様式 C-19

科学研究費補助金研究成果報告書

平成２１年　５月１６日現在

研究種目：基盤研究（C）
研究期間：2007　～　2008
課題番号：19500006
研究課題名（和文）　大規模数理計画的アプローチに基づく回路計算量の下限導出手法の開発

研究課題名（英文）　Development of a New Method for Circuit Complexity Based on Large Scale Mathematical Programs

研究代表者
天野　一幸（AMANO KAZUYUKI）
群馬大学・大学院工学研究科・准教授
研究者番号：30282031

研究成果の概要：論理回路モデルを代表とする各種計算モデルに対する，論理関数の計算量の下限導出手法に関する研究を行った．特に，計算量下限導出問題を大規模数理計画問題へと帰着するアプローチについて重点的に研究を行った．その結果，限定乱雑性を持つ論理関数に対する論理回路のサイズや，多数決関数を近似する論理関数に対する定数段数論理回路のサイズの漸近的値を明らかにすることに成功した．更には，単キュービット量子回路に対して，その表現の一意性が担保される正規形の概念を提案した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,700,000	510,000	2,210,000
２００８年度	1,000,000	300,000	1,300,000
年度			
年度			
年度			
総　計	2,700,000	810,000	3,510,000

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：回路計算量，下限，論理回路

１．研究開始当初の背景

与えられた仕様を満足するハードウェアを構成するのに必要な部品の個数や，与えられた問題を解くのに必要な計算資源の量を最小化する問題を考えるとき，予めコスト最小化の限界点を明らかにしておくことは極めて重要である．この問題を，論理関数を計算する論理回路の最小サイズとして定義される回路計算量の下限を導出する問題に還元し，解決することを目指すのが，本研究の対象とする論理関数の複雑さに関する研究である．計算機科学分野における最重要未解決問題とされる“Ｐ≠ＮＰ予想”の解決にも直結するこの問題に対しては，国内外を通じて，半世紀以上に渡り精力的な研究が続けられているものの，計算量の下限を導出し得る汎用手法は得られておらず，新たな証明手法の開発が熱望されている．

これまでに，単調や定数段数といった種々の制約を課した回路モデルに対する下限導出手法が個別に開発され，一定の成功を収めてはいるものの，これら手法の限界点についても次第に明らかにされつつある．特に，９０年代半ばに Razborov と Rudich によって導

入された Natural Proof と呼ばれる概念は，従来型証明手法の限界を強く示唆するものとして，多くの計算量理論の研究者に驚きを持って迎えられた．これは，従来開発されてきた下限導出手法は全て Natural Proof と呼ばれる証明の枠組みの中で捕らえられること．また，この枠組みに従った証明では，ある暗号学的に妥当な仮定のもとで，Ｐ≠ＮＰ予想の解決に結びつくような強い下限は証明し得ないことを厳密に証明したものである．

この結果を受け，国内外の研究者の間では，従来手法の枠組みを越えた新たな下限導出手法の開発が必要であるとする認識が広まった．従来広く用いられてきた組み合わせ論にとどまらず，様々な数学的理論を取り入れる試みなど，この状況を打破する手法を模索する試みが続いているが，現在のところ，決定打と目されるような手法は提案されるに至っていない．

２．研究の目的

本研究の最終的な目標は，種々な論理関数に対する回路計算量の下限を評価し得る汎用的手法を開発することである．この大きな目標へ向け，本研究では特に，組み合わせ論的解析と，大規模数理計画的計算に基づく解析との融合から，新たな下限導出手法の開発を目指す．

これまでに，論理回路の深さを限定したモデルである定数段数論理回路や，論理回路の各素子の出次数を１に制限したモデルである論理式など，いくつかの限定された計算モデルに対する下限導出問題に対して，これらが様々なタイプの数理計画的問題として定式化されることが明らかとなってきつつある．例えば，２段のしきい値回路における計算量の下限導出が線形計画問題に，また，論理式における下限導出問題が半正定値計画問題に帰着できることが明らかされてきた．特に近年，これらの事実を利用した下限導出手法がいくつか開発提案され，注目を浴びている，本研究では，このアプローチをより強力に推し進めることで，これらの手法の能力に関する，より詳細な解析，および，より一般的な計算モデルにも適用可能であるような手法への拡張を目指す．

また，最近の研究によって，高い計算複雑さを持つであろう論理関数には，その困難さの核ともいうべき，組み合わせ論的に記述可能な極限的構造が内在することが示唆されている．本研究では，このような構造を，従来型の離散数学的議論を駆使することに加えて，近年の爆発的な計算機の性能向上によって可能となった，大規模な数理計画的アプローチを通じて抽出することが，一つの大きな目的である．また，ここで捕らえた性質を理論的枠組みの中に定式化し，様々な計算モデルに対する複雑を評価し得る手法を得ようというのが，本研究における主たる目的である．

３．研究の方法

本研究は，論理関数の計算量の評価手法の開発を目指すものである．これに向けて，特に，計算困難な論理関数を困難たらしめている組み合わせ的構造を抽出するための理論的検証，および，これに対する仮説を得るための計算機実験，更には，得られた性質を理論的枠組みの中で定式化し，下限導出の手法として汎用化することの３点が主軸となる．

より具体的には，まず，これまで論理関数の複雑さの研究において多く研究され，様々な性質が知られるようになってきている，いくつかの関数を取り上げ，その関数が特徴的に持つ離散的性質をより詳細に検討する．例えば，定数段数論理回路に対する多数決関数や，単調論理回路に対するクリーク関数といった．強い下界が知られる関数に対して，その関数を，それぞれの計算モデルの中で困難たらしめている組み合わせ論的性質を明らかにすることを目指す．この際には，本研究の特徴の一つでもある，大規模な計算機による実験をも積極的に用いることとする．

こうして得られた性質が，より一般的な回路モデルに対しても，下界の導出の材料として使用可能であるかについて検討を行う．すなわち，上記で抽出した性質を持つ関数が，より上位の計算モデルにおいても，実際に計算困難であるかなどについて検討を行う．このような考証を通じて，種々の計算モデルに対して，計算量の下限導出に用いることが可能な，組み合わせ論的性質を明らかにすることを目指す．また，このような性質の発見に成功した場合には，これを理論的枠組みの中で定式化し，可能な限り汎用的な計算モデルに対する下限導出手法の開発を行う．

４．研究成果

現在までの，半世紀以上にわたる，回路計算量に関する研究の歴史において，強い下界を得ることのできる証明手法の開発に成功したのは，本質的に，定数段数論理回路と単

調論理回路の２つである．従って，これら両者における手法に対するより深い理解が，より一般的な計算モデルに対する手法の開発の手掛かりとなることが期待される．よって本研究では，まず，これら両者のモデルの計算能力に対して新たな知見を得るべく，より詳細な検討を行った．

最近（2008 年），Rossman によって，定数段数論理回路における下界導出手法の多くのベースとなっている，Hastad による交代補題を，巧妙に使用することで，k-クリーク関数を計算する定数段数論理回路に対するΩ(nˆ(k/4))の下界が証明され話題を呼んだ．同じ問題に対する，これ以前に知られていた下界は，例えば，Ω(nˆ{k/dˆ2})のように，回路の深さｄをその指数部に含み，それゆえ，深さが増加するごとに，下界の値が減少してしまうという性質を持っていた．これに対し，上記の結果は，深さｄが定数でありさえすればいくら増加しても，サイズに対する有効な下界が得られるという点において，画期的なものであった．

本研究では，この新たな手法を詳細に検討することで，この手法の限界，および，発展可能性を明らかにすることを目指した．その結果，まず，Rossman が下界を証明するために，クリーク関数の困難さを特徴付けると考え着目した入力分布の元では，これ以上の下界の改善が不可能であることを，構成的に証明することに成功した．また，k-クリーク問題を，ハイパーグラフ上に拡張した問題を考えることで，この下界が，より自明な上界である O(nˆk)に近づくことを証明することに成功した．この結果は，国際的にも評価を受け，計算量理論分野における最高峰の国際会議の一つである IEEE の計算量理論に関する国際会議(CCC09)に採択された．

本研究では，また，多数決関数を近似する定数段数論理回路のサイズに対する研究をも行った．多数決関数は，実用上様々な場面で現れる非常に一般的な論理関数であるのみならず，理論的にも，例えば，全ての単調論理関数のうちで，入力の変化に対する出力の変化が起きる割合を表わす，感受度と呼ばれるパラメータが最大であるなどの特徴を持つことから，その効率的な構成法等について，古くから多くの研究が行われてきた．

本研究では，この多数決関数を近似する，定数段数論理回路のサイズの漸近的値を，厳密に決定することに成功した．これについては，Valiant が 70 年代に開発した，単調論理式モデルにおける，多数決関数の厳密計算のサイズの上界を示すのに用いられた巧妙かつエレガントな構成法を，より一般化した手法を用いることで，これまで知られる上界の値を改良し，最近，O’Donnell らによって証明された下界の値に一致するサイズによるものが存在することを示した．この結果は，国際的にも評価を受け，欧州における理論計算機科学分野の最有力国際会議の一つである，ICALP09 に採択された．

本研究では，より一般的な，通常の論理回路サイズに対する研究も行った．まず，明示的に与えられた論理関数に対する回路計算量の下限に対する現在最良の結果である Lachish，Raz，岩間，森住による５ｎの下界の証明を，計算機援用の元で再構成することを試みた．この証明手法は，論理関数に対する，限定乱雑性と呼ばれる組み合わせ論的性質が，その証明の核として使用されていることが知られている．

計算機援用の基で組み立てた上記証明手法を，より拡張することで，この下限を改良しようという試みも行ったが，これについては既知の下界を超える下限を導出することは出来なかった．しかし，上記の実験を通じて得られた知見を手掛かりとして，限定乱雑性に基づく証明手法の限界を明らかにすることに成功した．より具体的には，論理回路モデルにおける下限導出手法が，その証明中で，計算困難さを担保する組み合わせ論的性質として限定乱雑性を用いている限り，５ｎを超える下限が証明不可能であることの厳密な証明を与えた．これは，サイズが５ｎの論理回路で，限定乱雑性を満たす論理関数を，実際に計算可能であることを，具体的回路を与えることにより示された．従って，上で述べた回路計算量の下限を改良しようという場合には，少なくとも，限定乱雑性に代わる，高い計算量が担保される，新たな論理関数に対する性質を探求することが必要不可欠であることを意味している．当然，このような性質を発見することが，非常に重要な今後の課題となる．

本研究では，以上述べてきた，従来型の論理式や論理回路モデルといった，いわゆる，古典計算モデルに加えて，近年，素因数分解等の重要な問題が，古典計算に比べて，非常に高速に解ける等の著しい性質を持つことから盛んに研究されている量子回路モデルに対しても研究を行った．

量子回路は，その基本素子をどのように選択するかによって，計算能力に差が出ることが知られている．例えば，Pauli-X,Y,Z，および，CNOT 素子を構成要素とする，いわゆる Clifford 量子回路は，その計算能力が，古典

論理回路を超え得ないことが知られている．一方，これに，π/8 素子と呼ばれる素子のみを加えることで，計算万能かつ，量子計算機で多項式時間計算可能な全ての計算を，多項式サイズの量子回路で行なうことができるように能力が上がることも知られている．すなわち，π/8 素子の存在が，量子計算機構における計算の高速化の要因の一つとなっているものと考えることができる．

そこで，本研究では，この Clifford 素子，および，π/8 素子からなる量子回路の計算能力に着目し研究を行った．その結果，最もシンプルなケースである，単キュービット量子回路の場合には，一意性が担保されるカノニカルな標準形を与えることに成功した．すなわち，任意の単キュービット回路は，それと等価な標準形回路で表現され，また，その表現は一意である．この結果を用いると，例えば，単キュービット量子回路によって表現可能なユニタリ行列を，重複も抜けも無く生成することが可能となる．また，現在は，この結果を，より実用的な場面においても適用可能となるように，複数キュービット量子回路に対する正規形へと拡張を試みている．

本研究では，以上述べてきた主たる研究成果に加えて，例えば，ある特定の離散構造を持つ対象の個数を効率的に評価することのできる手法などの開発にも取り組んだ．例えば，通常フロアプランと呼ばれる，方形のより小さな方形への分割問題に対して，そのパターンの個数の下限導出問題を，大規模行列の第一固有値の計算に帰着する手法を提案した．このようなパターン数に対する下限を与えることは，これに対する最も効率的なコード化によるコード長に対する下限を，その対数的値として与えることから，実用的見地からも価値があるものと考えられる．本研究では，上記の帰着によって得られた約１２００万次の大規模正方行列の第一固有値を，実際に計算機を用いて求めることによって，従来知られているものより強い下界を得ることに成功するなどの成果をも得た．

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５件）

① 天野　一幸, K-Subgraph Isomorphism on AC0 Circuit, Proceedings of the 24th IEEE Conference on Computational Complexity, 2009 (in press), 査読有

② 天野　一幸, Bounds on the Size of Small Depth Circuit for Approximation Majority, Proceedings of the 36th International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science, 5555, 2009 (in press), 査読有

③ 松本　健, 天野　一幸, Representation of Quantum Circuits with Clifford and π/8 Gates, Proceedings of the 8th Asian Conference on Quantum Information Science, 135-136, 2008, 査読有

④ 佐藤　貴之, 天野　一幸, 瀧本　英二, 丸岡　章, Monotone DNF Formulas that has a Minimal or Maximal Number of Satisfying Assignments, Lecture Notes in Computer Science, 5092, 191-203, 2008, 査読有

⑤ 天野　一幸, 垂井　淳, A Well-Mixed Function with Circuit Complexity 5n + o(n):Tightness of the Lachish-Raz-type Bounds, Lecture Notes in Computer Science, 4978, 342-350, 2008, 査読有

〔学会発表〕（計６件）

① 福原 秀明, 滝本 英二, 天野 一幸, 最簡な論理式でNPN同値類の代表のみを生成するアルゴリズム, 電子情報通信学会 コンピュテーション研究会 , 2009.3.1, 東京

② 天野 一幸, 部分グラフ同型性判定の回路計算量について, 電子情報通信学会 コンピュテーション研究会 , 2008.12.3, 群馬県伊香保

③ 松本　健, 天野　一幸, Clifford＋π/８量子回路の計算能力, 電子情報通信学会 コンピュテーション研究会, 2008.3.10, 神奈川

④ 天野　一幸, 中野　眞一, 山中　克久, 方形描画の数え上げ, 電子情報通信学会　コンピュテーション研究会, 2007.11.28, 新潟

⑤ 天野　一幸, 垂井　淳, A Well-Mixed Function with Circuit Complexity 5n + o(n):Tightness of the Lachish-Raz-type Bounds, The 10th Korea-Japan Joint Workshop on Algorithms and Computation (WAAC 07), 2007.8.9, 光州 (韓国)

⑥ 天野　一幸, 垂井　淳, 回路計算量の 5n の下界に対する 5nの上界, 2007 年夏のＬＡシンポジウム, 2007.7.20, 石川

６．研究組織

(1)研究代表者

天野　一幸（AMANO KAZUYUKI）
群馬大学・大学院工学研究科・准教授
研究者番号：30282031

(2)研究分担者

（　　）

研究者番号：

(3)連携研究者

（　　）

研究者番号：