査読付論文　14件／うち国際共著　1件／うちオープンアクセス　11件）

| | |
|---|---|
| １．著者名<br>Yoshiaki Takata, Ryoma Senda and Hiroyuki Seki | ４．巻<br>E105-D(9) |
| ２．論文標題<br>Reduction of Register Pushdown Systems with Freshness Property to Pushdown Systems in LTL Model Checking | ５．発行年<br>2022年 |
| ３．雑誌名<br>IEICE Transactions on Information and Systems | ６．最初と最後の頁<br>1620-1623 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transinf.2022EDL8030 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Ryoma Senda, Yoshiaki Takata and Hiroyuki Seki | ４．巻<br>923 |
| ２．論文標題<br>Complexity Results on Register Context-Free Grammars and Related Formalisms | ５．発行年<br>2022年 |
| ３．雑誌名<br>Theoretical Computer Science | ６．最初と最後の頁<br>99-125 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1016/j.tcs.2022.04.055 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Ryoma Senda, Yoshiaki Takata and Hiroyuki Seki | ４．巻<br>E104-D(12) |
| ２．論文標題<br>LTL Model Checking for Register Pushdown Systems | ５．発行年<br>2021年 |
| ３．雑誌名<br>IEICE Transactions on Information and Systems | ６．最初と最後の頁<br>2131-2144 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transinf.2020EDP7265 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Ryoma Senda, Yoshiaki Takata and Hiroyuki Seki | ４．巻<br>LNCS 12819 |
| ２．論文標題<br>Reactive Synthesis from Visibly Register Pushdown Automata | ５．発行年<br>2021年 |
| ３．雑誌名<br>18th International Colloquium on Theoretical Aspects of Computing (ICTAC 2021) | ６．最初と最後の頁<br>334-353 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1007/978-3-030-85315-0_19 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Ryoma Senda, Yoshiaki Takata and Hiroyuki Seki | 4．巻<br>E104-D(3) |
| 2．論文標題<br>Forward Regularity Preservation Property of Register Pushdown Systems | 5．発行年<br>2021年 |
| 3．雑誌名<br>IEICE Transactions on Information and Systems | 6．最初と最後の頁<br>370-380 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transinf.2020FCP0008 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Hiroyuki Seki, Reo Yoshimura and Yoshiaki Takata | 4．巻<br>850 |
| 2．論文標題<br>Optimal Run Problem for Weighted Register Automata | 5．発行年<br>2021年 |
| 3．雑誌名<br>Theoretical Computer Science | 6．最初と最後の頁<br>185-201 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1016/j.tcs.2020.11.003 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Xin Li, Patrick Gardy, Yu-Xi Deng and Hiroyuki Seki | 4．巻<br>35(6) |
| 2．論文標題<br>Reachability of Patterned Conditional Pushdown Systems | 5．発行年<br>2020年 |
| 3．雑誌名<br>Journal of Computer Science and Technology | 6．最初と最後の頁<br>1295-1311 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1007/s11390-020-0541-z | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>該当する |

| | |
|---|---|
| 1．著者名<br>Ryoma Senda, Yoshiaki Takata and Hiroyuki Seki | 4．巻<br>E103-D(3) |
| 2．論文標題<br>Generalized Register Context-Free Grammars | 5．発行年<br>2020年 |
| 3．雑誌名<br>IEICE Transactions on Information and Systems | 6．最初と最後の頁<br>540-548 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transinf.2019FCP0010 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Shuichi Sato, Shogo Hattori, Hiroyuki Seki, Yutaka Inamori and Shoji Yuen | 4．巻<br>28 |
| 2．論文標題<br>Automating Time-series Safety Analysis for Automotive Control Systems Using Weighted Partial Max-SMT | 5．発行年<br>2020年 |
| 3．雑誌名<br>Journal of Information Processing | 6．最初と最後の頁<br>124-135 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.2197/ipsjjip.28.124 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Bao Trung Chu, Kenji Hashimoto and Hiroyuki Seki | 4．巻<br>E102-D(10) |
| 2．論文標題<br>Quantifying Dynamic Leakage - Complexity Analysis and Model Counting-based Calculation - | 5．発行年<br>2019年 |
| 3．雑誌名<br>IEICE Transactions on Information and Systems | 6．最初と最後の頁<br>1952-1965 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transinf.2019EDP7132 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Hiroyuki Seki, Reo Yoshimura and Yoshiaki Takata | 4．巻<br>LNCS 11884 |
| 2．論文標題<br>Optimal Run Problem for Weighted Register Automata | 5．発行年<br>2019年 |
| 3．雑誌名<br>16th International Colloquium on Theoretical Aspects of Computing (ICTAC 2019) | 6．最初と最後の頁<br>91-110 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1007/978-3-030-32505-3_6 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Bao Trung Chu, Kenji Hashimoto and Hiroyuki Seki | 4．巻<br>- |
| 2．論文標題<br>On the Compositionality of Dynamic Leakage and Its Application to the Quantification Problem | 5．発行年<br>2019年 |
| 3．雑誌名<br>13th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2019) | 6．最初と最後の頁<br>1-8 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Ryoma Senda, Yoshiaki Takata and Hiroyuki Seki | 4．巻<br>- |
| 2．論文標題<br>Complexity Results on Register Pushdown Automata | 5．発行年<br>2019年 |
| 3．雑誌名<br>3rd Workshop on Software Foundations for Data Interoperability (SFDI 2019+) | 6．最初と最後の頁<br>1-5 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.48550/arXiv.1910.10357 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Anh V Vu and Mizuhito Ogawa | 4．巻<br>LNCS 11800 |
| 2．論文標題<br>Formal Semantics Extraction from Natural Language Specifications for ARM | 5．発行年<br>2019年 |
| 3．雑誌名<br>3rd World Congress on Formal Methods (FM 2019) | 6．最初と最後の頁<br>465-483 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1007/978-3-030-30942-8_28 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

〔学会発表〕　計13件（うち招待講演　1件／うち国際学会　1件）

| |
|---|
| 1．発表者名<br>Hiroyuki Seki |
| 2．発表標題<br>Quantitative Information Flow - An Introduction |
| 3．学会等名<br>3rd Workshop on Software Foundations for Data Interoperability (SFDI2019+)（招待講演）（国際学会） |
| 4．発表年<br>2019年 |

| |
|---|
| 1．発表者名<br>小出走，関浩之 |
| 2．発表標題<br>確率的Mullerゲームにおける非協調的合成問題 |
| 3．学会等名<br>組合せゲーム・パズルプロジェクト第16回研究集会（講演番号：16） |
| 4．発表年<br>2022年 |

１．発表者名
坂尾優斗，関浩之

２．発表標題
データ語書換え系の正則保存性とそのプロトコル検証への応用

３．学会等名
電子情報通信学会ソフトウェアサイエンス研究会（講演番号：SS2021-46）

４．発表年
2022年

１．発表者名
井上裕介，橋本健二，関浩之

２．発表標題
重み付き文脈自由文法の曖昧さ階層について

３．学会等名
電子情報通信学会コンピュテーション研究会（講演番号：COMP2021-31）

４．発表年
2022年

１．発表者名
中西凜道，高田喜朗，関浩之

２．発表標題
Pumping Lemmas for Languages Expressed by Computational Models with Registers

３．学会等名
2021年度 冬のLAシンポジウム（講演番号：16）

４．発表年
2022年

１．発表者名
大西晃，仙田涼摩，高田喜朗，関浩之

２．発表標題
レジスタオートマトンと能力等価な凍結演算子付きmu-計算の部分クラス

３．学会等名
電子情報通信学会ソフトウェアサイエンス研究会（講演番号：SS2021-17）

４．発表年
2021年

１．発表者名
大西晃，仙田涼摩，高田喜朗，関浩之

２．発表標題
レジスタオートマトンに変換可能な凍結演算子付き線形時相論理の部分クラス

３．学会等名
電子情報通信学会ソフトウェアサイエンス研究会（講演番号：SS2020-29）

４．発表年
2021年

１．発表者名
井上裕介，関浩之

２．発表標題
重み付き多重文脈自由文法とその性質について

３．学会等名
電子情報通信学会ソフトウェアサイエンス研究会（講演番号：SS2020-28）

４．発表年
2021年

１．発表者名
中西凜道，仙田涼摩，高田喜朗，関浩之

２．発表標題
レジスタをもつ計算モデルの表現する言語に対するポンプの補題

３．学会等名
電子情報通信学会ソフトウェアサイエンス研究会（講演番号：SS2020-26）

４．発表年
2021年

１．発表者名
Ryoma Senda, Yoshiaki Takata and Hiroyuki Seki

２．発表標題
LTL Model Checking for Register Pushdown Systems

３．学会等名
電子情報通信学会ソフトウェアサイエンス研究会（講演番号：SS2020-6）

４．発表年
2020年

１．発表者名
Ryoma Senda, Yoshiaki Takata and Hiroyuki Seki

２．発表標題
On the Regularity Preservation Property of Register Pushdown Systems

３．学会等名
2019年度 冬のLAシンポジウム（講演番号：S11）

４．発表年
2020年

１．発表者名
福田大地，関浩之

２．発表標題
モデル計数に基づく動的QIF解析法の提案と評価

３．学会等名
電子情報通信学会ソフトウェアサイエンス研究会（講演番号：SS2019-33）

４．発表年
2020年

１．発表者名
Reo Yoshimura, Yoshiaki Takata and Hiroyuki Seki

２．発表標題
Computing Optimal Weight in Weighted Register Automata and Related Decision Problems

３．学会等名
電子情報通信学会ソフトウェアサイエンス研究会（講演番号：SS2019-16）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
電子情報通信学会ディペンダブルコンピューティング研究会第9回研究会若手優秀講演賞，Oct 2022．（大西晃）
令和3年度電子情報通信学会ソフトウェアサイエンス研究会研究奨励賞，March 2022．（大西晃，仙田涼摩，高田喜朗，関浩之）
令和2年度電子情報通信学会ソフトウェアサイエンス研究会研究奨励賞，March 2021．（井上裕介，関浩之）
Best Paper Award, 16th International Colloquium on Theoretical Aspects of Computing, Nov 2019. (Hiroyuki Seki, Reo Yoshimura and Yoshiaki Takata)

## ６．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|
| 研究分担者 | 小川　瑞史<br>(Ogawa Mizuhito)<br>(40362024) | 北陸先端科学技術大学院大学・先端科学技術研究科・教授<br>(13302) | |
| 研究分担者 | 結縁　祥治<br>(Yuen Shoji)<br>(70230612) | 名古屋大学・情報学研究科・教授<br>(13901) | |
| 研究分担者 | 橋本　健二<br>(Hashimoto Kenji)<br>(90548447) | 名古屋大学・情報学研究科・助教<br>(13901) | |

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|
| 研究協力者 | 高田　喜朗<br>(Takata Yoshiaki)<br>(60294279) | 高知工科大学・情報学群・教授<br>(26402) | |

## ７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

## ８．本研究に関連して実施した国際共同研究の実施状況

| 共同研究相手国 | 相手方研究機関 |
|---|---|