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

平成　２９　年　　６　月　２７　日現在

機関番号：　３２６２９
研究種目：　若手研究(B)
研究期間：　2014～2016
課題番号：　２６７３０００７

研究課題名（和文）回路計算量の下界証明におけるアルゴリズム的手法の研究

研究課題名（英文）On Algorithmic Approaches to Proving Circuit Lower Bounds

研究代表者
脊戸　和寿（Seto, Kazuhisa）

成蹊大学・理工学部・講師

研究者番号：２０５８４０５６

交付決定額（研究期間全体）：（直接経費）　　2,600,000円

研究成果の概要（和文）：理論計算機科学分野における最大の未解決問題であるP vs. NP問題の解決に向け，充足可能性問題のアルゴリズム設計による回路計算量の下界証明の研究を行った．本研究では閾値素子を一定数含む定数段数論理回路の充足可能性問題に対して，全探索よりも真に高速なアルゴリズムを設計することに成功した．また付随する結果として，最大充足可能性問題の新たなアルゴリズムが得られた．

研究成果の概要（英文）：P versus NP problem is the most important problem in theoretical computer science. Our ultimate goal is to solve this problem. Toward this goal, we study on the connection between fast satisfiability algorithms and circuit complexity. In this research, we gave the first algorithm that solves the satisfiability problem of constant depth circuits with a few symmetric gates. It runs faster than brute force search. In addition, we gave a new algorithm for the maximum satisfiability problems.

研究分野：　情報学基礎理論

キーワード：　計算量理論　充足可能性問題　回路計算量　閾値回路

１．研究開始当初の背景

理論計算機科学における最大の未解決問題は P vs. NP 問題である．この問題はリーマン予想など数学上の重要な６つの未解決問題とともに，クレイ数学研究所によりミレニアム懸賞金問題に指定されている．この問題の解決に向け，これまで様々な取り組みが行われてきたが，未だ解決には至っていない．

代表的な取り組みの１つが回路計算量の研究である．回路計算量とは与えられた論理関数を計算する論理回路を構成する際に必要となるサイズや段数を定量的に評価する学問である．扱う素子の種類や回路のサイズ，段数に応じて，様々な回路計算量のクラスが定義される．最も重要な回路クラスが，PSIZE(=P/poly)である．これは，2 入力の AND，OR，単入力 NOT 素子を用いた段数制限なしの多項式サイズ回路で計算可能な論理関数の集合（＝クラス）である．このクラスは P vs. NP 問題と密接な関係を持っており，もし，クラス NP に存在するある論理関数が P/poly で計算できないなら，P と NP は分離されることが知られている．

回路計算量を用いた研究は，これまで数多く行われてきたが，P vs. NP 問題の解決への道は遠い．事実，非常に限定された回路（定数段数回路や単調回路等）でしか，NP に含まれる関数が計算不可能であることは示されていない．それどころか，Natural Proof という障壁の発見により，これまでの証明法では回路計算量理論の枠組みでは P vs. NP を解く事は不可能であるということが示唆されている．さらに，NP より大きなクラスである NEXP に対しても，同じ状況が続いていた．

しかし，近年，Natural Proof を打開する可能性のある手法が Ryan Williams によって提案された．それが論理回路の充足可能性問題の高速アルゴリズム設計である．論理回路の充足可能性問題とは，与えられた論理回路の出力が１となるような入力変数への割当が存在するか？という問題である．この問題を解く，自明なアルゴリズムは全探索であり，入力変数への 0/1 割当をすべて試すことである．

さらに，Ryan Willams は，実際に ACC^0 という計算量クラスに対して，それに対応する論理回路の充足可能性問題を解く非自明なアルゴリズムを開発し，ACC^0 と NEXP とを分離に成功した．これは大きなブレイクスルーとなり，近年，この手法の研究が活発になり，得られた結果は，STOC や FOCS，SODA，CCC といった理論計算機科学において権威のある国際会議に採択されている．

２．研究の目的

本研究の最終目的は制限のない多項式サイズの論理回路が計算可能なクラスと NEXP の分離である．そのための最初の段階として，本申請では，既存結果をさらに強めることを目標とする．本申請では，TC^0 と呼ばれる回路計算量のクラスを対象とする充足可能性問題の非自明なアルゴリズム開発の研究を行う．

TC^0 とは素子として，入力制限のない AND，OR，単入力 NOT に入力制限のない閾値素子（入力線に閾値以上の１が入力されれば１を出力する素子）を用いた定数段数の多項式サイズ回路で計算可能な論理関数のクラスである．本研究開始時には，北米チームの既存研究により，TC^0 を線形サイズかつ段数を 2 段に制限した論理回路の充足可能性問題に関しては全探索よりも高速なアルゴリズムが設計されていた．

また，本研究では最大充足可能性問題のアルゴリズム設計も目標とする．最大充足可能性問題とは与えられた変数の論理和からなる節の集合を最も多く充足させる変数割当を発見する問題である．この問題は TC^0 回路の特殊ケースであり，一段目を OR，二段目を閾値素子に限定した TC^0 回路の充足可能性問題となる．最大充足可能性問題については，重みに制限のない節の個数が多項式個のインスタンスに対して，全探索よりも高速に答えを導きだすアルゴリズムを設計することを目標とする．

論理関数を計算するモデルには論理回路以外にも分岐プログラムというものがある．分岐プログラムの充足可能性問題も本研究の対象とする．分岐プログラムの充足可能性問題とは，分岐プログラムの計算開始ノードから 1 を出力するノードに至るパスのうち，変数割当に矛盾のないパスが存在するかどうかを判定する問題である．この問題に対する全探索よりも真に高速なアルゴリズム設計によって，NEXP と NC^1 という計算量クラスの分離が可能であることも知られている．この計算量クラスの分離も未だ知られていない．そのため，分岐プログラムの充足可能性問題も本研究の対象とする．特に，本研究では計算開始ノードから出力ノードに至るどのパスにおいても，各変数が高々k 回しか現れないという制限をもつ k 回読み分岐プログラムの充足可能性問題を解く高速アルゴリズムの設計を目標とする．

これらの研究を通して，これまでの手法とは異なるアルゴリズムの設計による回路計算量の下界証明手法の可能性を追求することも本研究の目的となる．

３．研究の方法

本研究は理論研究を中心として行うため，様々な文献の調査から始め，最新のアルゴリズム設計技法や解析手法等の習得を中心に，研究目的の達成に向け研究を行う．個人での研究のみでは研究の停滞も予想されるため，共同研究者とのディスカッションも積極的に行うことで，できる限り停滞期を回避するように研究を進めていく．

また近年、計算機での実験結果を利用して未解決問題を解決した例は少なくない。特に充足可能性問題に関しては，非常に高速なソルバーが存在しているため，それを利用することで，難しいインスタンスの発見や必要な性質が存在するかの自動証明を行う．また，数式解析ソフトの利用により，アルゴリズムのパラメーターの最適値等を計算することも考え，これらの情報を理論的解析に活かす．

最新の解析手法やアルゴリズム設計手法の知見の獲得には，国内外で行われる国際会議やセミナーも利用する．本研究により得られた結果は，国内外で開催される会議，学術誌，ホームページ等を通して積極的に公表する．

４．研究成果

本研究により大きくわけて５つの結果を得ることができた．これらの結果はすべて査読付き雑誌論文または査読付き国際会議で発表を行った．

（1）対称素子を一定数含む定数段数論理回路の充足可能性問題に対する全探索よりも高速なアルゴリズムの設計と下界証明（学会発表 1）

TC^0 回路において対称素子を一定数含んだ回路の充足可能性問題に対して，全探索よりも高速なアルゴリズムを設計した．その解析の過程でこの論理関数に対して平均的に計算が難しい論理関数を示した．これまで対称素子が含まれる論理回路の下界証明に用いられていた通信複雑さの理論を用いた証明方法とは異なる新たな証明方法を与えた．アルゴリズムには Greedy Restriction という最も多く回路に現れる変数から順に 0/1 を割り当てていく手法，Beame，Impagliazzo，Srinivasan らによって開発された定数段数の深さを圧縮していく手法，動的計画法の 3 つの技法が用いられている．

回路計算量の下界証明には，Andreev 関数を一般化した関数を用いている．そのほかにも真理値表が与えられたときに，自明なサイズの論理回路よりも真にサイズの小さい回路を出力するアルゴリズムも示している．

（2）多項式サイズの最大充足可能性問題に対する全探索より真に高速なアルゴリズムの設計（学会発表 1）

節数が入力変数の個数の多項式かつ節への重みの制限が限りなく無制限に近い最大充足可能性問題に対して，全探索よりも真に高速なアルゴリズムを設計した．このアルゴリズムは（1）で用いた手法を最大充足可能性問題に特化させたことで得られた結果である．これまで，任意の多項式サイズのインスタンスを扱えるアルゴリズムは知られていなかった．

（3）線形サイズの最大充足可能性問題に対する全探索より指数的に高速な多項式領域アルゴリズムの設計（雑誌論文 3，学会発表 2,4）

節数が入力変数の個数の線形で抑えられる最大充足可能性問題に対して，全探索よりも指数的に高速なアルゴリズムを設計した．これは，これまでの多項式領域しか用いないアルゴリズムの計算時間を改良した結果である．指数領域を用いれば同じ計算時間を達成している結果はあるが，本アルゴリズムが多項式領域しか用いない点で，既存アルゴリズムを改良していると言える．本アルゴリズムは（1）と同様の Greedy Restriction と，Schuler による充足可能性問題の解を保証したまま各節内に含まれる変数の数を減らす Width Reduction という手法を最大充足可能性問題に拡張した手法を組み合わせることで実現することに成功した．

（4）k 回読み分岐プログラム及び各種制限された分岐プログラムの充足可能性問題に対する全探索より指数的に高速なアルゴリズムの設計（雑誌論文 1,2，学会発表 3）

k-indexed binary decision diagram と Oblivious Read-Twice Branching Program いう制限された分岐プログラムに対する充足可能性問題を解く全探索よりも指数的に高速なアルゴリズムを設計した．ただし，これらの結果は各分岐プログラムのサイズが変数の数の線形のみを対象としている．

さらにこれらの結果を進展させることで，k 回読み分岐プログラムの充足可能性問題に対しても全探索よりも指数的に高速なアルゴリズムを設計した．こちらは任意の多項式サイズのインスタンスを扱うことができる．このアルゴリズムは Borodin，Razborov，Smolensky による k 回読み分岐プログラムの分解法を用いることで設計することに成功した．この結果は現在国際会議に投稿準備中である．

（5）証明複雑さにおけるサーベイ論文の発行（雑誌論文 4）

証明の複雑さとは与えられた論理式が恒真式であることを与えられた特定のルールのみを用いて証明する際に，証明に必要となるルールの回数を定量的に評価する分野である．これらのルールの違いにより，様々な証明システムが考えられる．証明複雑さは P vs. NP 問題の解決にも非常に重要な役割を担っており，もし任意の証明システムで多項式回のルール適用で証明できない恒真式が存在すれば，NP と coNP が分離されることになり，その結論をもって P と NP が分離されるということが知られている．

また，証明の複雑さの分野で用いられる技法は充足可能性問題のアルゴリズムに応用されていることが多く，本研究とは関連性が深い．事実，証明システムの 1 つである Resolution という技法は k-CNF 充足可能性問題を解くための前処理として用いられている．Resolution を用いた証明システムに関する研究は数多く行われているため，それらについての調査を行いサーベイ論文としてまとめた．

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 4 件）

[1] Atsuki Nagao, Kazuhisa Seto, and Junichi Teruyama.
A Moderately Exponential Time Algorithm for k-IBDD Satisfiability.
Algorithmica, to appear.

[2] Kazuhisa Seto and Junichi Teruyama.
An Exact Algorithm for Oblivious Read-Twice Branching Program Satisfiability.
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E99-A(6):1019–1024, 2016.

[3] Takayuki Sakai, Kazuhisa Seto, and Suguru Tamaki.
Solving Sparse Instances of Max SAT via Width Reduction and Greedy Restriction.
Theory of Computing Systems,57(2):426–443, 2015.

[4] Kazuhisa Seto
An Introduction to Lower Bounds on Resolution Proof Systems.
Interdisciplinary Information Science, 21(4):307–328, 2015.

〔学会発表〕（計 4 件）

[1] Takayuki Sakai, Kazuhisa Seto, Suguru Tamaki, and Junichi Teruyama.
Bounded Depth Circuits with Weighted Symmetric Gates: Satisfiability, Lower Bounds and Compression.
In Proceedings of the 41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016), LIPICS 58, 82:1–82:16, August, 2016.

[2] Takayuki Sakai, Kazuhisa Seto, Suguru Tamaki, and Junichi Teruyama.
Improved Exact Algorithms for Mildly Sparse Instances of Max SAT.
In Proceedings of the 10th International Symposium on Parametrized and Exact Computation (IPEC 2015), LIPICS 43, pp.90–101, September, 2015.

[3] Atsuki Nagao, Kazuhisa Seto, and Junichi Teruyama.
A Moderately Exponential Time Algorithm for k-IBDD Satisfiability.
In Proceedings of the 14th Workshop on Algorithms and Data Structures (WADS 2015), LNCS 9214, pp.554–565, August, 2015.

[4] Takayuki Sakai, Kazuhisa Seto, and Suguru Tamaki.
Solving Sparse Instances of Max SAT via Width Reduction and Greedy Restriction.
In Proceedings of the 17th International Conference on Theory and Applications of Satisfiability Testing (SAT 2014), LNCS 8561, pp.32–47, July, 2014.

〔その他〕
ホームページ
http://www.ci.seikei.ac.jp/seto/index.html

６．研究組織
(1)研究代表者
脊戸　和寿（Kazuhisa Seto）
成蹊大学・理工学部・講師
研究者番号：20584506