数理解析研究所講究録
1041 巻 1998 年 71-78

否定素子数限定論理回路における単調論理関数の複雑さ

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　使用できるNOTゲートの個数を制限した論理回路における，論理関数の複雑さについて論じる．まず，NOTゲートの個数を制限した回路で単調論理関数を計算するのに必要なゲート数の下界導出が，ある条件を満たす関数を**単調**論理回路で計算するのに必要なゲート数の下界導出に帰着できることを表す一般的な規準を証明する (定理 2)．次に，この規準と近似法 ([Raz85]) による議論とを組み合わせて，m 頂点クリーク関数は，NOTゲートの使用を $(1/6)\log\log m$ 個以下に制限した場合には，多項式サイズの論理回路で計算できないことを示す (定理 4，系 5)．

1　はじめに

1.1　背景

ある特定の論理関数 $f:\{0,1\}^n \to \{0,1\}$ について，fを計算するAND，ORとNOTゲートからなる論理回路のゲート数に対する非線形下界を示すことは，理論計算機科学における重要な未解決問題の一つである．ところが，出力の個数を n 個に増やし，更に論理回路の深さを $O(\log n)$ に限定したとしても，依然非線形下界は知られていない．一方，使用可能な素子をANDゲートとORゲートに限定した回路 (これを**単調論理回路**とよぶ) に対しては，近年幾つもの興味深い結果が得られている．1985年，Razborov[Raz85] はクリーク関数を計算する単調論理回路のサイズに関する超多項式の下界を示した．その後 Alon と Boppana[AB87] はこの証明を改良し，この下界を指数関数へと押し上げた．また，特に最近，これらの結果の一般化やより簡単な証明法に関する研究が盛んに発表されている (例えば，[Hak95, AM96, BU97, Juk97, ST97])．更に先日，Raz と McKenzie[RM97] によって，単調-NC $\neq$ 単調-P であることも証明された．また，NOTゲートの使用を許した場合とそうでない場合の回路のサイズに指数関数的な差のある関数が知られる [Tar87] 一方，ほとんど差の生じない関数が存在することも知られている (例えば，[Val86, BNT95])．

そこで，論理回路におけるNOTゲートの働きについてより深く理解することが，一般の論理回路における非線形下界導出への糸口となることは十分に期待される．このような立場から，単調論理回路に限定された個数のNOTゲートを加えた回路に関する研究が行われている．Markov[Mar58] は全ての n 変数論理関数は高々 $\lceil\log(n+1)\rceil$ 個のNOTゲートを用いた論理回路で計算可能であることを示した．Beals, 西野と田中 [BNT95] はNOTゲートを任意個用いた論理回路を，同じ関数を計算し，かつ，NOTゲートの個数は $\lceil\log(n+1)\rceil$ 個で，かつ，全体のゲート数は元の回路のゲート数の高々2倍足す $O(n\log n)$ であるような論理回路に変換する手法を与えた．Santha と Wilson[SW93] は深さを定数に限定した回路を対象にして，NOTゲートの個数を限定した場合とそうでない場合の，関数の計算に要するゲート数の関係について調べた．Raz と Wigderson[RW89] は，全てのNOTゲートは入力変数に直接接続しているとした場合には，st-連結性関数を多項式サイズかつ段数 $O(\log n)$ の回路で計算するためには，入力変数の個数の定数以上の割合のNOTゲートが必要であることを示した．以上のように，幾つかの興味深い結果は得られてきているものの，論理回路におけるNOTゲートの役割については依然未知の部分が多い．例えば，単調論理回路に対して示された指数関数下界と同様の命題が，定数個のNOTゲートの使用を許した場合にも成立するかどうかという問題でさえ未解決であるとされていた [SW93]．

本稿では，この未解決問題を解決すべく，まず，NOTゲートの個数を限定した回路で単調論理関数を計算するのに必要なゲート数の下界を示す問題が，ある条件を満たす関数を**単調**論理回路で計算するのに必要なゲート数の下界を示す問題に帰着できることを示した一般的な規準を証明する．次に，この規準を用いて，次の主定理を証明する:

m 頂点無向グラフにサイズ $(\log m)^{3(\log m)^{1/2}}$ の完全グラフが含まれるか否かを判定するクリーク関数は，NOTゲートの使用を $\lfloor(1/6)\log\log m\rfloor$ 個に限定すると，多項式サイズの論理回路では計算できない．

1.2 証明法

本稿では，文献 [BT96, SW93] などで用いられた論理関数の感度 (sensitivity) をより一般化した特性グラフという概念を導入し，これを用いた議論と，Razborov による近似法 [Raz85] を用いた議論とを組み合わせて下界を導く．

論理関数 $f:\{0,1\}^n \to \{0,1\}$ の特性グラフとは，頂点集合が $\{0,1\}^n$の有向グラフで，頂点 $w, w' \in \{0,1\}^n$ が，$f(w)=0$ かつ $f(w')=1$ かつ wと w'のハミング距離が 1 であるとき，かつそのときに限り wから w'へ向かう辺を持つグラフである．この定義に基づくと，論理関数 fの感度 $s(f)$ は fの特性グラフの各頂点の入次数と出次数の和の平均値として定義される (例えば，[BT96, SW93])．本稿では，NOT ゲートはこのグラフの辺の向きを逆転する効果はあるが，新たな辺を生み出すことは無いことに着目する．いま，NOT ゲートの使用個数を制限されたなかで fを計算する，最適な論理回路 Cが与えられたとする．このとき，fの特性グラフの全ての辺は，回路 C中の全ての NOT ゲートの出力を適当に定数化して得られる論理回路における，出力線かまたはある NOT ゲートの入力線が計算する関数の特性グラフに含まれることを示すことができる．定数化によって得られる回路は全て単調論理回路で，かつ Cの部分回路であるからそのサイズは Cのサイズよりも小さい．したがって上の事実は，直感的には，ある Cよりサイズの小さな単調論理回路で，かつ fをある程度近似するものが存在することを意味している．したがって，fを近似する単調論理回路のサイズの下界を示すことができれば，fを計算する否定素子数限定論理回路のサイズの下界を得ることができる．

主定理の証明のためには，小さなサイズの単調論理回路ではクリーク関数を近似できないことを示す必要がある．これには，Razborov[Raz85] によって示されたクリーク関数の単調論理回路のサイズに対する証明を改良した，天野と丸岡 [AM96] による証明法を応用する．この証明をより精細に解析し，小さなサイズの単調論理回路では，クリーク関数は近似することすら難しいことを示す．最後に，この 2 つの結果を結び付けて主定理を得る．

1.3 本稿の構成

本稿は，以下 2 章で本稿を通じて用いる用語や記号の定義を述べ，3 章で，否定素子数限定論理回路におけるサイズの下界を示すことを単調論理回路のサイズの下界を示す問題に還元する定理を導く．4 章で，クリーク関数は単調論理回路では近似することすら難しいことを示す定理を証明し，これを 3 章で得た定理に適用し主定理を示す．

2 準備

wを $\{0,1\}^n$の要素とする．$i=1,\ldots,n$ に対して，w_i は wの i ビット目の値を表すものとする．$\{0,1\}^n$の要素 wと w'に対して，$w_i \le w'_i$がすべての $i=1,\ldots,n$ に対して成り立っているとき，$w \le w'$と書く．また，$w \le w'$かつ $w \ne w'$を満たしているとき，$w < w'$と書く．wと w'との間のハミング距離，すなわち $|\{i \in \{1,\ldots,n\} \mid w_i \ne w'_i\}|$ を $\mathrm{Ham}(w,w')$ と表す．ここで，集合 Sに対し，$|S|$ は Sの要素数を表すものとする．

入力端子に変数，または，定数が割り当てられた，2 入力 AND ゲート，2 入力 OR ゲート，NOT ゲートからなる非周期的な回路を**論理回路**という．NOT ゲートが現れない論理回路を，特に，**単調論理回路**という．n 変数論理関数 $f:\{0,1\}^n \to \{0,1\}$ が，任意の $w \le w'$なる $w, w' \in \{0,1\}^n$に対して $f(w) \le f(w')$ を満たしているとき，fを**単調論理関数**という．n 変数単調論理関数全体の集合を $\mathcal{M}$ と表す．任意の単量論理関数は単調論理回路で計算可能であり，かつ，単調論理関数で計算可能な関数は単調論理関数のみである．論理回路 Cに入力 wを与えたときの出力値を $C(w)$ と表す．論理回路 Cに含まれるゲートの個数を Cの**サイズ**といい，$\mathrm{size}(C)$ と表す．論理関数 fに対して，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，$\mathrm{size}(f)$ と表す．また，単調論理関数 fに対して，fを計算する最小のゲート数の単調論理回路のゲート数を fの**単調複雑さ**といい，$\mathrm{size}_{mon}(f)$ と表す．正整数 tと論理関数 fに対して，NOT ゲートを高々 t 個しか含まない論理回路のうち fを計算するもので最小サイズのもののゲート数を fの**否定 t 限定複雑さ**，あるいは単に否定限定複雑さといい，$\mathrm{size}_t(f)$ と表す．ただし，fが否定ゲート数 t 個以下の論理回路では計算不能の場合には，この値は定義されないものとする．

3 否定限定複雑さと単調複雑さとの関係

本章では否定限定複雑さと単調複雑さを関係づける定理 (定理 2) を証明する．まず，論理関数の有向グラフによる表現を導入する．

定義 1　n 変数論理関数 fに対して，fの**特性グラフ** $G(f)=(V,E)$ を次のように定める．

- $G(f)$ は有向グラフである．
- $G(f)$ の頂点集合 Vは $\{0,1\}^n$である．
- $G(f)$ の辺集合 Eは $E=\{(w,w') \mid \mathrm{Ham}(w,w')=1$ かつ $f(w)=0$ かつ $f(w')=1\}$．　□

$G(f)$は，入力を1ビット変化させたときに関数 fのとる値が変化する点に着目したグラフである．互いに等しい頂点集合をもつグラフ $G_1=(V,E_1)$ と $G_2=(V,E_2)$ に対して，G_1と G_2の和グラフ $(G_1\cup G_2)=(V_s,E_s)$ を $V_s=V$かつ $E_s=\{(u,v) \mid (u,v)\in G_1$または $(u,v)\in G_2\}$ と定義する．また，$G_1=(V,E_1)$ と $G_2=(V,E_2)$ に対して，$E_1\supseteq E_2$を満たすとき，G_1は G_2を**含む**といい，$G_1\supseteq G_2$と表す．

このとき次の定理が成り立つ．

定理 2　fを n 変数単調論理関数とする．任意の正整数 t に対して，

$$\mathrm{size}_t(f)\geq \min\left\{\max_{f'\in F'}\{\mathrm{size}_{mon}(f')\} \;\middle|\; F'=\{f_1,\ldots,f_\alpha\}\subseteq \mathcal{M},\ \bigcup_{f'\in F'}G(f')\supseteq G(f)\right\},$$

ここで，$\alpha=2^{t+1}-1$．　□

この定理は，否定限定複雑さの下界を示す問題が，特性グラフに関する条件を満たす一連の関数の単調複雑さの下界を示す問題に帰着されることを示している．以下で定理 2を証明する．証明の鍵となるのは次の簡単な事実である．

事実 3　論理回路 Cが任意個の NOT ゲートを含んでいるとする．Cの入力ベクトル w,w'が $C(w)\neq C(w')$ を満たしているとする．C中の任意の NOT ゲート gに対して，論理回路 C'をゲート gの入力線が回路 C'の出力となるような Cの部分回路とし，$C|_1$と $C|_0$をそれぞれ，C中のゲート gの出力結線を定数 1 と 0 で置き換えて得られる回路とする．このとき，次のうち，少なくとも一方が成り立つ．

(i) $C'(w)\neq C'(w')$,

(ii) $\exists z\in\{0,1\}$　$C|_z(w)\neq C|_z(w')$.

証明　$C(w)\neq C(w')$ とする．$C'(w)\neq C'(w')$ ならば証明すべきことはもうない．$C'(w)=C'(w')=a$ $(a\in\{0,1\})$ とする．$a=1$ ならば，$C|_0(w)=C(w)\neq C(w')=C|_0(w')$，$a=0$ ならば，$C|_1(w)=C(w)\neq C(w')=C|_1(w')$．　□

定理 2の証明は，直感的には，回路の出力に近い NOT ゲートから入力に近い NOT ゲートへと順に事実 3 を適用することで行われる．

証明 (定理 2)　fを n 変数単調論理関数とする．論理回路 Cを，使用できる NOT ゲートの個数を t 個以下に制限したなかでの fに対する最適な回路とする．すなわち，$\mathrm{size}(C)=\mathrm{size}_t(f)$．簡単のため Cには丁度 t 個の NOT ゲートが含まれているものとする．C中に含まれる NOT ゲートを，計算の順序に矛盾しないように並べたものを $g_1,\ldots,g_t$とする．一般に，このような順序づけは複数存在するが，以下では任意の順序づけに固定して考える．Cに wを入力したときの，ゲート gの出力を $g(w)$ と表す．$0\leq i\leq t$ と $u\in\{0,1\}^i$に対して，C_uを，C中の NOT ゲート $g_1,\ldots,g_i$の出力を，それぞれ定数 $u_1,\ldots,u_i$で置き換え，更に，NOT ゲート g_{i+1}の入力を C_u自身の出力として得られる回路とする．ただし，g_{t+1}は C自身の出力ゲートを表すものとし，また，空系列λに対して，C_λは NOT ゲート g_1の入力線を出力とする回路とする．こうして得られた回路 C_u は全て単調論理回路となることに注意されたい．

$(w,w')\in G(f)$ とする．すなわち，$f(w)=0$，$f(w')=1$ かつ $w<w'$．このとき，ある $0\leq i\leq t$ と，ある $u\in\{0,1\}^i$が存在して $C_u(w)=0$ かつ $C_u(w')=1$ を満たす．なぜなら，iを論理回路 Cに wと w'を入力したときに最初に異なる値を出力する NOT ゲートが g_{i+1}であるように定め，更に $0\leq j\leq i$ に対して $u_j=g_j(w)(=g_j(w'))$ と定めると $C_u(w)\neq C_u(w')$ を満たし，これと，C_uの単調性より $C_u(w)=0$ かつ $C_u(w')=1$ が成り立つからである．よって，それぞれの回路 C_u $(u\in\{0,1\}^*,\ |u|\leq t)$ が計算する関数 f_u全ての集合を F' とおくと，明らかに $\cup_{f'\in F'}G(f')\supseteq G(f)$，かつ，任意の $f'\in F'$に対して $\mathrm{size}_t(f)(=\mathrm{size}(C))\geq \mathrm{size}_{mon}(f')$．また，こうして得られる F'の要素数は $\sum_{j=1}^{t}2^j+1+1=2^{t+1}-1=\alpha$である．よって，定理は成り立つ．□

4 下界

m **頂点** s **クリーク関数** CLIQUE(m,s) とは，$X=\{x_{ij} \mid 1 \le i < j \le m\}$ 上の $m(m-1)/2$ 変数単調論理関数である．変数 x_{ij}が頂点 (i,j) 間の辺の有無を表すものとすると，Xに対する割り当ては m 頂点無向グラフを一つ指定する．CLIQUE(m,s) は入力に対応するグラフが s 個の頂点からなる完全グラフ (以後，s クリーク) 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．本章では次の主定理を証明する．

定理 4　十分大きな任意の正整数 m に対して，

$$\mathrm{size}_{\lfloor (1/6)\log\log m \rfloor}(\mathrm{CLIQUE}(m,(\log m)^{3(\log m)^{1/2}})) > 2^{(1/5)(\log m)^{(\log m)^{1/2}}}.$$ □

定理 4中の定数 1/6 は最適ではない (定数部分の最適化は本稿では行わない)．また，上の定理より自然に次の系が導かれる．

系 5　$(\log m)^{3\sqrt{\log m}} \le s \le m/2$ とする．このとき，CLIQUE(m,s) は m の多項式サイズ，かつ NOT ゲートの個数が $\lfloor (1/6)\log\log m \rfloor$ 個未満であるような論理回路では計算できない．

証明 (概略)　kを正整数とする．m 頂点グラフ $G=(V,E)$ に対して $m+k$頂点グラフ $G'=(V',E')$ を $V'=V\cup\{u_1,\ldots,u_k\}$，$E'=E\cup\{(u_i,u_j) \mid 1\le i<j\le k\}\cup\{(v,u_i) \mid v\in V,\ 1\le i\le k\}$ と定めると，明らかに CLIQUE$(m+k,s+k)(G')$ =CLIQUE$(m,s)(G)$ が成り立つ．したがって，任意の正整数 kと t に対して $\mathrm{size}_t(\mathrm{CLIQUE}(m+k,s+k)) \ge \mathrm{size}_t(\mathrm{CLIQUE}(m,s))$ が成り立ち，よってこれと定理 4より系が成り立つ．□

上の結果は NOT ゲートの使用を $\lfloor (1/6)\log\log m \rfloor$ 個以下に限定した論理回路では，クリーク関数を計算するのに，如何なる多項式をも超える個数のゲートが必要であることを示している．Fischer[Fis74] や，後に Beals, 西野と田中 [BNT95] によって，任意の n 変数論理関数に対して，$\mathrm{size}_{\lceil\log(n+1)\rceil}(f) \le 2\mathrm{size}(f)+O(n\log n)$ が示されている．したがって，m 頂点クリーク関数の入力変数の個数は $m(m-1)/2$ であるから，NOT ゲートの個数を $\lceil\log(m(m-1)/2+1)\rceil \le \lceil\log(m^2/2)\rceil \le \lfloor 2\log m \rfloor$ 個にまで増やして，定理 4や系 5と同様の超多項式下界が証明できれば，P≠NP が導かれる．ただし，$F'=\{x_1,\ldots,x_n\}$ とおくと，任意の単調論理関数 fに対して，$\cup_{f'\in F'}G(f') \supseteq G(f)$ が成り立つので，$\alpha \ge n$，すなわち，$t \ge \log(n+1)-1$ の場合には，定理 2を用いた議論によっては非自明な下界は導き得ない．

本章では，まず 4.1 節で，クリーク関数に対する単調複雑さの指数関数下界の証明を改良し，小さなサイズの単調論理回路ではクリーク関数を近似することすらできないことを示す (補題 6)．次に 4.2 節で，この補題と先に証明した定理 2を組み合わせて定理 4を証明する．

4.1 クリーク関数の近似不可能性

s_1と s_2を正整数とする．m 頂点無向グラフ $G=(V,E)$ が s_2クリークをただ一つ含み，その他には全く辺を含まないとき，これを**良いグラフ**と呼び，良いグラフの集合を $I(m,s_2)$ と表す．特に誤解の恐れのない場合，以下では，m 頂点無向グラフそのものと，そのグラフに対応する長さ $m(m-1)/2$ のベクトルを同一視する．グラフの m 個の頂点を，各分割に含まれる頂点の個数が $\lfloor m/(s_1-1)\rfloor$ または $\lceil m/(s_1-1)\rceil$ で，かつ，異なる分割に含まれる 2 頂点間には必ず辺が存在し，同一の分割に含まれる 2 頂点間には全く辺が存在しないような s_1-1 個の集合に分割できるとき，このグラフを**悪いグラフ**と呼び，悪いグラフの集合を $O(m,s_1)$ と表す．悪いグラフは s_1クリークを含まず，また，悪いグラフに任意に一本の辺を加えると s_1クリークを含む．

$F(m,s_1,s_2)$ を，入力として与えられたグラフ G が s_1クリークを含まないならば値 0 を，s_2クリークを含むならば値 1 を，そのどちらでもない場合には任意の値をとりうるとした単調論理関数全体からなる集合とする．$F(m,s,s)$ は CLIQUE(m,s) のみであり，$s_1<s_2$のとき，$F(m,s_1,s_2)$ は複数の関数を含むことに注意されたい．$F(m,s_1,s_2)$ に属する任意の関数 fに対して，fは $I(m,s_2)$ に属する任意のグラフに対して 1 を出力し，$O(m,s_1)$ に属する任意のグラフに対して 0 を出力する．Alon と Boppana[AB87] は $3\le s_1\le s_2$かつ $\sqrt{s_1}s_2 \le m/(8\log m)$ を満たしているならば，$F(m,s_1,s_2)$ に属する如何なる関数も $(1/8)2^{(\sqrt{s_1}+1)/2}$ を超える単調複雑さを持つことを示した．本節では，この結果を更に拡張し，ある一定の条件を満たす s_1と s_2の組みに対しては，$F(m,s_1,s_2)$ に属する如何なる関数も，小さなサイズの単調論理回路では，それを近似することすら難しいことを示す，次の補題を証明する．

補題 6　正整数 s_1と s_2が，$64\le s_1\le s_2$かつ $s_1^{1/3}s_2 \le m/200$ を満たしているとする．Cは単調論理回路で，かつ，$I(m,s_2)$ に含まれるグラフのうち Cが 1 を出力するものの割合が $h=h(s_2)$ 以上であるとする．こ

のとき，次のうち少なくとも一方が成り立つ．

(i) Cのゲートの個数は少なくとも $(h/2)2^{s_1^{1/3}/4}$，

(ii) $O(m,s_1)$ に含まれるグラフのうち Cが 0 を出力するものの割合が $2/s_1^{1/3}$以下． □

補題 6は，天野と丸岡 [AM96] によるクリーク関数の単調複雑さの指数関数下界の証明に沿った議論によって証明する．我々は文献 [AM96] で，Razborov によって開発された近似法を用い，その証明の鍵となる近似ゲートを DNF 式の項や CNF 式の節のサイズといった簡単な概念に基づいて定義し，従来の Alon と Boppana[AB87] による証明を簡単化した．ここでも，この証明と全く同じくように近似ゲート ∇ と $\barwedge$ を定義し，証明を構成する．ただし，証明中で用いられるパラメータ lと rの値は本補題の証明に適するように変更し，それにあわせて各ゲートでの誤差の見積もりも変更する．最後に文献 [AM96] の定理 1 の証明と同じく，これらの誤差に対する見積もりを基に，回路のサイズに対する下界を証明する．ここでは，細部については省略し，文献 [AM96] の定理 1 の証明からの変更点のみ記述する．まず，文献 [AM96] では，単調論理回路に$\wedge$ゲートと$\vee$ゲートが交互に出現するという条件を科しており，厳密にはこれによるサイズの増加も考慮に入れる必要がある (本稿では，後に式 (1) でこの点に対処する)．文献 [AM96] で近似ゲートを定義する際に必要なパラメータ lと rを $l=\lfloor s_1^{1/3}/4\rfloor$，$r=\lfloor 30s_1^{1/3}\rfloor$ と定める．これにしたがって定義された近似ゲートからなる回路を近似回路と呼ぶ．また，$w=m \bmod (s_1-1)$ とおく．紙面の都合で省略するが，[AM96] の定理 1 と全く同様の議論によって，次の事実 7，補題 8，補題 9と補題 10を示すことができる．

事実 7　$I(m,s_2)$ の要素数は $(m!)/(s_2!(m-s_2)!)$, $O(m,s_1)$ の要素数は

$$\frac{m!}{(\lceil m/(s_1-1)\rceil!)^w(\lfloor m/(s_1-1)\rfloor!)^{s_1-1-w}w!(s_1-1-w)!}.$$ □

補題 8　近似回路は恒等的に 0 を出力するか，または，少なくとも $1-s_1^{1/3}$以上の割合の悪いグラフに対して 1 を出力する． □

補題 9　OR ゲートを ∇ ゲートで置き換えたことによって生じる誤差 (すなわち，OR ゲートが 0 を出力し，∇ ゲートが 1 を出力するような悪いグラフの個数) は，高々

$$\frac{(m/s_1^{1/6})^{r+1}(m-r-1)!}{(\lceil m/(s_1-1)\rceil!)^w(\lfloor m/(s_1-1)\rfloor!)^{s_1-1-w}w!(s_1-1-w)!}.$$ □

補題 10　AND ゲートを $\barwedge$ ゲートで置き換えたことによって生じる誤差 (すなわち，AND ゲートが 1 を出力し，$\barwedge$ ゲートが 0 を出力するような良いグラフの個数) は，高々$((2rs_2)^{l+1}(m-l-1)!)/(s_2!(m-s_2)!)$. □

証明の概略 (補題 6)　単調論理回路 Cが $\Pr_{v\in I(m,s_2)}[C(v)=1]\geq h(s_2)$, かつ，$\Pr_{u\in O(m,s_1)}[C(u)=0]>2/s_1^{1/3}$ を満たしているとする．このとき単調論理回路 Cが補題 6 の条件 (i) を満たしていることを示せば十分である．

補題 8より，Cの近似回路$\overline{C}$は $\Pr_{v\in I(m,s_2)}[C(v)\neq\overline{C}(v)]\geq h(s_2)$, または，$\Pr_{u\in O(m,s_1)}[C(u)\neq\overline{C}(u)]>1/s_1^{1/3}$ を満たす．よって，事実 7と補題 8，9，10より，Cのサイズは少なくとも，

$$\frac{1}{2}\min\left(\frac{h(s_2)m!}{(2rs_2)^{l+1}(m-l-1)!}\ ,\ \frac{m!}{s_1^{1/3}(m/s_1^{1/6})^{r+1}(m-r-1)!}\right). \tag{1}$$

ここで，上式の係数 1/2 は，文献 [AM96] では単調論理回路に，AND ゲートと OR ゲートが交互に出現するという条件を科しており，この条件を取り除いたときの回路のサイズの減少分を考慮に入れたものである．上式と簡単な計算により補題は導かれる． □

4.2　主定理の証明

本節では，本稿の主定理である次の定理を証明する．

定理 4　十分大きな任意の正整数 m に対して，

$$\mathrm{size}_{\lfloor(1/6)\log\log m\rfloor}(\mathrm{CLIQUE}(m,(\log m)^{3(\log m)^{1/2}}))>2^{(1/5)(\log m)^{(\log m)^{1/2}}}.$$ □

証明　$t=\lfloor(1/6)\log\log m\rfloor$, $s=(\log m)^{3(\log m)^{1/2}}$, $M=2^{(1/5)(\log m)^{(\log m)^{1/2}}}$ とおく．$\alpha=2^{t+1}-1$ とおく．論理回路 Cが高々t 個の NOT ゲートを含み，CLIQUE(m,s) を計算していると仮定する．このとき，定理 2より，ある $f_1,\ldots,f_\alpha\in\mathcal{M}$ が存在して，$\bigcup_{i\in\{1,\ldots,\alpha\}}G(f_i)\supseteq G(\mathrm{CLIQUE}(m,s))(*1)$ かつ，任意の $i\in$

$\{1,\ldots,\alpha\}$ に対して $\mathrm{size}_{mon}(f_i) \leq \mathrm{size}_t(\mathrm{CLIQUE}(m,s))$. 以下で，ある単調論理関数 $f_1,\ldots,f_\alpha$が条件 (*1) を満たし，かつ，全ての $i \in \{1,\ldots,\alpha\}$ に対して $\mathrm{size}_{mon}(f_i) \leq M$を仮定して矛盾を導く．

いま，クリーク関数の入力の対象となる m 頂点無向グラフを $G=(V,E)$ とおく．$l_0=s$, $l_\alpha=m$ とおき，また，$j=1,\ldots,\alpha-1$ に対して，$l_j = m^{1/10+(1/3)(j-1)/(\log m)^{1/6}}$とおく．すなわち，$l_1,\ldots,l_{\alpha-1}$は公比 $m^{(1/3)/(\log m)^{1/6}}$の等比級数である．$t=\lfloor(1/6)\log\log m\rfloor$ より，$l_{\alpha-1} \leq m^{1/10+(1/3)(2^{(1/6)\log\log m+1})/(\log m)^{1/6}} = m^{1/10+2/3} < m^{9/10}$を満たすこと，よって十分大きな全ての整数 m に対して，$l_0 < l_1 < \cdots < l_\alpha$ を満たすことに注意されたい．$j=0,\ldots,\alpha$に対してグラフの頂点集合 Vのサイズ l_jの部分集合全てからなる集合族を $\mathcal{L}_j$ とおき，$L \subseteq V$に対して，Lの部分集合でかつサイズ l_jであるもの全てからなる集合族を $\mathcal{L}_j(L)$ とおく．すなわち，$\mathcal{L}_j = \{L \subseteq V \mid |L| = l_j\}$, $\mathcal{L}_j(L) = \{L' \subseteq L \mid L' \in \mathcal{L}_j\}$ と定義する．

$i \in 1,\ldots,\alpha$と，$L_i \in \mathcal{L}_i$に対して，グラフ vが**第 i 層の L_iに関する良いグラフ**であるとは，ある $L_{i-1} \in \mathcal{L}_{i-1}(L_i)$(すなわち，$|L_{i-1}| = l_{i-1}$かつ $L_{i-1} \subseteq L_i$) が存在して，vでは L_{i-1}に含まれる全ての二頂点間に辺があり (すなわち，l_{i-1}クリークを形成し)，その他には全く辺がないことをいう．第 i 層の L_iに関する良いグラフ全体を I_{L_i}と表す．$i \in 1,\ldots,\alpha$と，$L_i \in \mathcal{L}_i$に対して，グラフ uが**第 i 層の L_iに関する悪いグラフ**であるとは，ある L_iの分割 $V_1,\ldots,V_{s-1}$が存在して

(i) $|V_i| \in \{\lfloor |L_i|/(s-1)\rfloor, \lceil |L_i|/(s-1)\rceil\}$ $(i=1,\ldots,s-1)$,

(ii) uでは互いに異なるグループに入っている二頂点間には必ず辺が存在し，その他には全く辺は存在しない．

を満たすことをいう．また，第 i 層の L_iに関する悪いグラフ全体を O_{L_i}と表す．第 1 層の良いグラフは $\mathrm{CLIQUE}(m,s)$ の値を 1 にする極小なグラフであり，第α層の悪いグラフは $\mathrm{CLIQUE}(m,s)$ の値を 0 にする極大なグラフである．また，任意の i と $L_i \in \mathcal{L}_i$に対して，第 i 層の L_iに関する良いグラフは 4.1 節で定義した良いグラフ $I(l_i,l_{i-1})$ と一対一対応があり，第 i 層の L_iに関する悪いグラフは 4.1 節で定義した悪いグラフ $O(l_i,s)$ と一対一対応があることに注意されたい．このとき，$s^{1/3}l_{i-1} \leq l_i/200$ に注意すると，補題 6から，小さな複雑さを持つ単調論理関数では O_{L_i}と I_{L_i}を分離することが困難であることを示す次の補題が成り立つ．

補題 11　$i \in \{1,\ldots,\alpha\}$, $L_i \in \mathcal{L}_i$とする．単調論理回路 Cが第 i 層の L_iに関する良いグラフ O_{L_i}に対して h 以上の割合で 1 を出力しているとする．このとき，次のうち少なくとも一方が成り立つ．

(i) Cのゲートの個数は少なくとも $(h/2)2^{s^{1/3}/4}$,

(ii) 第 i 層の L_iに関する悪いグラフ I_{L_i}のうち Cが 0 を出力するものの割合が $2/s^{1/3}$以下．　□

証明つづき (定理 4)　$L \subseteq V$に対して，L に属する二頂点間には必ず辺が存在し，その他には全く辺を含まないグラフを v_Lと表す．$\mathcal{L}_0 = \{L \subseteq V \mid |L| = s\}$ と定義したことに注意すると，明らかに，任意の $L_0 \in \mathcal{L}_0$に対して，ある $u < v_{L_0}$が存在して，辺 (u,v_{L_0}) が $G(\mathrm{CLIQUE}(m,s))$ に属する．したがって，ある $i_1 \in \{1,\ldots,\alpha\}$ が存在して，$\Pr_{L_0\in\mathcal{L}_0}[\exists u < v_{L_0} \quad (u,v_{L_0}) \in G(f_{i_1})] \geq 1/\alpha > 1/2^{t+1}$ を満たす．よって，$\Pr_{L_0\in\mathcal{L}_0}[f_{i_1}(v_{L_0}) = 1] \geq 1/2^{t+1}$. したがって，簡単な議論によって

$$\Pr_{L_1\in\mathcal{L}_1}\left[\Pr_{v\in I_{L_1}}[f_{i_1}(v)=1] \geq \frac{1}{2^{t+2}}\right] \geq \frac{1}{2^{t+2}}. \tag{2}$$

ここで，$\Pr_{v\in I_{L_1}}[f_{i_1}(v)=1] \geq 1/2^{t+2}$ を満たす $L_1 \in \mathcal{L}_1$を**密な** L_1と呼ぶ．ここで，$h=1/2^{t+2}$とおく．簡単な計算により $h \geq 1/m$が示せる．個々の密な L_1に対して補題 11を適用すると，$\mathrm{size}_{mon}(f_{i_1}) \geq (1/2m)2^{s^{1/3}/4} = 2^{(1/4)(\log m)^{(\log m)^{1/2}}-\log m-1} > M$，または　$\Pr_{u\in O_{L_1}}[f_{i_1}(u)=1] \geq 1-2/s^{1/3} \geq 1/2$ が成り立つ．前者は $\mathrm{size}_{mon}(f_{i_1}) \leq M$とした仮定に反するので，任意の密な L_1に対して，$\Pr_{u\in O_{L_1}}[f_{i-1}(u)=1] \geq 1/2$. (2) 式より，

$$\Pr_{L_1\in\mathcal{L}_1}\left[\Pr_{u\in O_{L_1}}[f_{i_1}(u)=1] \geq \frac{1}{2}\right] \geq \frac{1}{2^{t+2}}. \tag{3}$$

証明は，以上と同様の手順を $\mathcal{L}_2,\mathcal{L}_3,\cdots$ へと順次繰り返すことにより行う．

補題 12　$0<c_1<1$, $0<c_2<1$とする．$c_3=\alpha$とおく．単調論理関数 $f_1,\ldots,f_{c_3}$が，$\cup_{i\in\{1,\ldots,c_3\}}G(f_i) \supseteq G(\mathrm{CLIQUE}(m,s))$ を満たし，かつ，どの f_iの単調複雑さも M以下であるとする．さらに，互いに異なる $i_1,\ldots,i_k \in \{1,\ldots,c_3\}$ に対して，

$$\Pr_{L_k\in\mathcal{L}_k}\left[\Pr_{u\in O_{L_k}}[f_{i_1}(u)=\cdots=f_{i_k}(u)=1] \geq \frac{1}{c_1}\right] \geq \frac{1}{c_2}$$

が成り立っているとする．このとき，$c_1c_2c_3 \leq s^{1/3}/8$ ならば，ある $i_{k+1} \in \{1,\ldots,c_3\}/\{i_1,\ldots,i_k\}$ が存在して，

$$\Pr_{L_{k+1}\in\mathcal{L}_{k+1}}\left[\Pr_{u\in O_{L_{k+1}}}[f_{i_1}(u)=\cdots=f_{i_k}(u)=f_{i_{k+1}}(u)=1]\geq\frac{1}{4c_1c_2c_3}\right]\geq\frac{1}{2c_2c_3}.$$

証明　$\Pr_{u\in O_{L_k}}[f_{i_1}(u)=\cdots=f_{i_k}(u)=1]\geq 1/c_1$ を満たす $L_k\in\mathcal{L}_k$ 全体の集合を $\mathcal{L}_k^{bad}$ と表す．補題 12の前提条件より，$\Pr_{L_k\in\mathcal{L}_k}[L_k\in\mathcal{L}_k^{bad}]\geq 1/c_2$(*2)．$f_{i_1}(u)=\cdots=f_{i_k}(u)=1$ を満たす $u\in O_{L_k}$ を任意に選び固定する．このとき，u を始点とする辺は $G(f_{i_1}),\ldots,G(f_{i_k})$ のどれにも含まれない．$\mathrm{CLIQUE}(m,s)(u)=0$ であり，また，u で接続していない L_k 内の 2 頂点を適当に選び，これを結ぶ辺を u に加えて u^+ とすると，$\mathrm{Ham}(u,u^+)=1$，かつ，$\mathrm{CLIQUE}(m,s)(u^+)=1$ を満たすので，$(u,u^+)\in G(\mathrm{CLIQUE}(m,s))$ が成り立つ．また，このとき，$u^+\leq v_{L_k}$．よって，

$$\forall L_k\in\mathcal{L}_k^{bad}\exists u\in O_{L_k}\exists u^+\leq v_{L_k}\quad (u,u^+)\in G(\mathrm{CLIQUE}(m,s))\text{ かつ }(u,u^+)\notin\bigcup_{j\in\{1,\ldots,k\}}G(f_{i_j}).$$

ゆえに，

$$\forall L_k\in\mathcal{L}_k^{bad}\exists u\in O_{L_k}\exists u^+\leq v_{L_k}\quad (u,u^+)\in\bigcup_{j\in\{1,\ldots,c_3\}/\{i_1,\ldots,i_k\}}G(f_j).$$

したがって，ある $l\in\{1,\ldots,c_3\}/\{i_1,\ldots,i_k\}$ が存在して，$\Pr_{L_k\in\mathcal{L}_k^{bad}}[\exists u\in O_{L_k}\exists u^+\leq v_{L_k}\quad (u,u^+)\in G(f_l)]\geq 1/c_3$．$u\in O_{L_k}$ に対して $(u,u^+)\in G(f_l)$ ならば，$f_l(u^+)=1$．$u^+\leq v_{L_k}$ ならば，f_l の単調性より $f_l(v_{L_k})=1$，よって，$\Pr_{L_k\in\mathcal{L}_k}[f_l(v_{L_k})=1\mid L_k\in\mathcal{L}_k^{bad}]\geq 1/c_3$．したがって，上式と (*2) 式より，ある $l\in\{1,\ldots,c_3\}/\{i_1,\ldots,i_k\}$ が存在して，$\Pr_{L_k\in\mathcal{L}_k}[L_k\in\mathcal{L}_k^{bad}\text{ かつ }f_l(v_{L_k})=1]\geq 1/c_2c_3$(*3)．上式を満たす任意の l を一つ選び以後 i_{k+1} とおく．$L_k\in\mathcal{L}_k^{bad}$ かつ $f_{i_{k+1}}(v_{L_k})=1$ を満たす $L_k\in\mathcal{L}_k$ 全体の集合を $\mathcal{L}_k^{target}$ と表すと，$\Pr_{L_k\in\mathcal{L}_k}[L_k\in\mathcal{L}_k^{target}]\geq 1/c_2c_3$．ここで，

$$\sum_{L_{k+1}\in\mathcal{L}_{k+1}}|\{L_k\in\mathcal{L}_k(L_{k+1})\mid L_k\in\mathcal{L}_k^{target}\}|=\sum_{L_k\in\mathcal{L}_k^{target}}|\{L_{k+1}\in\mathcal{L}_{k+1}\mid L_k\subseteq L_{k+1}\}|.$$

上式の右辺の総和記号中の項は，いかなる $L_k\in\mathcal{L}_k$ に対しても同じ値をとるので，これを a とおくと，(*3) 式より，

$$(\text{上式})=a\sum_{L_k\in\mathcal{L}_k^{target}}1\geq a\frac{|\mathcal{L}_k|}{c_2c_3}=\frac{1}{c_2c_3}\sum_{L_{k+1}\in\mathcal{L}_{k+1}}|\mathcal{L}_k(L_{k+1})|.$$

また，$|\mathcal{L}_k(L_{k+1})|$ の値も L_{k+1} の値によらず一定なのでこれを b とおくと，

$$\sum_{L_{k+1}\in\mathcal{L}_{k+1}}|\{L_k\in\mathcal{L}_k(L_{k+1})\mid L_k\in\mathcal{L}_k^{target}\}|\quad\geq\quad\frac{b|\mathcal{L}_{k+1}|}{c_2c_3}\tag{4}$$

したがって，

$$\Pr_{L_{k+1}\in\mathcal{L}_{k+1}}\left[\Pr_{L_k\in\mathcal{L}_k(L_{k+1})}[L_k\in\mathcal{L}_k^{target}]\geq\frac{1}{2c_2c_3}\right]\geq\frac{1}{2c_2c_3}.\tag{5}$$

なぜなら上式が成り立たないと仮定すると，

$$\sum_{L_{k+1}\in\mathcal{L}_{k+1}}|\{L_k\in\mathcal{L}_k(L_{k+1})\mid L_k\in\mathcal{L}_k^{target}\}|<\frac{|\mathcal{L}_{k+1}|}{2c_2c_3}b+|\mathcal{L}_{k+1}|\left(1-\frac{1}{2c_2c_3}\right)\frac{b}{2c_2c_3}<\frac{b|\mathcal{L}_{k+1}|}{c_2c_3}$$

となり，(4) 式に矛盾するからである．ここで，$\Pr_{L_k\in\mathcal{L}_k(L_{k+1})}[L_k\in\mathcal{L}_k^{target}]\geq 1/2c_2c_3$(*4) を満たす $L_{k+1}\in\mathcal{L}_{k+1}$ を**密な** L_{k+1} と呼び，密な L_{k+1} の集合を $\mathcal{L}_{k+1}^{dense}$ と表す．このとき，任意の $L_{k+1}\in\mathcal{L}_{k+1}^{dense}$ に対して，$\Pr_{v\in I_{L_{k+1}}}[f_{i_{k+1}}(v)=1]\geq 1/2c_2c_3$．したがって，$h=1/(2c_2c_3)>1/m$ とおくと，個々の密な L_{k+1} に対して補題 11が適用できて，$\mathrm{size}_{mon}(f_{i_{k+1}})>(1/2m)2^{s^{1/3}/4}>M$，または，$\Pr_{u\in O_{L_{k+1}}}[f_{i_{k+1}}(u)=0]\leq 2/s^{1/3}\leq 1/4c_1c_2c_3$ が成り立つ．(ここで，補題 12の前提条件 $c_1c_2c_3\leq s^{1/3}/8$ を用いた．) 前者は仮定に矛盾するので棄却され，したがって，任意の密な $L_{k+1}\in\mathcal{L}_{k+1}^{dense}$ に対して，$\Pr_{u\in O_{L_{k+1}}}[f_{i_{k+1}}(u)=0]\leq 1/4c_1c_2c_3$(*5)．(*4) 式より

$$\Pr_{L_k\in\mathcal{L}_k(L_{k+1})}\left[\Pr_{u\in O_{L_k}}[f_{i_1}(u)=\cdots=f_{i_k}(u)=1]\geq\frac{1}{c_1}\right]\geq\frac{1}{2c_2c_3},$$

また，このとき，$\Pr_{u\in O_{L_{k+1}}}[f_{i_1}(u)=\cdots=f_{i_k}(u)=1]\geq 1/2c_1c_2c_3$(*6) を示すことは難しくない．よって，(*6) 式と (*5) 式より，任意の密な $L_{k+1}\in\mathcal{L}_{k+1}^{dense}$ に対して，$\Pr_{u\in O_{L_{k+1}}}[f_{i_1}(u)=\cdots=f_{i_k}(u)=f_{i_{k+1}}(u)=1]\geq$

$1/2c_1c_2c_3 - 1/4c_1c_2c_3 = 1/4c_1c_2c_3$. 上式と (5) 式より補題 12は直ちに導かれる. □

証明つづき (定理 4) まず, 任意の $k \in \{1,\ldots,\alpha\}$ に対して, 互いに異なる $i_1,\ldots,i_k \in \{1,\ldots,\alpha\}$ が存在して,

$$\Pr_{L_k \in \mathcal{L}_k}\left[\Pr_{u \in O_{L_k}}[f_{i_1}(u) = \cdots = f_{i_k}(u) = 1] \geq \frac{1}{2^{k^2(t+2)}}\right] \geq \frac{1}{2^{k(t+2)}}. \quad (6)$$

を満たすことを, kに関する帰納法で証明する. $k = 1$ のときは, (3) 式より明らか. $k = l$まで成立しているとして, $k = l+1$ について証明する. 帰納法の仮定より,

$$\Pr_{L_l \in \mathcal{L}_l}\left[\Pr_{u \in O_{L_l}}[f_{i_1}(u) = \cdots = f_{i_l}(u) = 1] \geq \frac{1}{2^{l^2(t+2)}}\right] \geq \frac{1}{2^{l(t+2)}}.$$

$c_1 = 2^{l^2(t+2)}$, $c_2 = 2^{l(t+2)}$, $c_3 = 2^{t+1} - 1$ とおくと, $4c_1c_2c_3 \leq 2^{2+l^2(t+2)+l(t+2)+(t+1)} \leq 2^{(l+1)^2(t+2)}$, $2c_2c_3 \leq 2^{1+l(t+2)+t+1} = 2^{(l+1)(t+2)}$. また, $c_1c_2c_3 \leq 2^{(l+1)^2(t+2)}/4 \leq 2^{(2^{t+1})^2(t+2)}/4 \leq 2^{2^{3t}}/8 \leq 2^{2^{(1/2)\log\log m}}/8 = 2^{\sqrt{\log m}}/8 < (\log m)^{\sqrt{\log m}}/8 = s^{1/3}/8$. よって, 補題 12を適用すると,

$$\Pr_{L_{l+1} \in \mathcal{L}_{l+1}}\left[\Pr_{u \in O_{L_{l+1}}}[f_{i_1}(u) = \cdots = f_{i_{l+1}}(u) = 1] \geq \frac{1}{4c_1c_2c_3}\right] \geq \frac{1}{2c_2c_3},$$

ゆえに,

$$\Pr_{L_{l+1} \in \mathcal{L}_{l+1}}\left[\Pr_{u \in O_{L_{l+1}}}[f_{i_1}(u) = \cdots = f_{i_{l+1}}(u) = 1] \geq \frac{1}{2^{(l+1)^2(t+2)}}\right] \geq \frac{1}{2c_2c_3} \geq \frac{1}{2^{(l+1)(t+2)}}.$$

よって $k = l+1$ のときも成り立つ.

$\mathcal{L}_\alpha$の要素は Vのみであることに注意すると, $k = \alpha$としたときの (6) 式より, $\Pr_{u \in O_V}[\forall i \in \{1,\ldots,\alpha\} \quad f_i(u) = 1] > 0$. よって, ある $u \in O_V$と $u^+ \in \mathrm{CLIQUE}(m,s)^{-1}(1)$ が存在して, $(u,u^+) \in G(\mathrm{CLIQUE}(m,s))$, かつ, 任意の $i \in \{1,\ldots,\alpha\}$ に対して, $(u,u^+) \notin G(f_i)$. これは, 仮定 (*1) に矛盾する. よって定理 4は証明された. □

参考文献

[AB87] N. Alon and R. B. Boppana, "The Monotone Circuit Complexity of Boolean Functions", *Combinatorica*, Vol. 7, No. 1, pp. 1–22, 1987.

[AM96] K. Amano and A. Maruoka, "Potential of the Approximation Method", *Proc. 37th FOCS*, pp. 431–440, 1996.

[BNT95] R. Beals, T. Nishino and K. Tanaka, "More on the Complexity of Negation-Limited Circuits", *Proc. 27th STOC*, pp. 585–595, 1995.

[BT96] N.H. Bshouty and C. Tamon, "On the Fourier Spectrum of Monotone Functions", *J. ACM*, Vol. 43, No. 4, pp. 747–770, 1996.

[BU97] C. Berg and S. Ulfberg, "Symmetric Approximation Arguments for Monotone Lower Bounds without Sunflowers", To appear in:*Computational Complexity*.

[Fis74] M.J. Fischer, "The Complexity of Negation-Limited Networks–a Brief Survey", *Lecture Notes in Computer Science 33*, Springer-Verlag, Berlin, pp. 71–82, 1974.

[Hak95] A. Haken, "Counting Bottlenecks to Show Monotone P≠NP", *Proc. 36th FOCS*, pp. 36–40, 1995.

[Juk97] S. Jukna, "Finite Limits and Monotone Computations: The Lower Bounds Criterion", *Proc. 12th Computational Complexity*, 1997.

[Mar58] A. A. Markov, "On the Inversion Complexity of a System of Functions", *J. ACM*, Vol. 5, pp.331–334, 1958.

[Raz85] A. A. Razborov, "Lower Bounds on the Monotone Complexity of Some Boolean Functions", *Soviet Math. Dokl.*, Vol. 281, pp. 798–801, 1985.

[RM97] R. Raz and P. McKenzie, "Separation of the Monotone NC Hierarchy", *Proc. 38th FOCS*, 1997.

[RW89] R. Raz and A. Wigderson, "Probabilistic Communication Complexity of Boolean Relations", *Proc. 30th FOCS*, pp. 562–567, 1989.

[ST97] J. Simon and S.C. Tsai, "A Note on the Bottleneck Counting Argument", *Proc. 12th Computational Complexity*. 1997.

[SW93] M. Santha and C. Wilson, "Limiting Negations in Constant Depth Circuits", *SIAM J. Comput.*, Vol. 22, No. 2, pp. 294–302, 1993.

[Tar87] E. Tardos, "The Gap between Monotone and Non-Monotone Circuit Compleixty is Exponential", *Combinatorica*, Vol. 7, pp. 393–394, 1987.

[Val86] L.G. Valiant, "Negation is Powerless for Boolean Slice Functions", *SIAM J. Comput.*, Vol. 15, No. 2, pp. 531–535, 1986.