数理解析研究所講究録
992巻 1997年 199-206

論理関数の複雑さと近似演算

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
980-77 仙台市青葉区荒巻字青葉
E-Mail: {ama|maruoka}@ecei.tohoku.ac.jp

あらまし　Razborov(1985) がクリーク関数を計算する単調論理回路のサイズに対する多項式を超える下界を証明して以来，Andreev(1985)，Alon と Boppana(1987)，Haken(1995)，天野と丸岡 (1996) らが様々な手法を用いて，特定の関数を計算する単調論理回路のサイズに対する指数関数の下界を証明した．本稿では，一見異なるこれらの証明が全て近似法と呼ばれる手法によるものか，または，その本質的な部分を損なわずに近似法による証明に再構成できることを示し，更に，これらの証明の本質的な部分が全て類似の組合せ論的議論に基づいていることを明らかにする．また，この様な従来型論法の限界点についても議論し，サイズ $s(s$ は定数とする) のクリークが含まれるか否かを判定する関数を計算する単調論理回路のサイズの下界について，この型の証明では，既知の最良の値を凌ぐ結果は導き得ないことを示す．

1　はじめに

与えられた論理関数を計算する論理回路の最小サイズ—これをその論理関数の**複雑さ**と呼ぶ—の下界を求めるという問題は，長年に渡る精力的な研究にもかかわらず，現在までに知られている最良の下界は入力変数の個数の4倍という小さな値に過ぎない．一方，論理回路に単調という制約を設けた場合，つまり，与えられた論理関数を計算する単調論理回路の最小サイズ—これをその論理関数の**単調複雑さ**と呼ぶ— の下界を求めるという問題に関しては，最近大きな進展がみられる．すなわち，Razborov[7] がクリーク関数の単調複雑さに対する超多項式の下界を示したのを皮切に，これまでに Andreev[3]，Alon と Boppana[1]，Haken[5]，天野と丸岡 [2] らが幾つかの証明法を用いて，幾つかの関数に対する単調複雑さの指数関数の下界を導出した．しかし，単調という制約を外した元の問題に関しては，強い下界導出の糸口さえ掴めていないのが現状である．

本稿では，従来の単調複雑さの下界導出法についてより深く分析し，下界導出のための新たな手法の開発の手がかりをつかむことを目的とする．具体的には，先に挙げた従来の単調複雑さの下界の証明は，全て類似の議論に基づいていることを明らかにするとともに，従来の議論による証明の限界についても言及する．

本稿の構成と具体的な内容は次の通りである．2章では，本稿で用いる記号や記法などの諸定義を行ない，3章では，単調複雑さの下界の証明法として有効な近似法と呼ばれる手法について概説する．4章では，後に種々の証明を比較，解析する際に有用となる集合族に関する性質を3つ示し，これらの関係について述べる．5章では，これまでに知られている単調複雑さの下界の証明について議論し，それらの全てが近似法によるものであるか，またはその証明の本質的な部分を損なわずに近似法による証明に再構成できることを述べるとともに，証明の本質的な部分となる組合せ論的議論も，全ての証明において類似していることを明らかにする．6章では，これらの従来の証明法の限界を示す実例として，クリーク関数の単調複雑さに対する既知の最良の下界が，既にこの型の証明によって得られる最良の値となっていることを示す．

2　諸定義

n 変数論理関数の集合を $\mathcal{B}_n$ と表す．$\{x_1,\ldots,x_n,\bar{x}_1,\ldots,\bar{x}_n\}$ 上の項の集合を $\mathcal{T}_n$ と表す．$\{0,1\}^n$ の要素 v に対して，$v^{(i)}$ で v の i ビット目を表し，$||v||$ で v 中の1の個数を表す．u と v を $\{0,1\}^n$ の要素とする．全ての $1\leq i\leq n$ に対して，$u^{(i)}\leq v^{(i)}$ が成り立つとき $u\leq v$ と書く．f を n 変数論理関数とする．f の任意の入力 u と v に対して，$u\leq v$ ならば $f(u)\leq f(v)$ が成り立つとき，特に f を**単調論理関数**と呼ぶ．f の主項の中で最も変数の個数の多い項に現われる変数の個数を f の**階数**と呼び，$rank(f)$ と書く．n 変数論理関数 f_1 と f_2 の間に，任意の入力 v に対して $f_1(v)\leq f_2(v)$ の関係があるとき，$f_1\leq f_2$ と表す．f の主項の集合を $PI(f)$ と，主節の集合を $PC(f)$ と，それぞれ表す．n 変数論理関数 f より定まる項の集合 $I(f)$ を $I(f)=\{T\in\mathcal{T}_n\mid\exists T'\in PI(f)\ T\leq T'\}$ と定義する．論理関数 f_1 と f_2 に対して，f_1-f_2 を $f_1(v)=1$ かつ $f_2(v)=0$ となる入力 v に対してのみ値1をとる論理関数とする．論理関数 f に対して $[f]$ は $f(v)=1$ となる入力 v 全体の集合を表すものとする．n 変数論理関数 f と $\{0,1\}^n$ の部分集合 V に対して V の部分集合 $[f]_V$ を $[f]_V=\{v\in V\mid f(v)=1\}$ と定義する．

論理回路とは入力結線には定数(0または1)かリテラル(すなわち，論理変数またはその否定)が割り当てられた，2入力AND(以下$\wedge$)ゲートとOR(以下$\vee$)ゲートからなる非周期的な回路である．入力結線に変数の否定が現われない論理回路を，特に**単調論理回路**という．論理関数fに対して，fを計算する論理回路のうち最もゲート数の少ないもののゲート数をfの**複雑さ**と呼ぶ．同様に，単調論理関数fに対して，fを計算する単調論理回路のうち最もゲート数の少ないもののゲート数をfの**単調複雑さ**と呼び$size_{mon}(f)$と表す．

3 近似法

本稿における主目的は，従来の単調複雑さの下界の証明を解析し，従来型手法の可能性と限界を明らかにすることである．従来の単調複雑さの下界の証明法において，最も重要なものの一つがRazborov[7]によって開発された近似法と呼ばれる手法である．実際，Razborov[6]による証明，AlonとBoppana[1]による証明，天野と丸岡[2]による証明は近似法に基づくものである．また，本稿では後にこれ以外の証明も，その本質的な部分を損なわずに近似法の枠組に沿った証明に再構成できることを示す．そこで，本章では近似法について大まかに説明する．

下界を求める対象とするn変数単調論理関数をfとする．ゲート数tの単調論理回路Cがfを計算しているとする．$\overline{\wedge}$と$\overline{\vee}$を$\mathcal{B}_n \times \mathcal{B}_n$から$\mathcal{B}_n$への写像とし，これらを**近似演算**または**近似ゲート**と呼ぶ．回路Cの結線は変えずに，C中の$\vee$ゲートを全て$\overline{\vee}$で，$\wedge$ゲートを全て$\overline{\wedge}$で置き換えて得られる回路をCの**近似回路**と呼び$\overline{C}$と表し，$\overline{C}$が計算する関数を$\overline{f}$とおく．$\overline{C}$の各ゲートに計算の順序に矛盾しないように$1,\ldots,t$の番号を付け，i番目のゲートの入力結線が計算する関数を$\overline{g}_i$と$\overline{h}_i$とおく．$\overline{C}$のi番目のゲートに対応するCのゲートの機能($\wedge$または$\vee$)を$\star_i$とおく．

$[f-\overline{f}]$と$[\overline{f}-f]$をそれぞれ回路全体の正誤差と負誤差と呼び，$[(\overline{g}_i \star_i \overline{h}_i)-(\overline{g}_i \overline{\star}_i \overline{h}_i)]$と$[(\overline{g}_i \overline{\star}_i \overline{h}_i)-(\overline{g}_i \star_i \overline{h}_i)]$をそれぞれ$i$番目のゲートの正誤差と負誤差と呼ぶ．このとき，回路全体の正誤差(同様に負誤差)に含まれる全ての入力vはある$i \in \{1,\ldots,t\}$番目のゲートの正誤差(同様に負誤差)に含まれることを示すことができる[1, 7].

近似法を用いて下界を証明する際には，通常，入力全体ではなくテスト入力として与えられる一部の入力に対する近似回路の振舞いを解析する．このテスト入力に対応するものとして，UとVを，それぞれ$f^{-1}(0)$と$f^{-1}(1)$の部分集合とする．入力結線に定数か変数が割り当てられ，$\overline{\vee}$と$\overline{\wedge}$ゲートのみからなる論理回路で計算可能な関数のクラスを，$\overline{\vee}$と$\overline{\wedge}$より定まる**近似モデル**と呼び$\mathcal{M}$と表す．領域UとVに関する論理関数fと$\mathcal{M}$の距離$\overline{\rho}(f,\mathcal{M},U,V)$を以下を満たす最小の$s$と定義する: ある$\overline{f},\overline{g}_1,\ldots,\overline{g}_s,\overline{h}_1,\ldots,\overline{h}_s \in \mathcal{M}$と$\star_1,\ldots,\star_s \in \{\wedge,\vee\}$が存在して

$$[f-\overline{f}]_V \subseteq \bigcup_{i=1}^{s}[(\overline{g}_i \star_i \overline{h}_i)-(\overline{g}_i \overline{\star}_i \overline{h}_i)]_V \tag{1}$$

$$[\overline{f}-f]_U \subseteq \bigcup_{i=1}^{s}[(\overline{g}_i \overline{\star}_i \overline{h}_i)-(\overline{g}_i \star_i \overline{h}_i)]_U \tag{2}$$

を満たす．

また，特に$\overline{\rho}(f,\mathcal{M},f^{-1}(0),f^{-1}(1))$の値を$f$と$\mathcal{M}$の距離と呼び$\rho(f,\mathcal{M})$と表す．上で述べた議論より，$size_{mon}(f) \geq \rho(f,\mathcal{M}) \geq \overline{\rho}(f,\mathcal{M},U,V)$が成り立つ．つまり，$\rho(f,\mathcal{M})$や$\overline{\rho}(f,\mathcal{M},U,V)$に対する下界が示せれば，これをそのまま$f$の単調複雑さの下界として良いことが保証される．

したがって，近似法による証明は通常次の手順を踏む．まず，所望の論理関数に対して特徴的な入力をUとVとする．次に，適当な近似演算$\overline{\vee}$と$\overline{\wedge}$を定義する．この際なるべく回路全体の誤差が大きく，かつ各ゲートの誤差が小さくなるように，うまく定義することが肝要となる．その後，$\overline{\vee}$と$\overline{\wedge}$より定まるモデル$\mathcal{M}$に対して，距離$\rho(f,\mathcal{M},U,V)$を求め，fの複雑さの下界を得る．

4 閉包，矩形，安定

本章では，従来の単調複雑さの下界の証明をより詳しく解析するために，集合族に対する閉包，矩形，安定という3つの概念を定義し，またこれらの間の関係について調べる．

一つめの性質は，閉包とよばれる概念で，これはAlonとBoppana[1]がクリーク関数などに対する下界を示す際に用いたものである．二つめは，矩形と呼ばれる概念で，これは天野と丸岡[2]がクリーク関数などに対する下界を示す際に用いた概念を一般化したものである．三つめは，安定と呼ばれる概念で，これは，上の両者を統合的に扱うことのできる性質である．以下，これらの正確な定義について述べる．

$V=\{1,\ldots,n\}$ とする．rとlを適当な正整数とする．Vの要素数 l以下の部分集合全体からなる集合族を$\mathcal{V}(l)$ と表す．$\mathcal{V}$をVの巾集合の部分集合とする．任意の$\mathcal{V}$の要素 A とVの部分集合 Bに対して，$B\supseteq A$ ならば $B\in\mathcal{V}$を満たしているとき，$\mathcal{V}$は**上向きに閉じている**という．族 $\mathcal{V}$に対して $\lceil V\rceil$ は$\mathcal{V}$の全ての要素を含み上向きに閉じている最小の族を表すものとする．Aが族 $\mathcal{V}$に属し，かつ $A'\subsetneq A$ を満たす如何なる要素 A'も $\mathcal{V}$ に属さないとき，A を$\mathcal{V}$の**極小要素**という．族 $\mathcal{V}$に対して $\mathcal{V}$の極小要素の集合を $\lfloor\mathcal{V}\rfloor$ と表す．

必ずしも互いに異なっている必要のない Vの部分集合 $L,L_1,\ldots,L_r$が以下の (i) と (i) を満たすとき，$L_1,\ldots,L_r$は L を**導出する**といい，$L_1,\ldots,L_r\vdash_{(r,l)}L$ と表す．

(i) $L,L_1,\ldots,L_r$の要素数は全て l以下，

(ii) 任意の $1\leq i<j\leq r$に対して，$L_i\cap L_j\subseteq L$.

例えば，それぞれがサイズ l以下である集合 L'と L が $L'\supseteq L$ を満たすならば，r個の L のコピーは L'を導出する．Vの部分集合の族 $\mathcal{V}$に $L_1,\ldots,L_r\vdash_{(r,l)}L$ を満たす $L,L_1,\ldots,L_r$が含まれるとき，$\mathcal{V}$は L を導出するといい，$\mathcal{V}\vdash_{(r,l)}L$ と表す．族 $\mathcal{V}$が (r,l)-**閉包**であるとは，$\mathcal{V}\subseteq\mathcal{V}(l)$ かつ $\forall L(\mathcal{V}\vdash_{(r+1,l)}L\rightarrow L\in\mathcal{V})$ を満たすことをいう．族 $\mathcal{V}$が (r,n)-閉包であるとき，特に r-閉包という．

定義 1　集合族を要素とするクラス CL_rと $\mathrm{CL}_{r,l}$をそれぞれ以下の様に定義する．

$$\begin{aligned}\mathrm{CL}_r &= \{\lceil\mathcal{V}\rceil \mid \mathcal{V}\text{が } r\text{-閉包 }\},\\ \mathrm{CL}_{r,l} &= \{\lceil\mathcal{V}\rceil \mid \mathcal{V}\text{が } (r,l)\text{-閉包 }\}.\end{aligned}$$

□

閉包の基本的な性質として，次のことが知られている．

命題 2 [1]　次の 2 つが成り立つ．

(i) $\mathcal{V}\subseteq\mathcal{V}(l)$ が (r,l)-閉包であるならば，任意の l以下の正整数 l'に対して，$\mathcal{V}$の極小要素で，かつサイズ l'以下の要素の数は高々$r^{l'}$.

(ii) $\mathcal{V}_1,\mathcal{V}_2\subseteq\mathcal{V}(l)$ がともに (r,l)-閉包であるとする．このとき，$\mathcal{V}_1\cap\mathcal{V}_2$も (r,l)-閉包である．

□

集合族 $\mathcal{V}\subseteq\mathcal{V}(l)$ が (r,l)-**矩形**であるとは，$i=1,\ldots,l$に対して Vの部分集合 L_iで $|L_i|\leq r$を満たすものが存在して，$\lceil\mathcal{V}\rceil=\lceil L_1\times L_2\times\cdots\times L_l\rceil$ が成り立つことをいう．ある正整数 lが存在して $\mathcal{V}$が (r,l)-矩形であるとき，$\mathcal{V}$は単に r-矩形であるという．この性質を理解するためには，Vの部分集合 A に $T_A=\wedge_{i\in V}x_i$なる項を対応させ，族 $\mathcal{V}$に $D_{\mathcal{V}}=\vee_{A\in\mathcal{V}}T_A$なる DNF 式を対応させて考えるのがわかり易い．こうすると，族 $\mathcal{V}$は，その極小要素を主項とする論理関数を表していると考えられる．族 $\mathcal{V}$が (r,l)-矩形であることと，$D_{\mathcal{V}}$が表す関数が節数 l以下の r-CNF 式で表現可能であることとは同値である．また，$\mathcal{V}$が r-矩形であることと，$D_{\mathcal{V}}$が表す関数が r-CNF 式で表現可能であることとが同値である．

定義 3　集合族を要素とするクラス BL_rと $\mathrm{BL}_{r,l}$ をそれぞれ以下の様に定義する．

$$\begin{aligned}\mathrm{BL}_r &= \{\lceil\mathcal{V}\rceil \mid \mathcal{V}\text{が } r\text{-矩形 }\},\\ \mathrm{BL}_{r,l} &= \{\lceil\mathcal{V}\rceil \mid \mathcal{V}\text{が } (r,l)\text{-矩形 }\}.\end{aligned}$$

□

族 $\mathcal{V}$が (r,l)-**安定**であるとは，l以下の任意の正整数 s に対して，$\mathcal{V}$の極小要素でかつ要素数 s 以下であるものの個数が r^s以下であることをいう．

定義 4　集合族を要素とするクラス $\mathrm{ST}_{r,l}$を以下の様に定義する．

$$\mathrm{ST}_{r,l} = \{\lceil\mathcal{V}\rceil \mid \mathcal{V}\text{が } (r,l)\text{-安定 }\}.$$

□

上で定義した幾つかのクラスは，次に示す包含関係を満たす．これは，閉包と矩形の概念が類似した性質を持っていることを示している．

定理 5

$$\begin{array}{ccccc} & \subseteq & \mathrm{BL}_r=\mathrm{CL}_r & \subseteq & \\ \mathrm{BL}_{r,l} & & & & \mathrm{ST}_{r,l}\\ & \subseteq & \mathrm{CL}_{r,l} & \subseteq & \end{array}$$

証明　$\mathrm{BL}_{r,l}\subseteq\mathrm{BL}_r$は定義より明らかである．$\mathrm{CL}_{r,l}\subseteq\mathrm{ST}_{r,l}$は命題 2 の (ii) より直ちに導かれる．残りの包含関係について順次証明する．

($\mathrm{BL}_{r,l}\subseteq\mathrm{CL}_{r,l}$)　族 $\mathcal{V}$が $\mathrm{CL}_{r,l}$に属し，かつ $\mathrm{BL}_{r,l}$ には属さないと仮定する．定義より，$\mathcal{V}$は上向きに閉じていることに注意されたい．このとき，互いに異なる $\mathcal{V}$の極小要素 $L_1,\ldots,L_{r+1}$と $L\notin\mathcal{V}$が存在して，

$L_1,\ldots,L_{r+1}$はLを導出する．また，各々要素数r以下の集合$M_1,\ldots,M_l$が存在して，$\mathcal{V}=\lceil M_1\times\cdots\times M_l\rceil$．もし，全ての$i=1,\ldots l$に対して，$M_i$と$L$が通部分をもつならば，$L\in\mathcal{V}$となり矛盾．したがって，ある$1\leq k\leq l$に対して，$M_k$と$L$は共通部分を持たない．$i=1,\ldots,r+1$に対して$L_i$が$\mathcal{V}$の極小要素であるためには，$L_i-L$の要素が必ず$M_k$に含まれていなければならない．閉包の定義より$L_i-L$は各$i$について互いに素であるから，$M_k$は$r+1$個以上の要素を含むことになり，これは仮定に矛盾する．

($\mathrm{BL}_r\subseteq\mathrm{ST}_{r,l}$)　　$\mathcal{V}$がBL_rに属しているとする．このとき，ある定数kに対して，各々要素数r以下の集合$L_1,\ldots,L_k$が存在し，$\mathcal{V}=\lceil L_1\times\cdots\times L_k\rceil$を満たす．したがって，$\mathcal{V}$の極小要素は$\lfloor\lceil L_1\times\cdots\times L_k\rceil\rfloor=\lfloor L_1\times\cdots\times L_k\rfloor$に等しい．ここで，$L_1,\ldots,L_k$から，各辺に$V$の要素がラベル付けされた木$T_k$を次の様に再帰的に構成する．

T_0を根のみからなる木とする．

T_iが与えられているとする．vをT_iの葉とする．根からvへ到達する道上にある辺にラベル付けされた要素の集合とL_{i+1}が互いに素であるならば，T_iにvを始点としてL_{i+1}の各要素がラベル付けされた辺を加える．もしそうでなければ，なにもしない．以上の作業をT_iの全ての葉について行ない，得られた木をT_{i+1}とする．

こうして得られた木T_kの根から葉に至る道上の辺にラベル付けされた要素の集合を，全てのT_kの葉に対して集めた集合族は明らかに，$\lfloor L_1\times\cdots\times L_k\rfloor$の要素を全て含む．また，各節点からの出次数が$r$以下であるから，上で得られた族に属する集合でかつサイズl以下であるものの個数はr^lを超えない．よって，$\mathrm{BL}_r\subseteq\mathrm{ST}_{r,l}$

($\mathrm{BL}_r=\mathrm{CL}_r$)　　$\mathrm{BL}_r\subseteq\mathrm{CL}_r$を満たすことは，$\mathrm{BL}_{r,l}\subseteq\mathrm{CL}_{r,l}$の証明と同様にして示すことができるので，省略する．以下で，$\mathrm{BL}_r\supseteq\mathrm{CL}_r$を証明する．集合族$\mathcal{V}$を上向きに閉じているものとする．$\mathcal{V}$の各要素は$I(D_{\mathcal{V}})$と一対一に対応する．また，$\lfloor\mathcal{V}\rfloor$の各要素は$PI(D_{\mathcal{V}})$と一対一に対応する．ここで，$PC(D_{\mathcal{V}})$に含まれる各節に対応する集合を$M_1,\ldots,M_k$とおくと，集合族$\lceil M_1\times\cdots\times M_k\rceil$も，$I(D_{\mathcal{V}})$と一対一に対応するので，$\mathcal{V}=\lceil M_1\times\cdots\times M_k\rceil$を満たす．もし，$\mathcal{V}$が$\mathrm{BL}_r$に属さないとするならば，上で述べたことより，$PC(D_{\mathcal{V}})$に変数が$r+1$個以上含まれる節$M$が属する．$M=\{i_1,\ldots,i_s\}$ $(s\geq r+1)$とおく．主項，主節の性質より，(C1)$\forall L\in\lfloor\mathcal{V}\rfloor$ $L\cap M\neq\emptyset$が成り立つ．更に，(C2)$\forall j\in\{1,\ldots,s\}\exists L\in\lfloor\mathcal{V}\rfloor$ $L\cap M=\{i_j\}$が成り立つ．なぜならば，$i_j\in L\cap M$なる任意の$L\in\lfloor\mathcal{V}\rfloor$に対して，ある$k\neq j$が存在して$i_k\in L\cap M$が成り立つならば，$M-\{i_j\}$に対応する全ての変数に対する値0の割り当ては$D_{\mathcal{V}}$を0に決定する．これは，$M$が$PC(D_{\mathcal{V}})$に属するとしたことに矛盾する．

したがって，$L=\{1,\ldots,n\}-M$，$L_j=L\cup\{i_j\}$ $(j=1,\ldots,s)$とおくと，(C2)より$L_j\in\mathcal{V}$，また，(C1)より$L\notin\mathcal{V}$．$s\geq r+1$であるから，$\mathcal{V}$は閉じていない．つまり，$\mathcal{V}\notin\mathrm{CL}_r$．証明終り．　□

5　近似法と近似演算

本章では，従来の単調複雑さの証明を解析し，その証明が全て，近似法によるものであるか，またはその証明の本質的な部分を損なわずに近似法の枠組に沿った証明に再構成できることを述べる．更に，個々の証明を近似法の枠組に沿って再構成したときに，その中で定義される近似演算について比較し，これらが全て，前章で定義した$\mathrm{CL}_{r,l}$またはBL_rといった集合族の性質に基づいているものであることを明らかにする．このことは，幾つかの従来の単調複雑さの証明が，実際には本質的には類似の議論によるものであることを示している．以下，個々の証明ごとに議論する．原稿の長さの制約上，細部については大幅に省略せざるを得なかった．したがって，個々の証明のより精細については各々の原典を参照されたい．

定義 6　　**多項式関数** $\mathrm{POLY}(q,s)$ とは，$x=\{x_{i,j}\mid 1\leq i,j\leq q\}$ 上の $n=q^2$変数論理関数である．但し，qは素数であるとする．$V=\{v_1,\ldots,v_q\}$，$W=\{w_1,\ldots,w_q\}$ を頂点とする二分グラフを考え，$x_{i,j}$が(v_i,w_j) の辺の有無を表すものとすると x は二分グラフを一つ指定する．x に対応するグラフを $G(x)$ と表す．$\mathrm{POLY}(q,s)$ は，$s-1$ 次以下の体 Z_q上の多項式 p が存在して，$G(x)$ が全ての $1\leq i\leq q$に対する $(v_i,w_{p(i)})$ を含むとき，かつそのときに限り，値1をとるものとする．

m **頂点** s **クリーク関数** $\mathrm{CLIQUE}(m,s)$ とは，$x=\{x_{i,j}\mid 1\leq i<j\leq m\}$ 上の $m(m-1)/2$ 変数論理関数である．変数 $x_{i,j}$が頂点 (i,j) 間の辺の有無を表すものとすると，x は m 頂点無向グラフを一つ指定する．$\mathrm{CLIQUE}(m,s)$ は入力に対応するグラフが s 完全グラフを含むときかつ，そのときに限り1を出力する関数である．　□

```
1    入力：𝒱
2    𝒱_0 := 𝒱 ; i := 0;
3    while (𝒱_iが (r − 1, l)-閉包でない) do
4        W_{i+1} := {W ⊈ 𝒱_i | 𝒱_i ⊢_{(r,l)} W} の任意の極小要素;
5        𝒱_{i+1} := 𝒱_i ∪ {W | W_{i+1} ⊆ W かつ |W| ≤ l};
6        i := i + 1;
7    end while.
8    出力：𝒱_i
```

図 1: 手続き CLOSURE

5.1 Razborov, Alon, Boppana による証明—$\mathbf{CL}_{r,l}$

Razborov は文献 [6] で，クリーク関数の単調複雑さに対する超多項式下界を得た．その後 Alon と Boppana[1] がこの結果を改良し，クリーク関数と多項式関数の単調複雑さに対する指数関数の下界を導いた．本節では，Alon と Boppana のクリーク関数に対する下界の証明が閉包の性質に基づいたものであることについて述べる．

Alon らの証明は 3 章で述べた近似法に沿ったもので，彼らはその証明中で近似演算を以下の通りに定義した．

l と r を適当な正整数とする．対象とするグラフの頂点数を m とする．近似回路の各結線には $\{1,\ldots,m\}$ の部分集合を要素とする集合族が割り当てられるものとし，近似演算は 2 つの集合族から 1 つの集合族への写像として与えられる．$\{1,\ldots,m\}$ の部分集合 W が項 $T_W = \wedge_{i,j\in W} x_{i,j}$ を表すものとし，集合族 $\mathcal{V}$ は DNF 式 $\vee_{W\in\mathcal{V}} T_W$ を表すものとする．また，入力結線 $x_{1,2},\ldots,x_{m-1,m}$ にはそれぞれ，$\lceil\{1,2\}\rceil,\ldots,\lceil\{m-1,m\}\rceil$ を割り当てる．

近似演算 $\overline{\wedge}$ と $\overline{\vee}$ を図 1に示した手続き CLOSURE に基づいて以下の様に定義する．

$\overline{\wedge}$: 入力を $\mathcal{V}_1,\mathcal{V}_2$ とする．このとき，$\lceil\mathcal{V}_1\cap\mathcal{V}_2\cap\mathcal{V}(l)\rceil$ を出力する．

$\overline{\vee}$: 入力を $\mathcal{V}_1,\mathcal{V}_2$ とする．$(\mathcal{V}_1\cup\mathcal{V}_2)\cap\mathcal{V}(l)$ を手続き CLOSURE に入力として与えたときに出力として得られた集合族を $\mathcal{V}$ とし，$\lceil\mathcal{V}\rceil$ を出力する．

以上の定義に従い，Alon らは f を CLIQUE(m,s) とし，U を $s-1$ 彩色可能なグラフ全体の集合，V を s-完全グラフを只一つ含み，その他には辺を含まないグラフ全体の集合としたとき，$\overline{p}(f,\mathcal{M},U,V)$ が指数関数的となることを示し，前述した結果を得た．次の簡単な命題は，彼らの証明の最も重要な点である近似演算が閉包の性質に基づいて定義されたことを示している．

命題 7　上で定義した近似演算に基づく近似回路について次の 3 つが成り立つ．

(i) 入力結線に割り当てられる集合族は $\mathrm{CL}_{r,l}$ に属する．

(ii) $\mathcal{V}_1,\mathcal{V}_2\in\mathrm{CL}_{r,l}$ ならば $\mathcal{V}_1\,\overline{\wedge}\,\mathcal{V}_2\in\mathrm{CL}_{r,l}$.

(iii) $\mathcal{V}_1,\mathcal{V}_2\in\mathrm{CL}_{r,l}$ ならば $\mathcal{V}_1\,\overline{\vee}\,\mathcal{V}_2\in\mathrm{CL}_{r,l}$.

証明　(i) と (ii) は定義より，(iii) は命題 2の (ii) よりそれぞれ明らかである．□

5.2 天野，丸岡による証明—$\mathbf{BL}_r$

我々 [2] は最近，Haken[5] が開発した隘路数え挙げ (Bottleneck Counting) と呼ばれる手法を近似法の枠組の中に取り入れ，Alon らの用いた近似演算よりも単純な近似演算を導入し，これに基づいてクリーク関数と多項式関数の単調複雑さに対する指数関数の下界を導出した．

我々がその証明で用いた近似演算は以下の通りである．まず，多項式関数に対する下界の証明の際に用いた定義を述べる．本節では，単調論理回路は∧ゲートと∨ゲートが交互に現われているものとする．正整数 l と r を適当な値に定める．DNF 式の項，或いは CNF 式の節に対して，そのサイズを，項，或いは節に含まれる変数の個数と定義する．

$\overline{\wedge}$: 入力を f_1,f_2 とする．$f_1\wedge f_2$ を単調 DNF 式で表し，サイズ l を超える項を全て取り除いて得られる単調 DNF 式を出力とする．

$\overline{\vee}$: 入力を f_1,f_2 とする．$f_1\vee f_2$ を単調 CNF 式で表し，サイズ r を超える節を全て取り除いて得られる単調 CNF 式を出力とする．

我々の証明の最も重要な点は，∧ゲートと∨ゲートが交互に現われるとした仮定より，$\overline{\wedge}$ゲートの入力は全てサイズr以下の節のみからなるCNF式で表され，関数f_1, f_2がこの制約を満たしているならば，$(f_1 \overline{\wedge} f_2)$と$(f_1 \wedge f_2)$の間の誤差が小さいこと，同様に，$\overline{\vee}$ゲートの入力は全てサイズ$l$以下の項のみからなるDNF式で表され，関数$f_1, f_2$がこの制約を満たしているならば，$(f_1 \overline{\vee} f_2)$と$(f_1 \vee f_2)$の間の誤差が小さいことを示すことができる点である．

以下で，我々の近似演算の定義が矩形の性質に基づくものであることを述べる．まず，簡単の為に上の定義から近似演算$\overline{\wedge}$の定義のみ次の様に若干変更する．

> $\overline{\wedge}$: 入力をf_1, f_2とする．$f_1 \wedge f_2$を単調DNF式で表し，サイズlを超える項を全て取り除いて得られる単調DNF式をfとする．更に，fを単調CNF式で表し，サイズrを超える節を全て取り除いて得られる単調CNF式を出力とする．

この様に変更しても，我々の証明で用いた数え挙げの議論はそのまま適用できる．また，ここで示した近似演算$\overline{\wedge}$と$\overline{\vee}$を素子とする近似回路で計算可能な論理関数はサイズr以下の節のみからなるCNF式で表される関数に限定され，$\{1, \ldots, n\}$の部分集合を要素とする集合族$\mathcal{V}$とDNF式$\wedge_{W \in \mathcal{V}} \vee_{i \in W} x_i$を対応させると，この関数群は$\mathrm{BL}_r$に対応する．また，クリーク関数に対する証明についても同様の議論が成り立つ．ここで，我々の下界と，Alonらの下界を比較すると，多項式関数については一致した値であり，クリーク関数CLIQUE(m, s)についても，それぞれの下界として最大の値が得られるsについて見ると，我々の下界が$s = \lceil m^{2/3} \rceil$のときの$\exp(\Omega(m^{1/3}))$であるのに対し，Alonらの下界は$s = (1/4)(m/\log m)^{2/3}$のときの$\exp(\Omega((m/\log m)^{1/3}))$と近い値となっている．この事実は，我々の用いた矩形の概念とAlonらの用いた閉包の概念が互いに類似した性質を持つことを示した定理5の結果と合致し，したがってこれを凌ぐ下界を示す為には本質的に異なる議論が必要であることを示唆するものとして興味深い．

5.3 Andreevによる証明—$\mathrm{CL}_{r,l}$

Andreev[3]はRazborov[7]と同時期に独立に多項式関数POLY(q, s)の単調複雑さが$s = ((1/2)n^{1/8})/(\sqrt{\ln n} - 1)$に対して$\exp(\Omega(n^{1/8}/\sqrt{\ln n}))$であることを証明した．紙面の都合で省略するが，この証明も5.1節に挙げたAlonらによる証明と類似した議論に基づいていることを示すことができる．また，同様の考察が文献[4]の3.5.3節でも行なわれている．

5.4 Hakenによる証明—BL_r

Haken[5]は最近，穴空き網戸(Broken Mosquito Screen)問題と呼ばれるクリーク関数に類似した関数を定義し，この関数の単調複雑さが指数関数となることを，隘路数え挙げと呼ばれる手法を用いて証明した．

本節では，単調論理回路は入次数無制限の∧ゲートと入次数無制限の∨ゲートが交互に現われるとする．サイズmの穴空き網戸関数とは，$m^2 - 2$頂点無向グラフの辺の有無を自然な形で表した，$(m^2 - 2)(m^2 - 1)/2$個の入力変数をとる関数である．グラフの頂点を各々頂点数mのブロック$m - 1$個と，頂点数$m - 2$のブロック1個に分割したときに，同じブロック内の頂点間には全て辺が存在するような分割が存在するときそのグラフを**良い**グラフと呼ぶ．逆に，グラフの頂点を各々頂点数mのブロック$m - 1$個と，頂点数$m - 2$のブロック1個に分割したときに，同じブロック内の頂点間には全て辺が存在しないような分割が存在するときそのグラフを**悪い**グラフと呼ぶ．良いグラフであり，かつ悪いグラフでもあるグラフは存在しない．穴空き網戸問題を解くとは，全ての良いグラフに対して1を出力し，全ての悪いグラフに対して0を出力することをいう．穴空き網戸問題は単調論理回路で解くことができることに注意されたい．

この穴空き網戸問題の単調複雑さに関してHakenの示した定理は次の通りである．

定理 8 [5] $m > 4$とする．このとき，サイズmの穴空き網戸問題を解く単調論理回路のサイズは少なくとも$1.8^{\lfloor \sqrt{m}/2 \rfloor}$． □

この定理をHakenは隘路数え挙げと呼ばれる独自の手法を用いて示した．本節では，この証明の本質的な部分には手を加えずに，これを矩形の性質を用いた近似演算に基づく近似法による証明に再構成できることを述べる．

$k = m/2$とする．近似演算$\overline{\wedge}$と$\overline{\vee}$を次のように定義する．但し，ここでは近似演算$\overline{\wedge}$と$\overline{\vee}$の入力の個数は無制限であるとする．

$\overline{\wedge}$: 入力を $f_1,\ldots,f_j$ とする．$f_1\wedge\cdots\wedge f_j$ を単調 DNF 式で表し，k個以上の変数を含む項を全て取り除いて得られる単調 DNF 式を出力する．

$\overline{\vee}$: 入力を $f_1,\ldots,f_j$ とする．$f_1\vee\cdots\vee f_j$ を単調 CNF 式で表し，k個以上の変数を含む節を全て取り除いて得られる単調 CNF 式を出力とする．

この定義に基づいても，Haken の用いた数え挙げの議論がそのまま適用できて，以下の補題が成立することを示すことができる．

補題 9 [5]　$\overline{\wedge}$ と $\overline{\vee}$ を素子とする任意の回路に対して，0 を出力する良いグラフの個数と 1 を出力する悪いグラフの個数の和は少なくとも

$$\frac{(m^2-2)!}{(m!)^{(m-1)}(m-2)!(m-1)!}.$$

□

補題 10 [5]　$f_1,\ldots,f_j$ を k個未満の変数を含む節のみからなる単調 CNF 式としたとき，$(\wedge_{i=1}^{j}f_i)(v)=1$ かつ $(\overline{\wedge}_{i=1}^{j}f_i)(v)=0$ となる良いグラフ vの個数と，$f_1,\ldots,f_j$ を k個未満の変数を含む項のみからなる単調 DNF 式としたとき，$(\wedge_{i=1}^{j}f_i)(v)=0$ かつ $(\overline{\wedge}_{i=1}^{j}f_i)(v)=1$ となる悪いグラフ vの個数は，ともに高々

$$\frac{(km)^{r/2}(m^2-m)^{r/2}(m^2-2-r)!}{(m!)^{(m-1)}(m-2)!(m-1)!},$$

但し，rは$\sqrt{m}$を超えない最大の偶数とする．

□

定理 8は補題 9と補題 10から簡単な計算によって導かれる．

また，ここで用いた近似演算の定義は 5.2 節で示した天野と丸岡による証明で用いたものに，その入次数が無制限であることを除けば類似したものであり，したがって 5.2 節で行なったのと同様の議論によって，この近似演算が性質 BL_r に基づくものであることが示される．

6　従来型近似法の限界

本章では，従来型近似法による証明の限界を示す例として，s を定数としたときの CLIQUE(m,s) の単調複雑さに対する既知の最良の下界が，既にこの型の手法で到達し得る最良の下界となっていることを示す．f を n 変数単調論理関数とする．$\overline{\wedge}$，$\overline{\vee}:\mathcal{B}_n\times\mathcal{B}_n\to\mathcal{B}_n$ を近似演算とし，$\overline{\wedge}$ と $\overline{\vee}$ ゲートより定まる近似モデルを $\mathcal{M}$ とする．$U\subseteq f^{-1}(0)$，$V\subseteq f^{-1}(1)$ とする．$cover(\mathcal{M},U)$ を以下を満たす最小の s と定義する:

$$\overline{g}_1,\ldots,\overline{g}_s,\overline{h}_1,\ldots,\overline{h}_s\in\mathcal{M}\ \star_1,\ldots,\star_s\in\{\wedge,\vee\}\qquad\bigcup_{i=1}^{s}[(\overline{g}_i\star_i\overline{h}_i)-(\overline{g}_i\,\overline{\star_i}\,\overline{h}_i)]_U=U.$$

$cover(\mathcal{M},V)$ を以下を満たす最小の s と定義する:

$$\overline{g}_1\ldots,\overline{g}_s,\overline{h}_1,\ldots,\overline{h}_s\in\mathcal{M}\ \star_1,\ldots,\star_s\in\{\wedge,\vee\}\qquad\bigcup_{i=1}^{s}[(\overline{g}_i\,\overline{\star}_i\,\overline{h}_i)-(\overline{g}_i\star_i\overline{h}_i)]_V=V.$$

$cover(\mathcal{M},U)$ と $cover(\mathcal{M},V)$ は，与えられた近似演算による誤差で，それぞれ領域 U と V を“**覆う**”のに必要な誤差の個数を表している．$\mathcal{M}$ には定数関数 0 と 1 が含まれるから，$\overline{p}$の定義式中$\overline{f}$を定数関数 0 とすると (2) 式は恒真となり，また，$\overline{f}$を定数関数 1 とすると (1) 式が恒真となる．したがって，次の事実が成り立つ．

事実 11　fを n 変数論理関数とする．

$$\overline{p}(f,\mathcal{M},U,V)\le\min(cover(\mathcal{M},U),cover(\mathcal{M},V)).$$

□

本章では以下で，従来型近似法の限界を示す一つの例として，ある制限を設けた近似法では，s を定数としたとき CLIQUE(m,s) の単調複雑さの $w((m/\log m)^s)$ なる下界を証明し得ないことを示す．定数 s に対する CLIQUE(m,s) の単調複雑さの既知の最良の下界は Alon ら [1] による$\Omega((m/\log m)^s)$ である．彼らは Uを $s-1$ 彩色可能なグラフ全体の集合，Vを s 完全グラフを只一つ含み，その他には全く辺を含まないグラフの集合とし，$r=4se^s\log m$，$l=s-1$ とおいて 5.1 節で述べた通りに近似演算を定義し，このときの $\overline{p}(f,\mathcal{M},U,V)$ の下界として$\Omega((m/\log m)^s)$ を導いた．以下では，この証明に (i)Uを任意の (s より大きくても良い) 定数 kに対して k彩色可能で，かつ s 完全グラフを含まないグラフ全体の集合とする．(ii)rの値を任意とする．(iii) $\overline{\wedge}$ と $\overline{\vee}$ の定義に自由度を持たせる．という幾つかの拡張を行なったとしても，実際に領域 U または Vが $O((m/\log m)^s)$ 個の誤差で覆われることを示す定理 12を証明する．この定理は，従来の手法では既知の最良の下界を凌ぐ下界を導出し得ないことを示している．

s 完全グラフを只一つ含みそれ以外には全く辺を含まないグラフを**良い**グラフと呼ぶ．対象とするグラフの頂点数を m とし，$V_G=\{1,\ldots,m\}$ とおく．近似演算 $\overline{\wedge}$ と $\overline{\vee}$ は $2^{V_G}\times 2^{V_G}$から 2^{V_G}への関数として定義され，

各々の集合族 $\mathcal{V}_G$は DNF 式$\vee_{W\in\mathcal{V}_G}\wedge_{i,j\in W}x_{i,j}$と同一視するものとする．$l=s-1$とし，$r\leq m$を任意の正整数とする．$V_G$の要素数 l以下の部分集合全体からなる集合族を$\mathcal{V}_G(l)$と表す．近似演算$\overline{\wedge}$と$\overline{\vee}$は，次の3つを満たしているものとする．

(i) 任意の$\mathcal{V}_1,\mathcal{V}_2\in \mathrm{BL}_{r,l}$に対して，$\mathcal{V}_1\,\overline{\wedge}\,\mathcal{V}_2$が定義され，$(\mathcal{V}_1\,\overline{\wedge}\,\mathcal{V}_2)\leq(\mathcal{V}_1\wedge\mathcal{V}_2)$ かつ $\mathcal{V}_1\,\overline{\wedge}\,\mathcal{V}_2\in\mathcal{V}_G(l)$を満たす．

(ii) 任意の$\mathcal{V}_1,\mathcal{V}_2\in \mathrm{BL}_{r,l}$に対して，$\mathcal{V}_1\,\overline{\vee}\,\mathcal{V}_2$が定義され，$(\mathcal{V}_1\,\overline{\vee}\,\mathcal{V}_2)\geq(\mathcal{V}_1\vee\mathcal{V}_2)$ かつ $\mathcal{V}_1\,\overline{\vee}\,\mathcal{V}_2\in \mathrm{ST}_{r,l}$を満たす．

(iii) $\overline{\wedge}$と$\overline{\vee}$より定まる近似モデル $\mathcal{M}$ は $\mathcal{M}\supseteq \mathrm{BL}_{r,l}$を満たす．

定理 12　$s\geq 3$，kを任意の定数とする．Vを良いグラフ全体の集合，Uを k彩色可能なグラフでかつ s クリークを含まないグラフ全体の集合とする．$\overline{\wedge}$と$\overline{\vee}$を上の条件を満たす任意の近似演算とし，$\mathcal{M}$ を$\overline{\wedge}$と$\overline{\vee}$より定まる近似モデルとする．このとき，

$$\overline{p}(\mathrm{CLIQUE}(m,s),\mathcal{M},U,V)=O((m/\log m)^s).$$

補題 13　ある定数 c が存在して，$cover(\mathcal{M},U)\leq c^r$．

証明 (概略)　$v_1,\ldots,v_{r+1},u_1,\ldots,u_{r+1}$を互いに異なる頂点とする．$\mathcal{V}_1=\{v_1,\ldots,v_r\}\times\{u_1,\ldots,u_r\}$，$\mathcal{V}_2=\{v_{r+1},u_{r+1}\}$ とおく．条件より $\mathcal{V}_1\,\overline{\vee}\,\mathcal{V}_2$に対応する関数は恒等的に 1 をとることが確かめられる．したがって，$v_1,\ldots,v_{r+1},u_1,\ldots,u_{r+1}$の $2r+2$ 個の頂点が全て同色で塗られるグラフは全てこの$\overline{\vee}$ゲートの誤差に含まれる．ここで，グラフ G を k色に彩色したとする．G から任意に選んだ頂点 $w_1,\ldots,w_{k(2r+2)}$には必ず，$(2r+2)$ 個以上の同色の頂点が存在する．したがって，$w_1,\ldots,w_{k(2r+2)}$から $(2r+2)$ 個の頂点を選ぶ全ての組み合わせについて，選ばれた頂点を $v_1,\ldots,v_{r+1},u_1,\ldots,u_{r+1}$とおき，$\mathcal{V}_1$と $\mathcal{V}_2$を上で定義したようにおくと，全ての k彩色可能なグラフはある誤差に覆われる．このときの誤差の個数は，$\binom{k(2r+2)}{2r+2}\leq 2^{(2r+2)kH(1/k)}$であり，$k$は定数としたことより，この値は c を十分大きな定数とすると c^r で上から抑えられる．ここで，$0<p<1$ に対して $H(p)$ はエントロピー関数 $H(p)=-p\log p-(1-p)\log(1-p)$ とする．□

補題 14　$r\leq\sqrt{m}$ならば，$cover(\mathcal{M},V)=O((m/r)^s)$，$r\geq\sqrt{m}$ならば，$cover(\mathcal{M},V)=O(m^{s-1/2})$．

証明 (概略)　$b=\min(r,\sqrt{m})$ とおく．m 個の頂点をそれぞれサイズ b の m/b 個のブロックに分割する．ここで，任意の s 個のブロックを選び，$C_1,\ldots,C_s$とおく．$\mathcal{V}_1=C_1\times\cdots\times C_{s-1}$，$\mathcal{V}_2=C_2\times\cdots\times C_s$とする．条件より $\mathcal{V}_1\wedge\mathcal{V}_2=C_1\times\cdots\times C_s$，かつ $\mathcal{V}_1\,\overline{\wedge}\,\mathcal{V}_2=\emptyset$ となることが確かめられる．したがって，$C_1,\ldots,C_s$に一つずつ頂点の入った s 個の頂点に対応する良いグラフは，この$\overline{\wedge}$ゲートの誤差に含まれる．以上の誤差を m/b 個のブロックから s 個選択する全ての組合せに対して考えると，s 個の頂点が全て異なるブロックに入ったクリークに対応する良いグラフは，全てある誤差で覆われる．また，このようなグラフは全て 2 つ以上の異なる誤差には含まれることはない．したがって，$\binom{m/b}{s}$個の誤差で$\binom{m/b}{s}r^s$個の良いグラフが覆われる．ここで覆われなかった良いグラフの個数は，$\binom{m}{s}-\binom{m/r}{s}r^s$で，これは s が定数であることを考慮に入れると $O(m^{s-1/2})$ となることがわかる．任意の一つの良いグラフを覆う誤差を持つ$\overline{\wedge}$ゲートは容易に求められるので，したがって，$\binom{m/b}{s}+O(m^{s-1/2})$ 個の誤差で全ての良いグラフを覆うことができる．$b=\min(r,\sqrt{m})$ と s が定数であることに注意すると補題が導かれる．□

証明 (定理 12)　cを十分小さな定数とする．$r\leq c\log m$ならば補題 13より $cover(\mathcal{M},U)=O((m/\log m)^s)$．$r>c\log m$ ならば補題 14より $cover(\mathcal{M},V)=O((m/\log m)^s)$．これと事実 11より定理は導かれる．□

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] K. Amano and A. Maruoka, "Potential of the Approximation Method", *Proc. of 37th FOCS*, 1996.

[3] A. E. Andreev, "On a Method for Obtaining Lower Bounds for the Complexity of Individual Monotone Functions", *Dokl. Akad. Nauk SSSR* Vol. 282(5), pp. 1033–1037, 1985.(in Russian); English Translation in *Soviet Math. Dokl*, Vol. 31(3), pp. 530–534, 1985.

[4] P. E. Dunne, *The Complexity of Boolean Networks*, Academic Press, New York, 1988.

[5] A. Haken, "Counting Bottlenecks to Show Monotone P $\neq$ NP", *Proc. of 36th FOCS*, pp. 36-40, 1995.

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

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

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