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２５年６月５日現在

機関番号：１２６１２
研究種目：基盤研研究（C）
研究期間：２０１０～２０１２
課題番号：２２５００００１２
研究課題名（和文）命題論理の証明の複雑さに関する計算量理論からの解析

研究課題名（英文）Propositional Proof Complexity: Analysis from Computational Complexity Perspectives

研究代表者
垂井　淳（TARUI JUN）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：００２６０５３９

研究成果の概要（和文）：鳩ノ巣原理の証明複雑さに関して，ストリーム計算における重複要素発見問題の領域計算量および通信計算量の解析を応用して新結果を得ることに成功した。開発し用いた手法はさらなる応用が期待できる。証明の複雑さと密接に関連する回路計算量に関して，ノイズ下での AC0 関数の学習アルゴリズムの拡張，5n より大きい回路サイズ下界の証明に立ちふさがる障害の解析，パリティを計算するサイズ n^2 フォーミュラの本質的一意性などの結果を与えることができた。

研究成果の概要（英文）：We have obtained a new result about proof complexity of the pigeonhole principle by analyzing the space complexity and the communication complexity of findig a duplicate in a stream. Our new proof method is interesting in its own. For circuit complexity, which is closely related to proof complexity, we have (1) extended a noise-tolerant learning algorithm for AC0 functions, (2) have identified a concrete barrier for provindg a circuit-size lower bound bigger than 5n, and (3) have shown that, for n a power of 2, a smallest DeMorgan formula computing Parity of n Boolean variables is essentially unique.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	800,000	240,000	1,040,000
2011 年度	900,000	270,000	1,170,000
2012 年度	800,000	240,000	1,040,000
年度			
年度			
総　計	2,500,000	750,000	3,250,000

研究分野：計算量理論
科研費の分科・細目：情報学・情報学基礎
キーワード：計算量理論、計算の複雑さ、証明の複雑さ、ストリーム計算

１．研究開始当初の背景

（１）Resolution は命題論理式に対する証明系のなかでもっともよく知られているもののひとつである。任意の充足不可能な CNF 式に対して、その充足不可能性を Resolution によって証明できる。命題論理式 P が恒真であることは、P の否定が充足不可能であることと同値であり、また、任意の論理式は補助論理変数の追加により同値な CNF 式として表現できるので、Resolution は恒真命題論理式に対する完全で健全な証明系といえる。鳩

の巣原理を表現する命題論理式 P(n)について、P(n)の Resolution における最小の証明の長さは n に関して指数的に増大することが知られている。また、n 変数で 6n 個の clause からなるランダムな 3-CNF 式は高確率で充足不可能となるが、充足不可能性の Resolution における最短の証明の長さが高確率で exp(cn)以上となることが知られている。

（2）計算量クラスに関する２つの予想 NP≠coNP と P≠NP はともに広く信じられているものだが前者のほうが後者より強い。ともに現時点では解決が極めて困難と思われるが、より強いほうの前者の予想の分析から意味のある情報が得られる可能性は十分ある。NP≠coNP 予想について考えるひとつの自然なアプローチは、次に述べるような観点から証明の複雑さの解析となる。恒真な論理式の集合と充足不可能な論理式の集合はともに coNP 完全である。一方で、任意の効率的証明系において多項式サイズの証明をもつもの全体は NP に属する集合となる。したがって、広く信じられているように NP≠coNP であるならば、Resolution のような弱い証明系に限らず、任意の効率的証明系において最短証明の長さが超多項式となる恒真な論理式や充足不可能な論理式が存在する。

（3）このような観点による計算量理論の研究者による証明の複雑さに関する研究は２０年以上前より地道に続いてきたが、Pudlak, Krajicek, Razoborov らによる結果をきっかけとする活性化がはじまったのは数年前からである。計算量理論の本質的前進のために証明の複雑さの研究が重要であるという認識が広がりつつある。毎年夏に Krajicek と Pudlak がいるチェコ・プラハにおいて Proof Complexity の研究集会が開かれており、申請者は２００８年の集会に参加した。国内に関しては、申請者は計算量理論と数学基礎論の研究者と学生約３０名が参加した研究集会を２年半前に開催するなどして活性化を図ってきたが、関連研究は活発とは言いがたい。

２．研究の目的

（1）本研究の目的は、計算量理論にとって重要な設定における証明の複雑さ(proof complexity)の解析である。計算量クラス coNP に関する NP≠coNP 予想は、P≠NP 予想より強い予想であり、すべての効率的証明系において、恒真であることの最短の証明が長くなってしまう恒真な命題論理式が存在することを主張している。本研究では、制限された証明系についてこのような論理式の存在を実際に示すこと、すなわち、証明の長さに関するよい下界を与えることを達成したい。ランダムな k-CNF が充足不可能性であることの証明の複雑さも解析する。これら２つの課題に関して申請者が既にもつシードを展開させ、申請者が豊富な実績をもつ回路計算量における手法および代数的手法・確率的手法・組合せ論的手法による解析を進める。

（2）研究課題１ Frege より弱い命題論理証明系の解析： 命題論理に対する証明系として、Frege および Extended Frege という２つの自然なものがあるが、証明の長さに対する超多項式の下界をこれらの体系について示すという未解決問題は現時点では非常に困難であると認識されている。本研究では Frege 証明系に対して制限を加えて得られる証明系を解析する。具体的には、証明長に対する新しい下界を与えることと証明系に対する擬似ランダムネス生成器を構成してみせることを目指す。ブール関数の回路計算量における手法の拡張が、証明系の解析において有力な道具となっており、申請者の回路計算量における豊富な研究実績を生かしたい。また、申請者は通信計算量の手法によりストリーム計算の限界を示すことに最近成功した（J.Tarui：Finding a Duplicate and a Missing Item in a Stream. LNCS vol. 4484: Proc. of TAMC07,128--135, 2007）。そこでの予期せぬ副産物として、通信計算量を用いて命題論理の証明の長さに対する下界を導出することにも成功した。申請者の知る限り、証明の複雑さの解析に通信計算量が使われた研究は今までにない。この申請者オリジナルと思われる部分をさらに展開させたい。

（3）研究課題２ ランダム k-CNF の充足不可能性証明の複雑さ解析： n 変数で m 個の clause からなる k-CNF をランダムに生成した場合、$m \geq ckn$ ならば高確率で充足不可能となる。k=3 の場合、すなわちランダム 3-CNF については、たとえば 6n 個の clause をもつものは高確率で充足不可能となる。（実際の閾値は約 4.2n と予想されている。）本研究では、高確率で充足不可能となるランダム k-CNF に対して、その充足不可能性を証明する手間について解析する。ランダム 3-CNF については、$m \geq n1.4$ の場合、多項式サイズ証明が存在することが知られている。さらに、$m \geq n1.5$ の場合、多項式時間アルゴリズムによって証明を見つけることができることが知られている。(U. Feige and E. Ofek: Easily refutable subformulas of large random 3CNF formulas. Theory of Computing 3(1), 25--43, 2007; A.

Coja-Oghlan et al：On smoothed k-CNF formulas and the Walksat algorithm. SODA09: 451-460, 2009） 本研究では、これらの結果を clause の数 m がより小さい場合について拡張することを目指す。CNF を表現したハイパーグラフに対するスペクトル解析により充足不可能性を証明するというのが基本方針である。申請者は、この課題に深く関連する T. Tao（２００６年フィールズ賞）の問題に対してはアルゴリズムを与えることに成功した。このアルゴリズムを拡張させ深化させたい。(Tao の問題と申請者のアルゴリズムおよび両者の議論は、最近書籍化もされている Tao のブログ（2008 年 2 月）にて公開されている。”terence tao tarui”による検索でトップヒットする。)
逆に、clause の数 m が n に関して linear な場合、たとえば m=6n の場合については、ランダム 3-CNF は高確率で充足不可能となるが、充足不可能性の効率的証明は不可能と予想されている（上記 Feige-Ofek2007）。本研究ではこの予想と計算量理論における他の困難性予想の関係についても解析する。

３．研究の方法

主たる研究方法は理論的考察である。平成２２年度は、２つの研究課題それぞれに対して申請者が既にもつシードを発展させる。具体的には、Frege より弱い命題論理証明系の解析については、通信計算量の手法を拡張させて新たな結果を得ることを目指し、ランダムな k-CNF の解析においては、ハイパーグラフのスペクトル解析により充足不可能性を証明するという方針のもとにアルゴリズム設計を進める。平成２３年度以降は、命題論理の証明系の解析に関しては、擬似ランダムネス生成器の構成と代数的証明系の解析に取り組み、ランダム k-CNF に関しては、多項式サイズ証明が存在しないという予想の分析を進める。

４．研究成果

（１）本研究課題は回路計算量と密接な関係をもつものだが，回路計算量に関する研究結果として，Parity を計算する最小サイズフォーミュラは本質的に一意であるという結果を代表者単著の論文（Theoretical Computer Science 2010）として発表した。

（２）本研究課題は回路計算量と密接な関係をもつものだが，明示的ブール関数 f の回路計算量、すなわち f を計算する論理回路の最小サイズについて現在知られている最大の下界は Iwama ら(2005)によって与えられた 5n である。Iwama らの手法をさらに精密化することでより大きな下界を得ることができるのではないかという予想もあった。我々はこの予想を否定すること、すなわち、Iwama の枠組みでは 5n より大きな下界を示すことが不可能だ示すことに成功し、この結果を天野・垂井の共著として学術雑誌論文（Theoretical Computer Science 2011）として発表した。

（３）クラス ACO に属するブール関数に対するノイズ下での効率的学習：ACO 関数に対する効率的学習については、Linial ら(1993)がブール関数に対する調和解析を用いて肯定的結果が示された。この結果のノイズ確率が既知の場合への拡張が Bshouty ら(2002)によって示された。我々はこれをさらに拡張し、ノイズ率が未知の場合も効率的学習が可能であることを宮田・富田・垂井の共著学術雑誌論文（Theoretical Computer Science 2011）として発表した。

（４）Large-Scale Distributed Computation をテーマとする湘南会議において、ストリームにおける重複発見の計算複雑さについて招待講演をした。この問題は命題論理において非常によく研究されている鳩の巣原理に密接に関連しているものである。決定的計算の場合については、通信計算量の問題にいったん帰着し、さらにそれを回路計算量の問題に帰着させるという興味深い手法により、よい下界を与えることに成功しており、乱択計算の場合の計算複雑さの決定が未解決問題として残っている。このトピックと結果については、平成２３年１１月にデンマークのオーフス大を訪問した際にも講演した。本トピックについては，研究代表者の２００７年論文［J. Tarui: Finding a Duplicate and a Missing Item in a Stream. LNCS vol. 4484: Proc. of TAMC07, 128--135, 2007］において，ストリーム計算の領域計算量に対する下界を与えるために用いた手法を拡張し，その拡張によって命題論理の証明複雑さ，特に，鳩ノ巣原理の証明複雑さに関する新結果を得ることに成功したが，この拡張を新しい結果として得ることに成功した。この新結果は以上の会議論文の結果を合わせて雑誌論文として発表準備中である。

（５）コンピュテーション研究会における招待講演として，２０１０年夏に注目を集めた DeolalikarによるP≠NPを主張する論文に関して，論文が多くの問題を抱えていることを説明しつつこの論文のアプローチの可能性と限界について解説した。

（６）数学基礎論における証明論の研究者が主な参加者である研究集会『証明論と複雑性』（京大数理解析研究所，２０１２年９月１２日～１４日）において「計算の複雑さと証明の複雑さ」と題する招待講演を行った。本課題の研究を通じて得られた知見をふまえつつ重要な未解決問題に対する現状を説明し，証明論と計算量理論の学際領域研究の重要性も説明した。この学際領域の研究を促進する効果ももつ講演ができたと思う。

（６）２０１３年３月１３日から１９日の期間に開催された Tokyo Complexity Workshop および３つのサテライトワークショップについてプログラム委員長をつとめた。証明の複雑さの関係では，Pavel Pudlak と Ryan O'Donnell による招待講演を企画した。彼らとの個別議論により証明の複雑さと近似アルゴリズムにまたがる新たな重要問題を特定することもできた。また，彼らを含む研究者たちとの議論によって，Positivstellensetz に関連する問題に関して部分的結果を得ることができた。

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３件）

① K. Amano and J. Tarui: A Well-Mixed Function with Circuit Complexity 5n: Tightness of the Lachish-Raz-type Bounds. Theoretical Computer Science, vol 412, 1646—1651, 2011. 査読有. DOI: 10.1016/j.tcs.2010.12.040

② A. Miyata, J. Tarui, and E. Tomita: Learning Boolean Functions in AC0 on Attribute and Classification Noise. Theoretical Computer Science, vol 412, 4650 – 4660, 2011. 査読有. DOI: 10.1016/j.tcs.2011.04.047

③ Jun Tarui: Smallest Formulas for Parity of 2^k Variables Are Essentially Unique. Theoretical Computer Science, vol 411, 2623 – 2627. 2010. 査読有. DOI: 10.1016/j.tcs.2010.03.022

〔学会発表〕（計３件）

① 垂井淳：計算の複雑さと証明の複雑さ（招待講演），研究集会「証明論と複雑性」，2012 年 9 月 12 日～14 日（発表：9 月 13 日），京大数理研究所．（In: 数理解析研究所講究録，vol 1832,「証明論と複雑性」p. 1，京大数理研究所 2013 年）

② Jun Tarui: Complexity of Finding a Duplicate in a Stream（招待講演），NII Shonan Meeting: Large-scale Distributed Computation，2012 年 1 月 12 日～15 日（発表：1 月 13 日），湘南国際村センター

③ 垂井淳：Deolalikar の P≠NP 論文をめぐって（招待講演），電子情報学会・コンピュテーション研究会，2010 年 10 月 15 日，東北大学青葉山キャンパス．（In: 信学技法 COMP2010-38, p.47, 2010）

〔その他〕

垂井淳：「計算量理論のいろんな話題」，計算量理論秋学校講演,2012 年 9 月 24 日--26 日, 熱海.

ホームページ：
www.jtlab.ice.uec.ac.jp/~tarui

６．研究組織

(1)研究代表者：垂井　淳（TARUI JUN）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：００２６０５３９