氏名（本籍）	天野一幸（あまのかずゆき）（北海道）
学位の種類	博士（情報科学）
学位記番号	情博第11号
学位授与年月日	平成8年3月26日
学位授与の要件	学位規則第4条第1項該当
研究科，専攻	東北大学大学院情報科学研究科（博士課程）情報基礎科学専攻
学位論文題目	ブール代数に基づいた計算の複雑さに関する研究
論文審査委員	（主査） 東北大学教授　丸岡　章　東北大学教授　西関　隆夫 東北大学教授　阿曽　弘具 （工学研究科）

論文内容要旨

第1章　序　論

与えられた問題に対して，その問題を解くのに必要な計算資源の量を求めるというのは，実用上非常に重要な問いである。特定の問題に対してこの値の下界をその問題の複雑さと称すると，複雑さはその問題を解くアルゴリズムの効率化の限界を示すものと考えられ，それ故この値は非常に大きな意味を持つ。ところが，与えられた問題の複雑さの下界を示すことは一般に非常に難しく，現在のところこれに対する有効な手法は見つかっていない。複雑さのより厳密な定義として，問題を自然な形で論理関数として表現し，その論理関数を計算する論理回路の素子数の最小値を用いるというのは，計算の複雑さを論じる上で最も一般的な立場である。論理関数の複雑さの下界を示そうという研究は長年に渡り非常に多く行なわれてきたにもかかわらず，特定の論理関数の複雑さの下界として知られている最良の値は入力変数の個数の線形に過ぎず，良い下界を示すことは，理論計算機科学の分野における最も重要な未解決問題の一つとなっている。本研究では，この立場に立ち論理関数の複雑さの下界の導出方法について探ることを主な目的とした。本研究はまた，正確に値を求めることが非常に困難であることが知られる，ある種の問題に対して，その近似解を求めるアルゴリズムを構成する手法を開発することを目的とした。

第2章　論理関数の複雑さ

第2章では，ブール代数に基いた論理関数の複雑さについて議論する上で必要となる基本的事柄や諸定義について述べた。また，計算のモデルとして論理回路を用いることの妥当性についても，実際の計算時間をよく反映するモデルとして知られるチューリング機械との関係を示すことで言及した。更に，この分野において現在までに得られている結果を概観し，その中で特に否定ゲートを許さない回路（単調論理回路と呼ぶ）では，ある特定の関数を計算するのに指数関数個のゲートが必要であるという命題を証明する際に用いられたRazborovによって開発された近似法と呼ばれる下界導出の手法について詳しく解説した。

第3章　近似演算の一般化と否定限定論理回路

第3章では，従来単調論理回路モデルにおける複雑さの下界導出にのみ用いられてきた近似法を，論理回路に否定ゲートがある程度出現する場合についても下界導出が可能な方法へと拡張した。また，論理回路に対する制約として従来多

く考えられてきた単調性の制約を一般化し，論理回路で否定ゲートが用いられる度合を表すと考えられる指標を提案し，更に，この尺度に基づき否定の用いられる度合が小さな論理回路では，与えられたグラフにある指定されたサイズの完全グラフが含まれる否かを判定する関数であるクリーク関数を計算するのに指数関数個のゲートが必要であることを示した。

論理回路は，入力端子にリテラル（変数またはその否定）と定数が割り当てられ，回路中にはANDゲートとORゲートのみが現われるものとする。リテラルの集合Lに対して，Lに対応する項$\wedge_{\ell \in L} \ell$ を$\wedge L$と表す。単調論理関数fに対してその主項全体をPI（f）と表す。単調論理関数fを計算する論理回路Cが与えられたとする。回路Cの入力端子に現われる各否定リテラル$\overline{x}_i$（$i=1,\ldots,n$）を，新たに導入した論理変数y_iで置き換えて得られる$2n$変数単調論理回路をC_αとし,C_αで計算する関数をf_αとおく．$k=0,\ldots,n$に対して，PI（f）の部分集合PI_k（C）を

$$\mathrm{PI}_k(C) = \left\{ \wedge L \in \mathrm{PI}(f) \;\middle|\; \begin{array}{l} \exists Y \subseteq \{y_i \mid 1 \le i \le n,\ x_i \not\in L\} \\ \quad |Y| \le k,\ \text{かつ},\ \wedge(L \cup Y) \in \mathrm{PI}(f_\alpha) \end{array} \right\}$$

と定義する。定義より明らかに，単調論理関数fを計算する任意の（必ずしも単調でない）論理回路Cに対して$\mathrm{PI}_0(C) \subseteq \mathrm{PI}_1(C) \subseteq \cdots \subseteq \mathrm{PI}_n(C) = \mathrm{PI}(f)$が成り立ち，特に，$C$が単調論理回路の場合には$\mathrm{PI}_0(C) = \mathrm{PI}(f)$が成立する。また，この定義より，$\mathrm{PI}_k(C)$がPI（$f$）に 等しくなる最小の$k$の値は，論理回路$C$で否定の用いられる度合を表す一つの尺度である考えられる。

本研究では，この定義に従い次の定理を示した：入力として与えられるm頂点無向グラフに$\sqrt{m}$完全グラフが含まれるか否かを判定する$\binom{m}{2}$変数論理関数をfとし，論理回路Cがfを計算しているとする。εを任意の正定数とする。このとき，$\mathrm{PI}_{m^{0.2}}(C) = \mathrm{PI}(f)$を満たすならば，Cに含まれるゲートの個数はある指数関数で下から押さえられる。

この定理の証明は，これまで専ら単調回路モデルに対する複雑さの下界導出に用いられてきた近似法を，その中で用いられる近似演算を一般化することで，否定ゲートが許された回路に対する下界導出にも適用できる手法に拡張し，これを適用することで行なった。

第4章　切断の概念に基づいた近似理論

第4章では，切断の概念に基づく近似法について，主にこの手法による一般の回路モデルでの複雑さの下界導出の可能性について調べることを目的とした。この手法は従来単調回路モデルにおける複雑さ（以下，単調複雑さ）の下界導出に広く用いられてきた，近似演算の概念に基づく下界導出の手法が，単調性の制約を外した一般の回路における下界導出には適さないことが示されたのを受けて，これに変わるものとして提案されたものである。まず，この手法においては論理関数fの複雑さの下界がfによって定まる，単調論理関数の（近似モデルと呼ばれる）クラスF_fに対する，ある種の最小被覆問題の解として与えられることを述べる。また，従来得られていた単調回路モデルに対するクリーク関数の複雑さの指数関数の下界と同様の結果が，この切断の概念を用いた論法によっても証明できることを示した。

実際にこの手法を用いて複雑さの下界を示そうという場合には，その近似モデルを構成する際に，より単純で，サイズの小さなものであることが望ましい。本研究はこの点についても検討を行ない，自明でない下界を与えるための近似モデルに対する必要条件を示し，更に従来知られているものよりサイズの小さな近似モデルを実際に構成した。

この手法では，複雑さの下界を求める対象とする論理関数fを単調なものに限定した場合には，その最小被覆問題の解がfの単調複雑さの下界を与えるものとして，F_fを真に含む単調関数のクラスF_f'も定義される。本章ではさらに，F_fとF_f'の差の領域に着目し，この領域に対する最小被覆問題の解がBerkowitzによって導入されたfの擬似補関数の単調複雑さの下界を与えることを示し，更に，従来の単調複雑さの下界導出の手法がこの擬似補関数の単調複雑さの下界導出にも適用可能であることを指摘し，実際に，クリーク関数の擬似補関数の単調複雑さの指数関数の下界を証明した。また，非決定性論理回路を計算のモデルとして用いた場合の複雑さに対応する近似モデルの構造についても論じた。

第5章　*k*-限定独立性に基づいたDNF式の近似アルゴリズム

第5章では，DNF式を充足する変数への論理値の割り当ての割合を近似する決定性アルゴリズムを構成する方法について論じた。与えられた論理式を真にする割り当ての個数を求める問題や，グラフに含まれるハミルトニアン閉路の

個数を求める問題といったある種の数え上げ問題は NP≠P の仮定の元では多項式時間で解けないことが知られており，それ故，その近似解を求めるアルゴリズムの開発が求められている。本研究では，この種の問題の代表的なものとして，n 変数上のDNF式 F が与えられた時，Fを充足する変数への論理値の割当の個数の，変数への割り当て全体（2^n個存在する）に対する割合を求める問題を取り上げ，この近似値を求める決定性アルゴリズムを，確率分布に対する限定された独立性という概念を用いて構成する方法について検討を行なった。

$\{0, 1\}^n$の上の確率分布 D が k-限定独立であるとは，各々 0 か 1 の値をとる確率変数 $x_1, \ldots, x_n$ が Dに従うとしたときに，

$$\forall j \leq k \, \forall \, \{i_1, \ldots, i_j\} \subseteq \{1, \ldots, n\} \, \forall \, \{v_1, \ldots, v_j\} \in \{0, 1\}^j \, \mathrm{Pr}_D\left[\bigwedge_{\ell=1}^{j} (x_{i_\ell} = v_\ell)\right] = (1/2)^j$$

を満たすことをいう。ただし，ここで Pr_D [ ] は,確率変数の値を添字で示された分布に従って抽出した時に,括弧内に示される事象が生起する確率を表す。これに関連して Luby らは次の予想を提示した：F を n 変数 m 項DNF式とする。$\varepsilon > 0$ を任意の定数とする。$\{0, 1\}^n$上の一様分布を $\mathcal{U}$ とする。このとき，ある定数 c が存在して，$\{0, 1\}^n$上の確率分布 D が $c\log(m/\varepsilon)$-限定独立分布ならば，$|\mathrm{Pr}_D[F(x)=1] - \mathrm{Pr}_{\mathcal{U}}[F(x)=1]| \leq \varepsilon$ が成り立つ。

k-限定独立性の条件を満たす確率分布は，k の値が小さな場合には小さな標本空間上に実現できることが知られているので，この予想が真ならば，D の標本空間中の全ての割り当てについて検査することで，実用的時間で動作する所望のアルゴリズムが実現できる。本研究ではこの予想について検討を行ない，各リテラルが高々 1 度しか現われないDNF式に対しては，この予想が肯定的であることを示した。また，この様な制約を満たす DNF 式を充足する割り当ての割合を近似する多項式時間決定性アルゴリズムを構成した。

第 6 章　結　　論

第 6 章は本論文の結論であり，本研究によって得られた結果とその意味について総括した。

審 査 結 果 の 要 旨

与えられた問題を解くのに必要となる計算量を求めることは，問題に内在する計算の複雑さを解明するだけでなく，アルゴリズムの効率化の限界を知る上でも重要である。しかし，正確な計算量を下からおさえる値（下界）を導く一般的な手法は知られておらず，この手法を開発することは計算量理論における最も重要な課題のひとつとして残されている。本論文は，論理関数の複雑さの下界を導出する手法を提案し，複雑さの下界を具体的に求めるとともに，計算が困難なある種の組合せ問題を近似的に解くアルゴリズムを与えたもので，全編6章よりなる。

第1章は序論である。第2章では，与えられた問題の計算量を求める問題が，論理関数を計算する論理回路のサイズを求める問題に帰着されることを述べた後，論理関数の複雑さについてこれまでに知られている結果をまとめている。

第3章では，論理回路が単調という制約のもとで，回路のサイズの下界を導く手法として知られている近似法を拡張し，回路に否定がある程度現われる場合にも適用可能な手法を与えている。また，この手法を用い，回路に現われる否定がある範囲内に限定されている場合には，クリーク関数を計算する論理回路のサイズの下界が指数関数で与えられることを証明している。これは優れた結果である。

第4章では，クリーク関数を計算する単調論理回路のサイズの下界を，切断の概念を用いて導出できることを示している。また，切断の概念に基づく近似法では,論理関数 f の複雑さの下界が，f の近似モデルに対する最小被覆問題の解として与えられることを示し，自明ではない下界を得るための近似モデルに関する条件を導いている。

第5章では，論理値の割当てが積和型論理式（DNF式）を充足する確率を近似的に求めるアルゴリズムについて論じている。DNF式を充足する確率は，論理値の割当てが一様分布に従って生起する場合と，限定された独立性を持つ k-限定独立確率分布に従って生起する場合とでは，大きな差のないことが予想されていたが，各リテラルが高々一度しか現われないDNF式を対象とした場合は，この予想が成立することを証明している。

第6章は結論である。

以上要するに本論文は，アルゴリズムの効率化の限界を与える計算の複雑さの下界を導く手法を与えるとともに，ある種の組合せ問題に対する近似アルゴリズムを示したもので，情報基礎科学の発展に寄与するところが少なくない。

よって，本論文は博士（情報科学）の学位論文として合格と認める。