数理解析研究所講究録
第871巻 1994年 94-99

否定数限定反転回路の複雑さの下界について

田中 圭介　　西野 哲朗
Keisuke Tanaka　　Tetsuro Nishino
北陸先端科学技術大学院大学 情報科学研究科

1 はじめに

$B=\{0,1\}$, $B_n=\{f \mid f: B^n \to B\}$ とする. Markov [2] は, すべての $F \subseteq B_n$ を計算するには, $b(n)=\lceil \log(n+1) \rceil$ 個の NOT ゲートが必要かつ十分であることを示した. 以下では, 回路中で使用できる NOT ゲートの個数を $b(n)$ に制限したときの組合せ回路を, **否定数限定回路** と呼ぶ. Fischer [1] は, n 変数を反転する否定数限定回路のサイズの上界が, $O(n^2(\log n)^2)$ であることを示した. Tanaka と Nishino [4] は, この上界を $O(n(\log n)^2)$ に改良した.

本稿では, この n 変数を反転する否定数限定回路のサイズおよび深さの下界について考察し, サイズおよび深さについてそれぞれ, $5n+3\log(n+1)-6$, $4\log(n+1)+2$ の下界を示す. また, n 変数を反転する否定数限定回路にある種の制約を加え, その回路サイズが超線形下界をもつような二つの特殊な場合を紹介する.

2 準備

組合せ回路 の **基底** を $\{\wedge,\vee,\neg\}$ とし, **単調回路**の基底を $\{\wedge,\vee\}$ とする. また, n 個の **ブール変数** の集合 $\{x_1,\ldots,x_n\}$ を X_n で表し, $V_n=\{\neg x_1,\ldots,\neg x_n\}$ とする. $C^{b(n)}(f)$ で, 関数 f の否定数限定回路計算量を表すものとし, $D^{b(n)}(f)$ で, 関数 f の否定数限定回路の深さを表すものとする. また, V_n を計算する否定数限定回路を $\mathcal{I}_n$ で表す.

$\#_1(X_n)$ は X_n に対する入力中の 1 の個数を表す. また, $A=(a_1,\ldots,a_n) \in \{0,1\}^n$, $B=(b_1,\ldots,b_n) \in \{0,1\}^n$ としたとき, すべての $1 \leq i \leq n$ について $a_i \leq b_i$ ならば $A \leq B$ とし, $A \leq B$, かつ $a_i < b_i$ なる $1 \leq i \leq n$ が存在するなら $A<B$ とする. また, 任意の n 変数 **対称ブール関数** f を *spectrum* と呼ばれる長さ $n+1$ の二進列 $s_0 \ldots s_n$ によって定義する. すなわち, s_i は $\#_1(X_n)=i$ のときの $f(X_n)$ の値を表すものとする.

3 反転回路の複雑さの下界

以下では, 一般性を失うことなく, $n = 2^l - 1$ と仮定する. $\mathcal{I}_n$ に含まれる l 個 ($l = \log(n+1)$) の NOT ゲートにおいて計算される関数を, $y_1, \ldots, y_l$ とする (図 1). さらに,

$$Y(X_n) \stackrel{\text{def}}{=} (y_1(X_n), \ldots, y_l(X_n))$$

とする.

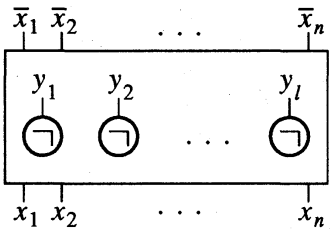

図 1: 回路 $\mathcal{I}_n$

ここで, 任意のベクトル $A \in \{0,1\}^n$ に対して, $A_1, \ldots, A_n$ ($A_i \in \{0,1\}^n$, $1 \leq i \leq n$) を以下のように定義する.

1. $\#_1(A) = k$ ならば $A_k = A$ と定義する.
2. A_{k-1} は, $\#_1(A_{k-1}) = k-1$ かつ $A_{k-1} < A_k$ を満たす任意のベクトルとする.
   A_{k-2} は, $\#_1(A_{k-2}) = k-2$ かつ $A_{k-2} < A_k$ を満たす任意のベクトルとする.
   $\vdots$
   $A_0 = (0,0,\ldots,0) \in \{0,1\}^n$ とする.
3. A_{k+1} は, $\#_1(A_{k+1}) = k+1$ かつ $A_k < A_{k+1}$ を満たす任意のベクトルとする.
   A_{k+2} は, $\#_1(A_{k+2}) = k+2$ かつ $A_{k+1} < A_{k+2}$ を満たす任意のベクトルとする.
   $\vdots$
   $A_n = (1,1,\ldots,1) \in \{0,1\}^n$ とする.

補題 1 上のように定義された $A_0, \ldots, A_n$ に対して, $A_i \neq A_j$ ならば $Y(A_i) \neq Y(A_j)$ が成り立つ. □

補題 2 $A, B \in \{0,1\}^n$ とする. このとき, $\#_1(A) = \#_1(B)$ ならば $Y(A) = Y(B)$ である. □

補題 3 $A, B \in \{0,1\}^n$ とする．このとき $\#_1(A) \neq \#_1(B)$ ならば $Y(A) \neq Y(B)$ である． □

補題 3 より，$Y(A_0), \ldots, Y(A_n)$ は，すべて互いに異なる値をとらなくてはならない．すなわち Y は，$n+1$ 通りに変化しなくてはならない．Y の長さは $l = \log(n+1)$ なので，$2^l = n+1$ より，Y は $(0,\ldots,0)$ から $(1,\ldots,1)$ までの，長さ l のすべての列を網羅することになる．したがって，補題 2 も考慮すると，$y_1, \ldots, y_l$ は，**すべて互いに異なる対称関数** であることがわかる．

ここで，NOT ゲートは 1 入力 1 出力なので，$y_1, \ldots, y_l$ を計算する NOT ゲートの入力において計算される関数をそれぞれ，$z_1, \ldots, z_l$ とすると，これらもまた，互いに異なる対称関数である．$Z(X_n) = (z_1(X_n), \ldots, z_l(X_n))$ と定義する．

補題 4 $A = (0,\ldots,0)$, $B = (1,\ldots,1) \in \{0,1\}^n$ とする．$Z(A) = (0,\ldots,0)$, かつ $Z(B) = (1,\ldots,1)$ である． □

$A_0 = (0,\ldots,0)$, $A_n = (1,\ldots,1)$ とし，A_i, $1 \leq i \leq n-1$ を上と同様に一通りに固定する．以下では，z_i の spectrum を，$s(z_i) = (r_1, \ldots, r_k)$ と表すことにする．ただし，$\{r_1, \ldots, r_k\} = \{t \mid 1 \leq t \leq n,\ z_i(A_{t-1}) \neq z_i(A_t)\}$ かつ，$r_1 < r_2 < \cdots < r_k$ とする．z_i が対称関数なので，$s(z_i)$ をこのように表現できることに注意する．

ここで，すべての $1 \leq i \leq l$ に対し，補題 4 より，$z_i(A_0) = 0$ となることに注意する．よって，この表記法により z_i は一意に表現される．y_i の spectrum も同様に $s(y_i)$ と表す．

事実 1 我々は，$Y(A_i) = (\overline{z_1(A_i)}, \ldots, \overline{z_l(A_i)})$, $0 \leq i \leq n$ と定義した．ここで，i を 0 から n まで変化させると，上で述べたように，$Y(A_i)$ は $(0,\ldots,0)$ から $(1,\ldots,1)$ までの，長さ l のすべての二進列を値として取る．したがって，$(z_i(A_0), \ldots, z_i(A_n))$ の中には，$(n+1)/2 = 2^{l-1}$ 個の 0 と 1 が表れる．

定理 1 関数 $z_1, \ldots, z_l$ を，以下の条件を満たすように並べることができる：各 i $(1 \leq i \leq l)$ に対し，z_i のみが，$\mathcal{I}_n$ 内において $y_1, \ldots, y_{i-1}$ の値と，*AND* ゲート，*OR* ゲートのみを用いた部分回路によって計算される．さらに z_i の *spectrum* は，

$$s(z_i) = \left(\frac{n+1}{2^i}, \frac{2(n+1)}{2^i}, \ldots, \frac{(2^i-1)(n+1)}{2^i} \right)$$

である．

Proof. **場合 1** ($i = 1$ のとき)： $z_1, \ldots, z_l$ のうちの少なくとも一つの関数は，$\mathcal{I}_n$ 内で NOT ゲートを一つも用いずに，すなわち単調回路によって計算されている．そこで，一般性を失うことなく，z_1 が単調回路で計算されているものとする．したがって，z_1 は単調な対称関数，すなわち，しきい値関数である．さらに事実 1 より，

$$z_1 = T^n_{(n+1)/2}$$

となる. すなわち,

$$s(z_1) = \left(\frac{n+1}{2}\right)$$

である. (このとき $\mathcal{I}_n$ 内で, z_1 を計算するのに用いられる素子数, すなわち AND ゲートと OR ゲートの個数は, $C^m(T^n_{(n+1)/2})$ 以上であることに注意する.)

一方, $z_2, \ldots, z_l$ のなかに, 単調回路で計算される関数が存在したとすると, その関数 z_j の spectrum も $s(z_j) = ((n+1)/2)$ となり, $z_j = z_1$ となるので矛盾である.

場合 2 ($i \geq 2$ のとき): $z_2, \ldots, z_l$ を計算する回路のなかから, NOT ゲートの個数が最小の回路 (D と呼ぶ) を選び出す. 一般性を失うことなく, D は関数 z_2 を計算する回路であると仮定する. いま, D に NOT ゲートが 2 個以上含まれていたとする. 場合 1 より, それらの NOT ゲートに対する入力 $z_j, z_k, \ldots$ のうちの少なくとも一つは, NOT ゲートを一つは含まなければならない. そのような入力の一つを z_j としよう. しかし, z_j を計算する回路中に存在する NOT ゲートの個数は, D 中の NOT ゲートの個数よりも少なくとも一つは少ない. これは矛盾である.

場合 1 より, $z_2, \ldots, z_l$ を計算する回路は, すべて NOT ゲートを含んでいる. したがって, z_2 の回路 D は NOT ゲートを 1 個だけ含むことになる. よって D は, y_1 の出力と AND ゲート, OR ゲートのみから構成されうる. もし, D が y_1 の出力を用いないとすると, z_2 は単調関数となるので矛盾である.

一方, 場合 1 より, $y_1 = \neg T^n_{(n+1)/2}$ である. したがって, $\#_1(X_n) < (n+1)/2$ のときは常に $y_1(X_n) = 1$ であり, $\#_1(X_n) \geq (n+1)/2$ のときは常に $y_1(X_n) = 0$ である. よって, z_2 の spectrum が 1 から 0 に非単調に変化するのは, $\#_1(X_n) = (n+1)/2$ のときにのみ可能である. また 補題 4 より, $z_2(A_0) = 0$ かつ $z_2(A_n) = 1$ である. 以上のことから z_2 の spectrum は,

$$\underbrace{0\cdots01\cdots1}_{(n+1)/2}\underbrace{0\cdots01\cdots1}_{(n+1)/2}$$

という形になる. さらに事実 1 より, z_2 の spectrum も同数の 0 と 1 を含む.

ところで, 第 i 行第 j 列成分 ($1 \leq i \leq n$, $1 \leq j \leq l$) が $z_j(A_{i-1})$ であるような $n+1$ 行 l 列の 0-1 行列を考えよう ($l = 3$ の場合の例を図 2 に示す.). この行列の同一行内の第 1 列目と第 2 列目の数の組 (p, q) の値の可能な組合せとしては, (0, 0), (0, 1), (1, 0), (1, 1) があるが, 事実 1 を満足するためには, 行列内にこれらの組がすべて同数ずつ現れていなければならない.

したがって, z_2 の spectrum は,

$$s(z_2) = \left(\frac{n+1}{4}, \frac{n+1}{2}, \frac{3(n+1)}{4}\right)$$

でなければならない.

最後に, $\mathcal{I}_n$ 内で, y_1 の値と, AND ゲート, OR ゲートのみを用いた部分回路によって計算できる関数が, $z_3, \ldots, z_l$ のなかにも存在したとすると, それらの関数の spectrum は z_2 の spectrum と同一となり, 矛盾を生じる.

	z_1	z_2	z_3	
A_0	0	0	0	$= Z(A_0)$
A_1	0	0	1	$= Z(A_1)$
A_2	0	1	0	$= Z(A_2)$
A_3	0	1	1	$= Z(A_3)$
A_4	1	0	0	$= Z(A_4)$
A_5	1	0	1	$= Z(A_5)$
A_6	1	1	0	$= Z(A_6)$
A_7	1	1	1	$= Z(A_7)$

図 2: $l = 3$ の場合の例

以下, 同様の議論を繰り返すことにより, $3 \leq i \leq l$ なる各 i についても定理が成り立つ. □

定理 1 を用い, 以下の下界に関する二つの定理を得た.

定理 2 すべての $n \geq 1$ に対して,

$$C^{b(n)}(V_n) \geq 5n + 3\log(n+1) - 6. \quad \square$$

定理 3 すべての $n \geq 3$ に対して,

$$D^{b(n)}(V_n) \geq 4\log(n+1) + 2. \quad \square$$

4 超線形下界をもつ特殊な反転回路

n 変数を反転する否定数限定回路のサイズが, 超線形下界をもつような二つの場合について紹介する. まず, 入力から各ゲートへのすべての path の長さが等しいという制約を持つ **synchronous circuit** について考える (see [3]).

定理 4 すべての $n \geq 3$ に対して, V_n を計算する否定数限定 *synchronous circuit* のサイズは, $4n\log(n+1) + 2n$ 以上である. □

$\mathcal{I}_n$ 内に現れる $b(n)$ 個の NOT ゲートを $N_1, \ldots, N_{b(n)}$ と表す. ただし, これらの NOT ゲートの順序は以下の条件を満たすものとする:

N_{i+1} $(0 \leq i \leq b(n)-1)$ に入力を供給する NOT ゲートは $N_1, \ldots, N_i$ のみであり, かつ, $N_1, \ldots, N_i$ のすべてから, N_{i+1} に至るパスが存在する.

実際に, $\mathcal{I}_n$ 内の NOT ゲートが, 上のような順序に整列していることを証明した [4].

次に, V_n を計算する否定数限定回路のサイズが, 超線形下界を持つようなもう一つの場合を示す. そのために, 以下のような制約を考える.

制約 A: 反転回路 $\mathcal{I}_n$ 内の以下の条件を満たすゲート G が, すべて対称関数を計算する:

A1 $\mathcal{I}_n$ 内に $N_1, \ldots, N_{b(n)-1}$ のいずれかから G への path が存在し, かつ,

A2 $\mathcal{I}_n$ 内に G から $N_{b(n)}$ へ至る path が存在する.

定理 5 制約 A を満たし, かつ V_n を計算する否定数限定回路のサイズは $\Omega(n \log n)$ である. □

参考文献

[1] M. J. Fischer, The complexity of negation-limited networks–a brief survey, In *Lecture Notes in Computer Science 33*, pp. 71–82. Springer-Verlag, Berlin, 1974.

[2] A. A. Markov, On the inversion complexity of a system of functions, *Journal of the ACM*, **5**:331–334, 1958.

[3] J. E. Savage, *The Complexity of Computing*, John Wiley & Sons, 1976.

[4] K. Tanaka and T. Nishino, On the complexity of negation-limited Boolean networks, To appear in *1994 ACM Symposium on Theory of Computing*. Also available as: Research Report, IS-RR-93-0013F, JAIST, November 1993.