様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月 １５ 日現在

機関番号：１２６１２
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５３３００１０

研究課題名（和文）ブール関数の多項式表現を用いた回路計算量の解析

研究課題名（英文）Study of Circuit Complexity Using Polynomial Representations of Boolean Functions

研究代表者
垂井　淳（Tarui, Jun）

電気通信大学・情報理工学（系）研究科・准教授

研究者番号：００２６０５３９

交付決定額（研究期間全体）：（直接経費）　　2,700,000円

研究成果の概要（和文）：n個の頂点とm本の辺をもつ無向グラフに対して，n+o(n)ビットの記憶領域だけを用いて深さ優先探索が可能であり，有向非巡回グラフの場合は，n/[exp(Omega(root(log n)))]ビットの記憶容量だけを用いて深さ優先探索が可能であることがわかった．深さ優先探索以外の複数の問題についても同様の結果を得た．指数時間予想と「この問題をnの3乗より早くは解けない」といった予想の関連性が最近明らかになりつつあるが，我々の結果は，「記憶領域量がnの(1-epsilon)乗しかない場合は計算は不可能」といった予想と他の問題の領域計算量との関係解明の重要性を示唆している点が特に興味深い．

研究成果の概要（英文）：We have shown that for an undirected graph with n vertices and m edges, Depth-First Search (DFS) is possible using n+o(n) bits of memory. For a directed acyclic graph, DFS is possible using n/[exp(Omega(root(log n)))] bits of memory. We have also obtained similar results for several other graph problems. Recently, researchers are finding more and more interesting connections between Exponential-Time Hypothesis (ETH) and the time complexity of polynomial-time solvable problems. For example, it is now known that ETH implies that a truly sub-cubic algorithm does *not* exist for a certain graph problem. Our results above seem to suggest that we should investigate space-complexity analogues of this phenomena: What are the consequences of the conjecture "Problem A requires linear space" ?

研究分野：計算量理論

キーワード：計算量

１．研究開始当初の背景

（１）２０１０年に計算量理論における大きなブレークスルーが Ryan Williams によってもたらされた．すなわち，Williams は，ACC 回路と呼ばれる弱いと思われる計算モデルにおける計算量が超多項式となることを証明し，計算量理論において 20 年間未解決課題となっていた「ACC 問題」の解決に成功した．ACC 問題は，計算量理論における最重要未解決問題である「P vs NP 予想」の解決・解析への道筋において，「ここから先への進み方がわからない」という既知研究の限界を浮き彫りにする問題だった．Williams による ACC 問題解決の鍵となった結果のひとつは，本研究課題代表者の ACC 回路計算を整数係数低次多項式を用いて特徴づける結果（R. Beigel and J. Tarui: "On ACC", Computational Complexity, 350-364, 1994）であった．

（２）低次多項式表現を用いる一方で，Williams は対角線論法や Easy Witness と呼ばれる構造的計算量理論の手法も巧妙に組み合わせて用いた. ACC 問題を解決することと並行して，Williams は，k-SAT を解くには指数時間が必要であるという「指数時間予想」と多項式時間で解ける問題の計算量との間に密接な関係があるという非常に興味深い結果を示すことにも成功した．

（３）本研究課題では，上述の Williams の結果をふまえて，手法・結果の拡張と関連問題の研究を進めることをテーマとした．

２．研究の目的

本研究課題の目的は，主に次の２つのアプローチにより，上述の Williams の結果・手法を展開させることであった．

（１）指数時間予想（Exponential Time Hypothesis (ETH))と多項式時間計算可能な問題の間に発見された関連をふまえた領域計算量における類似の探求：

William 結果の副産物として，特に興味深いもののひとつは，指数時間予想（ETH)と多項式時間計算可能な問題群との関係の発見である．たとえば，指数時間予想，あるいは，強指数時間予想を仮定すると，いくつかのグラフに関する問題を n の 3 乗より早い時間で解くことができないことがわかった．

時間計算量の世界ではこのような現象が発見されたが，領域計算量の世界において，似たような現象があるのかについては，あまり研究されてきていない．そもそも，指数時間予想の類似物を領域計算量について考えた研究がなかったと思われた．

本課題では，指数時間予想とそれをとりまく現象に関して，領域計算量での類似物・類似現象について解明を進める．

（２）Williams の計算量クラス ACC に関する結果における手法の深化：

Williams の証明手法は充足可能性判定アルゴリズムと対角線論法を巧妙に組み合わせたものであった．この手法の枠組みについてさまざまな角度から分析する．

一方で，回路の充足性判定アルゴリズとして自明なものより少し早いアルゴリズムを設計することと回路のサイズに対する下界を証明するというふたつのことの間に duality とも言うべき関係があることが明らかになりつつあるが，正確な関係はまだまだはっきりしないので，この duality 現象についての解明を進めたい．

もう一方で，Williams の ACC vs NEXP 結果について，対角線論法などをまったく用いない証明があってもおかしくない．または，あるアプローチでの別証明は厳密な意味で困難なのかもしれないが，そうだとすれば何が障害なのかわかっていない．たとえば，通信計算量を用いて, Williams とはまったく別の証明を与えることはできないのか？それが本質的に難しいのだとしたら，なぜ難しいかということを障害を特定して明らかにできるか？このような課題の解明を進めることにより Williams 手法に対する理解を深化させたい．

３．研究の方法

（１）領域計算量の世界における指数時間予想の類似を解明していく方法は，次の２つとなる．

(a) まず，複数の具体的問題に対してその領域計算量の上界と下界を解析していくことになる．特に，上界についてどこまで小さくできるかが重要となる．アルゴリズムの設計においては，時間計算量を抑える方法，すなわち，高速なアルゴリズムを与える方法については多くが知られているが，記憶領域を節約する方法については相対的にそれほど知られていないので，新手法の開発にも取り組むことになる．

(b) 複数の具体的問題について領域計算量の解明が進んだら，問題の間の関係，特に，「問題 A が小さな記憶領域領域で解けてしまえば, 問題 B,C,D,E も小さな記憶領域で解けてしまう」といったことが示せるような問題 A はあるのか、ということについての解析を進めることになる．

（２）Williams の枠組みの分析，および，別ルートでの別証明の可能性探求の方法は次の２つとなる．

（a）充足可能性判定高速アルゴリズムの存在と回路サイズ下界証明の duality について全貌解明をめざすという立場からの研究では，本質的には，「下界を証明するということは必然的にある種のアルゴリズムを与えることでもあるのか？」について考えていくことになる．Razborov-Rudich による natural proof という枠組みについても，Williams 結果をふまえた再考が必要になる．

（b）もう一方の Williams 証明とはまったく異なる別証明を探る，または，そのルートの障害を特定しようとするためには，Williams 証明は natural か，あるいは，naturalizable かということの検討を含む考察が必要となる．

４．研究成果

（１） 深さ優先探索に関する結果

グラフに関する最も基本的な操作である深さ優先探索（Depth-First Search，DFS）の領域計算量について解析し，ここまでの節約が可能であるという次のような領域計算量に対する上界の結果を与えることに成功した．グラフは，n 個の頂点と m 本の辺をもつとする．

(a)無向グラフに対して，O(n)ビットの記憶領域（メモリー）だけ用いて，O(m log n)時間で DFS が可能である．

(b)別のアルゴリズムを用いると，無向グラフに対して，n+o(n)ビットの記憶領域だけ用いて，多項式時間での DFS も可能である．

(c)有向非巡回グラフに対しては，n/(2^Omega(root(log n)))ビットの記憶容量を用いて，多項式時間で DFS が可能である．

(d)無向木に対する DFS は，O(log n)ビットの記憶容量を用いて線形時間で可能である．

(e) O(1)-サイズのフィードバックセットをもつグラフに対する DFS は O(log n)ビットの計算量で可能である．

以上の我々の結果で鍵として用いているものは２つの既知結果である．ひとつは，有向グラフ G と 2 頂点 s，t が与えられて，グラフ G において s から t へのパスが存在するかの判定，すなわち，到達可能性判定問題に対する既知で最も少ない記憶領域を用いる Barnes らによるアルゴリズムである（G. Barnes et al: A Sublinear Space, Polynomial Time Algorithm for Directed s-t Connectivity，SIAM J. Comput.，1998）．

もうひとつは，無向グラフにおける同様の問題は領域計算量 O(log n)で解けるという Reingold による有名な結果である（Omer Reingold: Undirected Connectivity in Log-Space，Journal of the ACM 2008）．

深さ優先探索の性質の解析，および，以上のアルゴリズムを深さ優先探索において，主に，「この頂点は既に訪問済みか？」ということの判定にうまく使うことによって以上の結果が得られる．

（２）深さ優先探索以外のグラフに関する問題に関する結果

次の問題それぞれについて，n/[exp(Omega(root(log n)))]ビットの記憶領域だけ用いて，多項式時間で解くアルゴリズムを与えることに成功した．

(a)非巡回有向グラフ G とその頂点 s が与えられたとき，グラフ G の各頂点 v について，v から s までの最長パスの長さを計算せよ(パスが存在しない場合の距離はマイナス無限大とする)．

(b) 各辺に正整数重みをもつ非巡回有向グラフ G とその頂点 s が与えられたとき，各頂点 v から s への最も重いパスの重さを計算せよ．

(c) 非巡回グラフ G が与えられたとき，頂点をトポロジカルソートした結果のリストを出力せよ．

(d) 非巡回グラフ G が与えられたとき，topological-first search tree を出力せよ．

次の２つの問題については，同様の結果が成立するのかどうかについて未解決に終わった．

(e) 与えられた無向グラフ G について，maximum cardinality search (MCS) tree を計算せよ．

(f) 与えられた無向グラフ G に対して，perfect elimination order の存在を判定せよ．存在する場合は perfect elimination order をひとつ計算せよ．

（３）結果の解釈・意義，未解決問題

上述の結果と証明は，有向グラフにおける到達可能性判定問題が，一群の問題の領域計算量を考える鍵となることを示唆している．一方で，「有向グラフにおける到達可能性がもしより小さな記憶領域で解ければ，問題 X も同じ小さな記憶領域で解ける」という明確な還元性についての結果を得ることはできずに未解決として残った．その理由は，我々の証明においては，Barnes らの有向グラフ到

達可能性判定アルゴリズムをブラックボックスとしてルーティーンとして用いているのではなく，設計方針という中身まで立ち入って用いているということにある．

深さ優先探索については，o(n)ビットだけ用いて実行することが可能なのかどうか，あるいは，C < 1である定数Cについて，Cnビットだけ用いて実行することが可能なのかどうか，2016年6月現在，未解決な興味深い問題となっている．

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）

〔学会発表〕（計１件）

[1] T. Asano, T. Izumi, M. Kiyomi, M. Konagaya, H. Ono, Y. Otachi, P. Schweitzer, <u>J. Tarui</u>, and R. Uehara: Depth-First Search Using O(n) Bits, Lecture Notes in Computer Science (LNCS) vol. 8889: Proceedings of ISAAC2014: the 33rd International Symposium on Algorithms and Computation, Springer, 553-564, 2014. DOI: 10.1007/978-3-319-13075-0_44
発表者：M. Konagaya, **発表年月日：**Dec 15, 2014, **発表場所：**Jeonju (Korea)

６．研究組織

(1)研究代表者
垂井淳　（Jun TARUI）
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