数理解析研究所講究録
950巻 1996年 15-21

単調論理関数と擬似補関数に対する近似モデル

天野 一幸　　丸岡 章
Kazuyuki AMANO　　Akira MARUOKA

東北大学大学院情報科学研究科
E-Mail: {ama|maruoka}@ecei.tohoku.ac.jp

あらまし　Razborovによる拡張された近似法は，原理的には否定を許す論理回路に基づいた複雑さのほぼ正確な下界を導出し得る方法である．切断の概念を用いてこの近似法により単調論理関数 fの単調複雑さ $\mathrm{size}_{mon}(f)$ の下界を導くには，fにより定まるある汎関数のクラス $\mathcal{F}_f^+$を適当に定め，次いで $\mathcal{F}_f^+$を切断する対の集合で，対の個数が最小のものの個数を求め，この値を $\mathrm{size}_{mon}(f)$ の下界とするという手順をふむ．本稿では，まずクリーク関数の単調複雑さの下界として，AlonやBoppanaらの示した指数関数のものと同様の結果がこの手法によっても導かれることを示す．否定も許す回路に基づいた複雑さ $\mathrm{size}(f)$ を求めるには，$\mathcal{F}_f^+$の代わりに $\mathcal{F}_f \subseteq \mathcal{F}_f^+$の関係にある汎関数のクラス $\mathcal{F}_f$を適当に定め，上の手順により下界を求めればよい．本稿では，この両者のクラスの差として定義される $\mathcal{F}_f^\Delta = \mathcal{F}_f^+ - \mathcal{F}_f$ をとりあげ，$\mathcal{F}_f^\Delta$ の最小切断対の個数が fの擬似補関数の単調複雑さの下界を与えることを示す．更に，クリーク関数に対する単調複雑さの指数関数の下界を導く従来の議論が，$\mathcal{F}_f^\Delta$ の最小切断対のサイズの導出にも使えることを示し，結果としてクリーク関数の擬似補関数の単調複雑さの指数関数下界を得る．

1　はじめに

与えられた論理関数 fの複雑さ $\mathrm{size}(f)$(回路計算量) の下界を求めるという問題は，長年にわたる挑戦にもかかわらず，これまでのところ，自然な論理関数に対して変数の個数の線形を超える下界すら知られていない [14, 4].

近年，論理回路に制約を設けて，その制約のもとで複雑さを定義し，その下界を求める研究が数多くなされ，特に，定数深さ (但し，ここではゲートの入次数は無制限であるとする) や単調という制約の元では，パリティ関数やクリーク関数を計算するにはいずれも指数関数個のゲートが必要となることが示された [6, 9, 10, 1, 3].

Razborovは1985年に単調複雑さの下界導出のための近似法と呼ばれる強力な手法を開発し，与えられたグラフに指定されたサイズのクリーク (完全グラフ) が含まれるか否かを判定するクリーク関数 CLQ の単調回路に基づいた単調複雑さ $\mathrm{size}_{mon}(\mathrm{CLQ})$ の下界として，超多項式として与えられるものを導いた [9]. のちに，AlonとBoppanaがこの結果を改良し，これに対する指数関数の下界を得た [1].

それ以後，この手法による否定を許した場合の複雑さ (否定も許す回路に基づいた回路計算量) の下界導出の可能性を探る研究が幾つかなされているが [8, 7, 11]，この手法には今だ未知の部分が多く，そのため近似法の可能性と限界についてより深い洞察を得ることが望まれる．我々は，この立場に立って研究を行ない，これに関して得られたいくつかの結果について報告する．

近似法では，$U \subseteq \{0,1\}^n$上で定義された2値関数のクラスを定義域とする近似モデルと呼ばれる汎関数のクラスを導入する．下界を求める対象を単調論理関数に限定し，単調複雑さと否定も許した場合の複雑さを対象とする場合，この汎関数のクラスとしてそれぞれ $\mathcal{F}_f^+$と $\mathcal{F}_f$と表されるクラスが定められ，両者の間には $\mathcal{F}_f \subseteq \mathcal{F}_f^+$の関係が成立する．切断の概念に基づく近似法では，これらの汎関数のクラスを切断する対集合のなかでサイズ最小のもの (最小切断対) のサイズを求める．対象とする汎関数のクラスが $\mathcal{F}_f^+$, $\mathcal{F}_f$の場合，切断対集合の最小サイズは，それぞれ$\rho(\mathcal{F}_f^+)$, $\rho(\mathcal{F}_f)$ と表される．一般に論理関数 fの複雑さは，fにより定まる汎関数のクラスの最小切断対のサイズにより下からおさえられ，$\mathrm{size}(f) \geq \rho(\mathcal{F}_f)$ や $\mathrm{size}_{mon}(f) \geq \rho(\mathcal{F}_f^+)$ 等の不等式が成立するので，最小切断対のサイズが論理関数の複雑さの下界を与える．本稿では **2** において，以上のことを詳しく解説し，**3** では，クリーク関数の単調複雑さの指数関数の下界を，近似法の切断の概念によって与える．

更に本稿では **4** において，上で述べた2つの汎関数のクラスの差として与えられるクラス $\mathcal{F}_f^+ - \mathcal{F}_f$に注目し，これを $\mathcal{F}_f^\Delta$と表し，これの最小切断対のサイズを求める．まず，$\mathcal{F}_f^\Delta$の最小切断対の個数$\rho(\mathcal{F}_f^\Delta)$ 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，次いで，$\rho(\mathcal{F}_f^\Delta)$ の指数関数の下界を導く．また，この$\rho(\mathcal{F}_f^\Delta)$ の下界は$\rho(\mathcal{F}_f^+)$ の下界の場合と同様に導出されることを示

し，このことから，従来の切断に基づいた議論では，$\mathcal{F}_f$の否定を許した場合の自明でない下界を最小切断対のサイズから求めることは難しいことを指摘する．すなわち，$\mathcal{F}_f^+ = \mathcal{F}_f \cup \mathcal{F}_f^{\mathsf{A}}$が成立するので，$\mathcal{F}_f^+$の最小切断対は当然$\mathcal{F}_f$をも切断している訳であるが，$\rho(\mathcal{F}_f^+)$の下界は主に$\mathcal{F}_f^{\mathsf{A}}$を切断しているという事実を根拠にして求められているということが明らかにされる．

2 近似法

本章では近似法の定義を与える．一般の論理回路における論理関数の計算量の下界を証明し得るように拡張された近似法の定義は，まず，Razborov[11]が示し，その後，より直観的な定義がKarchmar[7]によって与えられた．

論理回路とは，$x_1,\ldots,x_n,\bar{x}_1,\ldots,\bar{x}_n,0,1$を入力とし，2入力のANDゲートとORゲートから構成される回路である．論理回路Cのゲート数をsize(C)と表し，論理関数fを計算する最小のゲート数の論理回路のゲート数を，fの複雑さといい(回路計算量と言うこともある)，size(f)と表す．特に，入力に変数の否定が現れない回路を，単調論理回路と呼ぶ．単調論理関数fを計算する，ゲート数が最小の単調論理回路のゲート数を，fの単調複雑さといい(単調回路計算量と言うこともある)，size$_{mon}(f)$と表す．

複雑さの下界を求めようとする$x_1,\ldots,x_n$を論理変数とするn変数論理関数をfと表す．n変数論理関数全体を$\mathcal{B}^n$で，n変数単調論理関数全体を$\mathcal{M}^n$で表す．wは$\{0,1\}^n$の要素を表すものとし，$i=1,\ldots,n$に対して，w_iでwのiビット目の値を表すものとする．x_i^1とx_i^0は，それぞれx_iと$\bar{x}_i$を表す．

$U \subseteq f^{-1}(0)$，$V \subseteq f^{-1}(1)$とする．n変数論理関数gに対して，Uの部分集合$[g]_U$を

$$[g]_U = \{u \in U \mid g(u) = 1\}$$

と定義する．Uが明らかな場合は，$[g]_U$は単に$[g]$と表すこともある．$v \in V$に対して，$\mathcal{M}^{|U|}$の部分集合$\mathcal{F}_{U,v}$を

$$\mathcal{F}_{U,v} = \left\{ F \in \mathcal{M}^{|U|} \;\middle|\; \begin{array}{l} F(\phi) = 0 \text{ かつ} \\ \forall i \in \{1,\ldots,n\}\ F([x_i^{v_i}]_U) = 1 \end{array} \right\}$$

と定義する．$\mathcal{M}^{|U|}$の単調関数は，自然に2^Uから$\{0,1\}$への単調関数ともみなせることに注意されたい．同様に$\mathcal{M}^{|U|}$の部分集合$\mathcal{F}_{U,v}^+$を

$$\mathcal{F}_{U,v}^+ = \left\{ F \in \mathcal{M}^{|U|} \;\middle|\; \begin{array}{l} F(\phi) = 0 \text{ かつ} \\ \forall i \in \{1,\ldots,n\} \\ \qquad (v_i = 1 \Rightarrow F([x_i]_U) = 1) \end{array} \right\}$$

と定義する．$\mathcal{M}^{|U|}$の部分集合$\mathcal{F}_{U,V}$と，$\mathcal{F}_{U,V}^+$を

$$\begin{aligned} \mathcal{F}_{U,V} &= \bigcup_{v \in V} \mathcal{F}_{U,v}, \\ \mathcal{F}_{U,V}^+ &= \bigcup_{v \in V} \mathcal{F}_{U,v}^+ \end{aligned}$$

とおく．$\mathcal{F}_{U,V}$の部分集合$\mathcal{F}$を，fに対する近似モデルという．同様に，$\mathcal{F}_{U,V}^+$の部分集合$\mathcal{F}^+$を，fに対する単調近似モデルという．後に述べるように，$\mathcal{F}$と$\mathcal{F}^+$を適当に定めると，これらのモデルを用いてそれぞれfの複雑さとfの単調複雑さの下界を導くことができる．$\mathcal{F}_{f^{-1}(0),f^{-1}(1)}$を，特に，$f$の最大モデルと呼び，$\mathcal{F}_f$と表す．同様に$\mathcal{F}_{f^{-1}(0),f^{-1}(1)}^+$を$f$の単調最大モデルと呼び，$\mathcal{F}_f^+$と表す．

定義 1 Uの部分集合の対(A,B)が，近似モデル$\mathcal{F}$の要素Fを切断するとは，

$$F(A) = 1,\ F(B) = 1,\ F(A \cap B) = 0$$

を満たすことをいう．また，近似モデル$\mathcal{F}$と，Uの部分集合の対からなる集合$T = \{(A_i,B_i) \mid 1 \le i \le t\}$に対して，

$$\forall F \in \mathcal{F} \exists (A,B) \in T\ (A,B) \text{ が } F \text{を切断する},$$

が成り立つ時，Tは$\mathcal{F}$を切断するという．□

定義 2 $f \in \mathcal{B}^n$，$U \subseteq f^{-1}(0)$，$V \subseteq f^{-1}(1)$とする．近似モデル$\mathcal{F} \subseteq F_{U,V}$(または，$\mathcal{F} \subseteq F_{U,V}^+$)に対して，$\mathcal{F}$を切断するのに必要な$U$の部分集合の対の個数を$\rho(\mathcal{F})$と表す．□

このように近似モデルと切断の概念を定義すると，次の定理1に述べるようにfの複雑さは，fの近似モデル$\mathcal{F}_f$を切断する集合のうちで，サイズが最小のもののサイズで下からおさえられることが示せるので，fの複雑さの下界を求める問題は$\mathcal{F}_f$の最小切断集合を求める問題に帰着されることになる．近似法は，fの複雑さをfの近似モデルの最小切断集合のサイズを求めることにより導く手法である．

定理 1 [11, 7] 任意の$f \in \mathcal{B}^n$に対して，

$$\begin{aligned} \text{size}(f) &\ge \rho(\mathcal{F}_f), \\ \text{size}_{mon}(f) &\ge \rho(\mathcal{F}_f^+). \end{aligned}$$

□

3 $\rho(\mathcal{F}_f^+)$の指数関数下界

$s = 2,\ldots,m$に対して，m頂点無向グラフGの各頂点間の辺の有無を表す$n = m(m-1)/2$個の論理変数を入力とし，Gがs–完全グラフを含むとき，かつ，そのときに限り値1をとる論理関数をm頂点s–

クリーク関数と呼び，$\mathrm{CLQ}(m,s)$ と表す．

文献 [1] で，Alon と Boppana が $\mathrm{CLQ}(m,\lfloor 1/4(m/\log m)^{2/3}\rfloor)$ の単調回路計算量が $\exp(\Omega((m/\log m)^{1/3}))$ となることを示した．Alon らは，通常の論理ゲートの演算を近似する近似ゲートからなる近似回路の概念を導入し，fを計算する通常の論理回路 Cの各ゲートを近似ゲートで置き換えて得られる近似回路$\overline{C}$に基づき，$\overline{C}$の出力の誤差と$\overline{C}$の各ゲートで生じる誤差の間に成立する包含関係を 2 つの不等式として表し，これらの不等式を同時に満たすゲートの誤差の組に含まれる誤差の個数の最小値が，$\mathrm{size}_{mon}(f)$ の下界を与えるという命題を用いて，下界を導出している．一方，Karchmar は，近似ゲートの概念を用いずに切断の概念のみで，Alon らの下界の証明と同様の議論が展開できることを指摘したが，実際には Karchmar は s の値が 3 の場合の証明を与えただけである．本節では，Alon らと同じ s の範囲に対して，切断の概念のみに基づき，Alon らの結果とほぼ同じ s-クリーク関数の複雑さの下界を導く．

定義 3 $f \in \mathcal{B}^n$, $U \subseteq f^{-1}(0)$, $V \subseteq f^{-1}(1)$ とする．Uの部分集合の対からなる集合 Tを $T = \{(A_i,B_i) \mid 1 \le i \le s\}$ とする．$1 \le j \le n$ に対して，$A_{s+j} = [x_j]_U$, $B_{s+j} = [\bar{x}_j]_U$とし，S_{max}を

$$\begin{aligned} S_{max} = {} & \{A_i \mid 1 \le i \le s+n\} \cup \\ & \{B_i \mid 1 \le i \le s+n\} \cup \\ & \{A_i \cap B_i \mid 1 \le i \le s\} \cup \phi \end{aligned}$$

とおく．S_{max}上に次のルールトを導入する．

$$A_i, B_i \ \vdash \ A_i \cap B_i \ , \tag{1}$$

$$X \ \vdash \ Y \ . \tag{2}$$

ここで，XとYはS_{max}に属し，$X \subseteq Y$とする．ルールトを左辺の集合から右辺の集合が導出される ((1) の場合は，A_iと B_iが共に存在するとき，$A_i \cap B_i$が導出される) 関係とみなし，$S \subseteq S_{max}$に対して，関係$\vdash$に関する閉包を $cl_T(S)$ と表す．特に (1) のルールを定める Tが明らかな場合は，$cl_T(S)$ を単に $cl(S)$ と表す． □

定理 2 $4 \le s \le (1/4)(m/\log m)^{2/3}$とする．$f = \mathrm{CLQ}(m,s)$ とおく．このとき，

$$\rho(\mathcal{F}_f^+) \ge \frac{1}{3}\left(\frac{m}{4s^{3/2}\log m}\right)^{(\sqrt{s}+1)/4}$$

証明 まず，証明の流れを示す．証明の中の組合せ論的な議論は，対応する定理の Alon と Boppana による証明の場合と同様である．文中に “(主張 ?)” と記した点については全て後に証明することにして，ここでは成立するものとして扱う．

$t < (1/3)(m/(4s^{3/2}\log m))^{(\sqrt{s}+1)/4}$となる t に対して，t 個の Uの部分集合の対からなる $T = \{(A_i,B_i) \mid 1 \le i \le t\}$ が $\mathcal{F}_f^+$を切断すると仮定し，矛盾を導く．$i = 1,\ldots,t$, $j = 1,\ldots,t$ に対して，$A_{i,j} = A_i$, $B_{i,j} = B_i$とおき，t^2個の Uの部分集合の対からなる多重集合 T_2を

$$T_2 = \{(A_{i,j},B_{i,j}) \mid 1 \le i \le t, 1 \le j \le t\}$$

と定義する．Tを入力とし，$|T|^2$個の Uの部分集合の対 $T_2'(= \{(A'_{i,j},B'_{i,j}) \mid 1 \le i \le t, 1 \le j \le t\})$ を出力とする変換を Ex とする．この具体的な定義は後に示すものとするが，任意の $1 \le i,j \le t$ に対して，$A'_{i,j} \supseteq A_{i,j}$, $B'_{i,j} \supseteq B_{i,j}$を満たすように定義される．$U$の部分集合 Hを

$$H = \bigcup_{i,j \in \{1,\ldots,t\}} (A'_{i,j} - A_{i,j}) \cup (B'_{i,j} - B_{i,j})$$

と定義する．

ベクトル間の関係$\le$を，$v \le v' \Leftrightarrow \forall i \ v_i \le v'_i$と定義する．関係$\le$の元での $f^{-1}(1)$ の極小元の集合を V_m と表す．すなわち，

$$v \in V_m \Leftrightarrow v \in f^{-1}(1) \text{ かつ } \forall v' \lneq v \ v' \notin f^{-1}(1).$$

$w \in V_m$に対して $S_{w,0}$を

$$S_{w,0} = \{[x_i]_U \mid i \in true(w)\}$$

と定義する．ここに，$\{0,1\}^n$の要素 wに対して $true(w)$ は $w_i = 1$ となる添字 i からなる集合を表す．任意の $v \in V_m$に対して，$\phi \in cl_T(S_{v,0})$ が成り立つことは容易に確かめられる．ここで，$cl_T(S_{v,0})$ は $T = \{(A_i,B_i) \mid 1 \le i \le t\}$ に基づいた $S_{v,0}$の閉包を表す．同様に，S_{max}に Hを含めるとすると，T_2'に基づいた閉包 $cl_{T_2'}$に関して，任意の $v \in V_m$に対して $H \in cl_{T_2'}(S_{v,0})$ が成立する (主張 A)．定義より vに対応するグラフは s-クリークを只一つ含み，そのクリーク以外の辺を含まない．そこで，このグラフにおいてクリークを構成する頂点の集合を C_vで表す．グラフの頂点の集合 Cに対して，$\prod C$は，両端点が Cに含まれる辺に対応する論理変数の積として表される関数，すなわち，長さ $|C|(|C|-1)/2$ の単項関数を表すものとする．V_mの要素 vに対して，$F'_v \in \mathcal{M}^{|U|}$を

$$F'_v(D) = 1 \Leftrightarrow \exists C \subseteq C_v \text{ s.t. } |C| = \lceil\sqrt{s}\rceil \ [\Pi C]_U \subseteq D$$

と定義する．$\mathcal{F}_f'^+ \subseteq \mathcal{F}_f^+$を

$$\mathcal{F}_f'^+ = \{F'_v \mid v \in V_m\}$$

と定義する．このとき，任意の $v \in V_m$に対して $F'_v(H) = 0$ であるから (主張 B)，T'_2は F'_vを切断する (主張 C)．ところが，Ex の性質より，T'_2が $\mathcal{F}'^{+}_f$を切断するならば，$|T'_2|$ が定理の右辺の 2 乗を超えることが必要である (主張 D)．$|T'_2| = t^2$であるから，これは仮定に矛盾． □

さて，上の証明で残された点について順次示すことにする．まず，証明中で用いられる手続き Ex の定義を与える．

最初に，向日葵と呼ばれる集合族の構造に関する性質を定義する．グラフ $G = (V_G, E_G)$ の l個以下の頂点の集合からなる集合族を $\mathcal{V}(l)$ で表し，$\mathcal{W}$を $\mathcal{V}(l)$ の部分集合とする．rを整数とし，その具体的な値は後に定める．$\mathcal{W}$に対して以下の条件を満たす Zが存在する時 $\mathcal{W}$から Zが導出されると言い，$\mathcal{W} \vdash Z$と表すことにする．

条件：$\exists Z_1, \ldots, Z_r \in \mathcal{W} \exists Z \in \mathcal{V}(l) \forall i \neq j \; Z_i \cap Z_j \subseteq Z$

ここで，各 $Z_1, \ldots, Z_r$は必ずしも互いに異なる必要はない．例えば，$Z_1 \in \mathcal{W}$，$Z_1 \subseteq Z$，$|Z| \leq l$ならば，r個の Z_1は Zを導出する．集合族 $\mathcal{W}$に対して，

$$\forall Z(\mathcal{W} \vdash Z \Rightarrow Z \in \mathcal{W})$$

が成り立つ時，$\mathcal{W}$は閉じていると言うことにする．また，$\mathcal{V}(l)$ の部分集合 $\mathcal{W}$に対して，$\mathcal{V}(l)$ の部分集合 $\mathcal{W}^*$を

$$\mathcal{W}^* = \{Z \in \mathcal{V}(l) \mid \mathcal{W} \vdash Z \;\&\; Z \notin \mathcal{W}\}$$

と定義する．このとき，次が成り立つ．

補題 1 [1]　集合族 $\mathcal{W}$が閉じているならば，任意の $k \leq l$に対して，$\mathcal{W}$は要素数 k以下の極小要素を高々 $(r-1)^k$個含む． □

ここで，手続き Ex は以下の様に定義される．

```
Function Cl(A)      /*A ⊆ U */
begin
lp: W_A = {X ∈ V(l) | [ΠX]_U ⊆ A};
    if (W_A が閉じていない) then begin
        Z := W*_A の任意の極小要素;
        A := A ∪ [ΠZ]_U;
        goto lp;
    return A
end;
```

図 1:関数 Cl

```
Function Ex(T)      /* T = {(A_i, B_i) | 1 ≤ i ≤ t} */
begin
    for j := 1 to |T| do begin
        H_j = φ;
        for i := 1 to |T| do begin
            A'_{i,j} :=Cl(A_{i,j}); B'_{i,j} :=Cl(B_{i,j});
            H_j := (A'_{i,j} − A_{i,j}) ∪ (B'_{i,j} − B_{i,j}) ∪ H_j;
            A_{i,j} := A'_{i,j}; B_{i,j} := B'_{i,j};
        end;
        for k := j + 1 to |T| do begin
            for i := 1 to |T| do begin
                A_{i,k} := A_{i,k} ∪ H_j;
                B_{i,k} := B_{i,k} ∪ H_j;
            end;
        end;
    end;
    T' = {(A'_{i,j}, B'_{i,j}) | 1 ≤ i ≤ |T|, 1 ≤ j ≤ |T|}
    return T'
end.
```

図 2:関数 Ex

まず，主張 A を示す．

主張 A　$\phi \in cl_T(S_{v,0})$ ならば $H \in cl_{T'_2}(S_{v,0})$.

証明 (概略)　$S_{v,0}$に属する集合に Tに基づいたルール (1)，(2)，また T'_2に基づいたルール (1)，(2) を高々 i 回適用して得られる集合のクラスを，それぞれ $S_{v,i}$，$S'_{v,i}$と表す．

$S_{v,i}$に A_k，B_k，$A_k \cap B_k$が含まれるならば，$S'_{v,2i}$にそれぞれ $A'_{k,2i}$，$B'_{k,2i}$，$A'_{k,2i} \cap B'_{k,2i}$が含まれるという命題を任意の i に対して成り立つことを i に関する帰納法で証明することができる．従って，

$A'_{k,6(|T|+n)-2} \cap B'_{k,6(|T|+n)-2} \subseteq \cup_{j=1}^{6(|T|+n)-2} H_j \subseteq H$

より，$H \in cl_{T'_2}(S_{v,0})$.

□

m 個の頂点の集合 V_Gの色集合 $\{1, \ldots, g\}$ による彩色とは，V_Gから $\{1, \ldots, g\}$ への関数であり，この関数を c と表す．彩色 c で，頂点 vは $c(v)$ に彩色される．2 つ頂点が相異なる色に彩色されたとき，かつそのときにのみその頂点間に辺が存在するものとすると，彩色はひとつのグラフを指定する．以下では $g = s - 1$ に固定する．適当な彩色 c で指定されるグラフに対応する長さ n のベクトルの集合を U_{s-1} とあらわす．$U_{s-1} \subseteq f^{-1}(0)$ となることに注意されたい．$(s-1)^m$個の $s-1$ 色彩色から等確率で選ば

れた彩色に対応する(グラフに対応する)ベクトルを $u \in_R U_{s-1}$ と表す．U_{s-1}の部分集合 A に対して，$\mu(A)$ を

$$\mu(A) = \mathrm{Pr}_{u \in_R U_{s-1}}[u \in A]$$

と定義する．

さて主張 B を証明する．これには，次の 2 つの命題を示せば良い．何故ならば，$F'_v(H) = 1$ となる $v \in V_m$が存在するとすると，$|C| = \lceil\sqrt{s}\rceil$ となる $C \subseteq C_v$が存在して，$H \supseteq [\Pi C]$ となる．したがって，主張 B.1，B.2 より，$1/3 > \mu(H \cap U_{s-1}) \geq \mu([\Pi C]_{U_{s-1}}) \geq 1/3$ となり，矛盾が導かれるからである．$r = \lceil 4\sqrt{s}\log m\rceil$，$l = \lceil\sqrt{s}\rceil$ とする．

主張 B.1　$\lceil\sqrt{s}\rceil$ 個の頂点からなる任意の集合 C に対して，$\mu([\Pi C]_{U_{s-1}}) \geq 1/3$.

主張 B.2　$\mu(H \cap U_{s-1}) < 1/3$.

証明(主張 B.1)　$\mu([\Pi C]_{U_{s-1}})$ の値は，彩色 c をランダムに選んだときに Cに含まれる頂点に全て異なる色が割り当てられる確率に等しい．従って，

$$\mu([\Pi C]_{U_{s-1}}) = \frac{(s-1)(s-2)\cdots(s-\lceil\sqrt{s}\rceil)}{(s-1)^{\lceil\sqrt{s}\rceil}} \geq 1/3.$$

□

証明(主張 B.2)　関数 $\mathrm{C_L}$ で，同じ Zの値に対して，2 度以上 if 文の条件節が成立することはないので，ループの繰り返し回数は，高々$\sum_{l=1}^{\lceil\sqrt{s}\rceil}\binom{m}{l} \leq m^{\lceil\sqrt{s}\rceil} < m^{\sqrt{s}+1}$回である．関数 Ex による関数 $\mathrm{C_L}$ の呼び出しは，丁度 $2t^2$ 回行なわれる．さらに，$\mu((\mathrm{C_L}(A) - A) \cap U_{s-1})$ の値が，

$$\mu((\mathrm{C_L}(A) - A) \cap U_{s-1}) \leq \left\{1 - \frac{(s-1)(s-2)\cdots(s-\lceil\sqrt{s}\rceil)}{(s-1)^{\lceil\sqrt{s}\rceil}}\right\}^r$$

を満たすことは，文献 [1] の補題 3.6 と全く同様にして証明できる．したがって，

$$\mu(H \cap U_{s-1}) \leq 2t^2 m^{\sqrt{s}+1}\left\{1 - \frac{(s-1)(s-2)\cdots(s-\lceil\sqrt{s}\rceil)}{(s-1)^{\lceil\sqrt{s}\rceil}}\right\}^r.$$

簡単な計算により，この値は 1/3 未満であることが示される．□

主張 C は 4 章に示した補題 2と同じものである(証明は 4 章に譲る)．残されたのは主張 D である．Uの部分集合 Dに対して，$\mathcal{W}_D$を

$$\mathcal{W}_D = \{C \in \mathcal{V}(l) \mid [\Pi C]_U \subseteq D\}$$

とおき，$\mathcal{W}_D$の極小要素の集合を $\mathcal{W}_D^m$とおく．また，頂点集合 Cに対して，$[\Pi C]_U \subseteq D$，かつ任意の $C' \subsetneq C$に対して，$[\Pi C']_U \not\subseteq D$ を満たす時，$[\Pi C]_U \subseteq_m D$ と書く．T'_2の要素 (A, B) が F'_vを切断するためには，ある C_vの要素数 $\lceil\sqrt{s}\rceil$ 以下の部分集合 C_1と C_2に対して，

$$[\Pi C_1]_U \subseteq_m A \;\&\; [\Pi C_2]_U \subseteq_m B \;\&\; |C_1 \cup C_2| > \lceil\sqrt{s}\rceil$$

を満たすことが必要である．このとき，$\mathcal{W}_A^m$，$\mathcal{W}_B^m$ は閉じていることに注意されたい．従って，あとは文献 [1] と全く同様の議論によって T'_2の各要素 (A, B) が F'_vを切断し得る $v \in V_m$の個数 jは，

$$j \leq 4\left(\frac{s(r-1)}{m}\right)^{\lceil(\lceil\sqrt{s}\rceil+1)/2\rceil}\binom{m}{s}$$

を満たすことが示される．従って，$|F'_f| = \binom{m}{s}$に注意すると，主張 D は直ちに導かれる．□

4　単調回路と一般の回路に対する近似モデルの差

近似法において単調複雑さの下界を与える近似モデル $\mathcal{F}_f^+$と否定も許した回路における複雑さの下界を与える近似モデル $\mathcal{F}_f$の違いについて考えてみる．本節では下界を証明しようとする対象を単調論理関数に限定する．クリーク関数やハミルトニアン閉路問題など多くの NP-完全問題に対応する論理関数は単調であることに注意されたい．

以下本節を通じて，fを n 変数単調論理関数とし，$U = f^{-1}(0)$，$V = f^{-1}(1)$ とする．定義より，$\mathcal{F}_f \subseteq \mathcal{F}_f^+$は明らかである．そこで，$\mathcal{F}_f^\Delta = \mathcal{F}_f^+ - \mathcal{F}_f$とおく．この時，

$$\max\{\rho(\mathcal{F}_f), \rho(\mathcal{F}_f^\Delta)\} \leq \rho(\mathcal{F}_f^+) \leq \rho(\mathcal{F}_f) + \rho(\mathcal{F}_f^\Delta)$$

が成り立つことは定義より明らかである．

これまでに，幾つかの関数 fに対して$\rho(\mathcal{F}_f^+)$ が指数関数的であるということが示されている．一方，$\rho(\mathcal{F}_f)$ に対する非線形の下界は示されていない．では，$\rho(\mathcal{F}_f^\Delta)$ は何を意味するのか．まず，Berkowitz [2] によって導入された擬似補関数という概念を示す．

定義 4　f, $h_i \in \mathcal{M}^n$とする．fを計算する，どの様な論理回路に対しても，$\bar{x_i}$を h_iで置き換えて得られる回路もまた fを計算する時，h_iを fに関して x_i の擬似補関数 (pseudo complement) であるという．$H =< h_1, \ldots, h_n >$，$h_i \in \mathcal{M}^n$が fの擬似補関数ベクトルであるとは，各 $1 \leq i \leq n$ に対して h_iが fに関する x_iの擬似補関数であることをいう．

擬似補関数，擬似補関数ベクトルとも，一般には一意ではない．擬似補関数については次の定理が知られている．

定理 3 [5]　$h_i \in \mathcal{M}^n$が $f \in \mathcal{M}^n$に関して x_iの

擬似補関数である為の必要十分条件は,

$$f_{|x_i=0} \leq h_i \leq f_{|x_i=1}$$

を満たすことである．但し，$e=0$ または，$e=1$ に対して，$f_{|x_i=e}$ は fに部分割り当て $x_i=e$ を施して得られた関数を表すものとする．□

fを n 変数単調論理関数とする．fの擬似補関数ベクトルに含まれる全ての関数を単調論理回路で計算するのに必要なゲートの個数を fの擬似補関数の複雑さと呼び，$\mathrm{size}_{mon}(H(f))$ と表す．すなわち,

$$\mathrm{size}_{mon}(H(f)) = \min\{\mathrm{size}_{mon}(H) \mid H\text{が } f\text{の擬似補関数ベクトル}\}.$$

f自身は，fに関するどの x_iの擬似補関数でもあるので $\mathrm{size}_{mon}(H(f)) \leq \mathrm{size}_{mon}(f)$ が成り立つ．また，fを計算する論理回路の入力に現われる $\bar{x_1},\ldots,\bar{x_n}$ を，その擬似補関数 $h_1,\ldots,h_n$を計算する単調論理回路で置き換えると，結果として，fを計算する単調論理回路が得られることから，関係式 $\mathrm{size}(f) + \mathrm{size}_{mon}(H(f)) \geq \mathrm{size}_{mon}(f)$ も成立する．このとき，以下の定理が成り立つ．

定理 4　$f \in \mathcal{M}^n$とする．このとき,

$$\rho(\mathcal{F}_f^{\Delta}) \leq \mathrm{size}_{mon}(H(f)).$$

証明　fの擬似補関数ベクトルに含まれる全ての関数を計算し，そのサイズが $\mathrm{size}_{mon}(H(f))$ に等しい単調回路を Cとする．Cの入力端子，出力端子の個数は共に nである．Cに含まれる AND ゲートの入力線で計算される関数を g，h とし，$A=g^{-1}(1)\cap U$，$B=h^{-1}(1)\cap U$とした時に，Cの全ての AND ゲートに対する対 (A,B) を集めた集合 $T=\{(A,B)\}$ が $\mathcal{F}_f^{\Delta}$を切断することを示せば十分である．

$v\in\{0,1\}^n$に対して，$\{i \mid v_i=1\}$ と $\{i \mid v_i=0\}$ をそれぞれ $true(v)$ と $false(v)$ と表すと，$\mathcal{F}_f^{\Delta}$は

$$\bigcup_{v\in V}\{F\in F^+_{U,v} \mid \exists i\in false(v)\, F([x_i])=F([\bar{x}_i])=0\}$$

に等しい．

$F\in\mathcal{F}_f^{\Delta}$を任意に選び固定する．ある $v\in V$と $i\in false(v)$ に対して，$F\in F^+_{U,v}$，$F([x_i])=F([\bar{x}_i])=0$ が成立することも容易に確かめられる．$f(v)=1$，$\bar{x}_i(v)=1$であるから，定理 3より $h_i(v)=1$．従って，Fが Tで切断されていないと仮定すると，$F([h_i])=1$．定理 3より $[h_i]\subseteq[\bar{x}_i]$ であるから，$F([\bar{x}_i])=1$．これは，$F([x_i])=F([\bar{x}_i])=0$ に矛盾する．従って，Fは Tで切断される．以上で (i) は証明された．□

上の定理より，単調最大近似モデル $\mathcal{F}_f^+$と最大近似モデル $\mathcal{F}_f$の差 $\mathcal{F}_f^{\Delta}$ に対する最小切断対のサイズは，擬似補関数の複雑さの下界を与えることがわかる．

注) 単調論理関数 fに対して一般的に成立する，単調複雑さと擬似補関数の複雑さの差の大きさを表す不等式は知られていない．NP-完全問題で，かつ，$\mathrm{size}_{mon}(H(f))$ の値が小さくなることが示されている関数が存在することは知られている [14].

さて，**3** で示したクリーク関数 fの単調最大近似モデル $\mathcal{F}_f^+$ に対する$\rho(\mathcal{F}_f^+)$の指数関数下界の証明と，$\rho(\mathcal{F}_f)$ や$\rho(\mathcal{F}_f^{\Delta})$ の関係について考えてみる．上で見てきたように $\mathcal{F}_f^+=\mathcal{F}_f\cup\mathcal{F}_f^{\Delta}$ が成立するので，この証明を解析することで，クリーク関数の非単調回路における複雑さの下界を与える領域 $\mathcal{F}_f$に対する最小切断対を求める問題を解くための，何らかの手がかりを得ることができないかという疑問が生じる．我々は，この見地に立って解析を進めたところ，**3** に示した証明においては，領域 $\mathcal{F}_f$に依存した議論は用いられておらず，$\rho(\mathcal{F}_f^+)$ の下界は主に $\mathcal{F}_f^{\Delta}$を切断しているという事実を根拠にして求められているという結論を得た．よって，$\mathcal{F}_f^+$を $\mathcal{F}_f^{\Delta}$で置き換えたとしても同様の議論が成立し，結論として$\rho(\mathcal{F}_f^+)$ に対して得られたのと全く同じ値の下界が$\rho(\mathcal{F}_f^{\Delta})$ に対しても得られる．このことは，この様な従来の議論に基づいた証明からは領域 $\mathcal{F}_f$の最小切断対の個数を求める為の手がかりを得ることも難しいということを示唆していると考えられる．以下でこのことについて述べる．

まず，準備として，幾つかの補題を挙げる．共に証明は省略する．

補題 2　$w\in V$，$F\in\mathcal{F}_{U,w}$とする．$C\in cl_T(S_{w,0})$ が存在して，$F(C)=0$ となるとき，Tは Fを切断する．□

補題 3　Uの部分集合の対の集合 Tが $\mathcal{F}_f^{\Delta}$を切断しているとする．このとき，次が成り立つ．

$$\forall v\in V\forall i\in false(v)\ ([x_i]\in cl_T(S_{v,0})\text{ または }[\bar{x}_i]\in cl_T(S_{v,0})).$$

□

さて，定理 2の証明に現われる $\mathcal{F}_f^+$を $\mathcal{F}_f^{\Delta}$に置き換えて，証明の流れを追ってみることにする．$cl_{T_2'}$ の定義の直前までは，任意の $v\in V_m$に対して，$\phi\in cl_T(S_{v,0})$ が成り立つとしてある部分を，上で示した補題 3で置き換えるのみで，その他は全く同様とする．T_2'に基づく閉包 $cl_{T_2'}$を定義する際に S_{max}に要素 $[x_i]\cup H$，$[\bar{x}_i]\cup H$を加える．主張 A は次に示す主

張 A' で置き換える.

主張 A' 任意の $v \in V_m$と，任意の $i \in false(v)$ に対して，$[x_i] \cup H$または $[\bar{x}_i] \cup H$が $cl_{T_2'}(S_{v,0})$ に属する. □

主張 A' は補題 3を考慮すると，主張 A と同様にして証明できる. 主張 B に対応する主張 B' は次のようにする.

主張 B' 任意の $v \in V_m$と，任意の $i \in false(v)$ に対して，

$$F_v'([x_i] \cup H) = 0 \text{ かつ } F_v'([\bar{x}_i] \cup H) = 0.$$

□

vを V_mの任意の要素とする. 主張 B' は C_vの部分集合で要素数が $\lceil \sqrt{s} \rceil$ である任意の Cと，$false(v)$ に属する任意の iに対して，$\mu([\Pi C \wedge x_i] \cap U_{s-1}) \geq 1/(3m)$，$\mu([\Pi C \wedge \bar{x}_i] \cap U_{s-1}) \geq 1/(3m)$(主張 B'.1)，$\mu(H \cap U_{s-1}) < 1/(3m)$(主張 B'.2) を示せば十分である.

上で述べた条件を満たす v, i, Cに対して，$\mu([\Pi C \wedge x_i] \cap U_{s-1})$ は，$(s-1)$ 彩色 cをランダムに選んだ時に，Cに含まれる各頂点に全て異なる色が割り当てられ，かつ，x_iに対応する頂点間に異なる色が割り当てられる確率に等しい. このことと，主張 B より，簡単な計算によって，主張 B'.1 は証明でき，また，主張 B'.2 は主張 B.2 と全く同様にして証明できる. 主張 A', B' と主張 2より F_v'が T_2'で切断されることが導かれ，これが主張 C に相当する. 主張 D に関しては変更する必要はない. 結論として，以下の結果が得られた. 定理 5の右辺の値は，定理 2で示したクリーク関数に対する下界の値と等しい.

定理 5 $9 \leq s \leq (1/4)(m/\log m)^{2/3}$とし，$f = \mathrm{CLQ}(m,s)$ とおく. このとき，

$$\rho(\mathcal{F}_f^{\Delta}) \geq \frac{1}{3}\left(\frac{m}{4s^{3/2}\log m}\right)^{(\sqrt{s}+1)/4}.$$

□

定理 5, 6 より直ちに $\mathrm{size}_{mon}(H(f)) \geq (1/3)(m/4s^{3/2}\log m)^{(\sqrt{s}+1)/4}$ なる結果が得られる. また，これより次の系も示すことができる.

系 1 $9 \leq s \leq (1/4)(m/\log m)^{2/3}$とし，$f = \mathrm{CLQ}(m,s)$ とおく. hを fの任意の変数の擬似補関数とする. このとき，

$$\mathrm{size}_{mon}(h) \geq \frac{2}{3m(m-1)}\left(\frac{m}{4s^{3/2}\log m}\right)^{(\sqrt{s}+1)/4}$$

□

参考文献

[1] N. Alon and R. B. Boppana, "The Monotone Circuit Complexity of Boolean Functions", *Combinatorica*, Vol. 7, No. 1, pp. 1–22, 1987.

[2] S. Berkowitz, "On Some Relationships Between Monotone and Non-monotone Circuit Complexity", *Technical Report, Univ. of Toronto*, 1982.

[3] R. Beals, T. Nishino and K. Tanaka, "More on the Complexity of Negation-Limited Circuits", *Proc. of 27th STOC*, pp. 585–595, 1995.

[4] R. B. Boppana and M. Sipser, "The Complexity of Finite Functions", *Handbook of Theoretical Computer Science*, pp. 758–804, Elsevier Science Pub. B. V., 1990.

[5] P. E. Dunne, "Techniques for the Analysis of Monotone Boolean Networks", *Ph.D Dissertation; Theory of Computation Report, Univ of Warwick*, No. 69, 1984.

[6] J. Håstad, "Almost Optimal Lower Bounds for Small Depth Circuits", *Advances in Computer Reserch*, Vol. 5, 1986.

[7] M. Karchmer, "On Proving Lower Bounds for Circuit Size", *Proc. 8th Structure in Complexity Theory*, pp. 112–118, 1993.

[8] K. Nakayama and A. Maruoka, "Loop Circuits and Their Relation to Razborov's Approximation Model", *Information and Computation*, Vol 119, No. 2, pp. 154–159, 1995.

[9] A. A. Razborov, "Lower Bounds on the Monotone Complexity of Some Boolean Functions", *Sov. Math. Doklady*, Vol 31, pp. 354–357, 1985.

[10] A.A. Razborov, " Lower Bound on the Monotone Complexity of the Logical Permanent", *Math. Notes of the Acad. of Sci. of the USSR*, Vol 37, pp. 485–493, 1985.

[11] A. A. Razborov, "On the Method of Approximations", *Proc. of 21st STOC*, pp. 167–176, 1989.

[12] A. A. Razborov and S. Rudich, "Natural Proofs", *Proc. of 26th STOC*, pp. 204– 213, 1994.

[13] I. Wegner, "On the Complexity of Slice Functions", *Theoretical Computer Science*, Vol. 38, pp. 55–68, 1985.

[14] I. Wegener, *The Complexity of Boolean Funcions*, B. G. Teubner, 1987.