数理解析研究所講究録
906巻 1995年 89-95



# 対称関数の否定数限定回路計算量について

田中 圭介 (Keisuke Tanaka)
北陸先端科学技術大学院大学 情報科学研究科
tanaka@jaist.ac.jp

西野 哲朗 (Tetsuro Nishino)
電気通信大学 電子情報学科
nishino@sw.cas.uec.ac.jp

## 1 はじめに

Markov [3] は, すべての $n$ 変数ブール関数を計算するには, $\lceil \log(n+1) \rceil$ 個の NOT ゲートが必要かつ十分であることを示した. Tanaka と Nishino は, 使用できる NOT ゲートを $\lceil \log(n+1) \rceil$ 個に制限した, $n$ 変数を反転する組合せ回路の複雑さについて考察し [6], さらに, 使用できる NOT ゲートを $\lceil \log(n+1) \rceil - 1$ 個に制限した, parity 関数を計算する組合せ回路の複雑さについて考察した [7].

本稿では, 任意の対称関数 $F$ に対して, 使用できる NOT ゲートを $\lceil \log(g+1) \rceil$ 個 ($g$ は $F$ の decrease) に制限した, $F$ を計算する組合せ回路の 複雑さについて考察する.

## 2 準備

NOT ゲートを高々 $r$ 個含むような $\{\wedge, \vee, \neg\}$- 基底上の回路を $r$-circuit と呼ぶ. $C^r(f)$ $(D^r(f))$ で, ブール関数 $f$ を計算する $r$-circuit の素子数の最小値 ($r$-circuit の深さの最小値) を表す. $r$ が制限されているとき, $r$-circuit を **否定数限定回路** と呼び, $C^r(f)$ を $f$ の **否定数限定回路計算量** と呼ぶ. 特に, 0-circuit を **単調回路** と呼び, $C^0(f)$ を $f$ の **単調回路計算量** と呼ぶ. $C^0(f)$ を $C^m(f)$ とも表記する. $r$ が制限されていないとき, $r$-circuit を **組合せ回路** と呼び, $C^r(f)$ を $f$ の **組合せ回路計算量** と呼ぶ. この場合, $C^r(f)$ を $C(f)$ とも表記する.

$A = (a_1, \ldots, a_n) \in \{0,1\}^n$, $B = (b_1, \ldots, b_n) \in \{0,1\}^n$ とするとき, すべての $1 \leq i \leq n$ に対して $a_i \leq b_i$ ならば $A \leq B$ する. さらに, $A \leq B$ であり, かつ $a_i < b_i$ なる $1 \leq i \leq n$ が存在するならば $A < B$ とする. $S$ を $X_n$ の任意の部分集合とする. **部分割り当て** $\pi$ とは, $\pi : S \to \{0,1\}$ なる形の関数のことをいう. 以下では, $|S|$ を $|\pi|$ で表し, 部分割り当て $\pi$ によって $n$ 変数ブール関数 $f$ から導かれる $n - |\pi|$ 変数ブール関数を $f^{|\pi}$ で表すものとする.

$n$ 個の **ブール変数** の集合を $X_n = \{x_1, \ldots, x_n\}$ で表し, $\#_1(X_n)$ で $X_n$ に対する割り当て中の 1 の個数を表す. $n$ 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 $s_0 \cdots s_n$ によって定義する. ただし, $s_i$ は $\#_1(X_n) = i$ のときの $f(X_n)$ の値を表す. また, $\#_1(X_n) \geq k$ のとき, かつそのときに限り 1 を出力するような $k$-**しきい値関数** を $T_n^k(X_n)$ で表す.

## 3 主補題

本節では, 対称関数を計算する否定数限定回路中の NOT ゲートにおいて計算される関数に関する, 主補題 (補題 1) を示す.

$g(F_n) = (d_1, \ldots, d_m)$ を以下のように定義する: $A_i \in \{0,1\}^n$ $(0 \leq i \leq n)$ かつ $A_0 < \cdots < A_n$ とする. $A_0 = (0, \ldots, 0)$ であることに注意する. 任意の $n$ 変数入力関数 $f$ に対して, $g(f) = (d_1, \ldots, d_m)$ と定義する. ただし, $\{d_1, \ldots, d_m\} = \{d \mid 1 \leq d \leq n,\ f(A_{d-1}) \not\leq f(A_d)\}$ かつ $d_1 < \cdots < d_m$ であるとする. $|g(f)|$ を $f$ の decrease とよぶ. $F_n$ を,

$$g(F_n) = (d_1, \ldots, d_m)$$

であるような $X_n$ 上の任意の対称関数とする. 以下では, 記述を単純にするために, 一般性を失うことなく, $m = 2^r - 1$ $(r = 0, 1, \ldots)$ であるような $F_n$ についてのみ考察する. このとき, $r = \log(m+1) = \lceil \log(|g(F_n)| + 1) \rceil$ であることに注意する. [3] より, $F_n$ を計算するには $r$ 個の NOT ゲートが必要かつ十分であることが知られている. $F_n$ を計算する最適な $r$-circuit を $\mathcal{F}_n$ で表す.

$\mathcal{F}_n$ に含まれる $r$ 個の NOT ゲートを $N_1, \ldots, N_r$ とし, その出力において計算される関数を, それぞれ $y_1, \ldots, y_r$ とする. また, $N_1, \ldots, N_r$ の入力において計算される関数を, それぞれ $z_1, \ldots, z_r$ とする. NOT ゲートは 1 入力 1 出力 なので, すべての $i$, $1 \leq i \leq r$ に対して, $y_i = \neg z_i$ であることに注意する.

$f$ を $f(A_0) = 0$ を満たす任意の対称関数とする. 以下では, $f$ の spectrum を $s(f) = (r_1, \ldots, r_k)$ と表す. ただし, $\{r_1, \ldots, r_k\} = \{t \mid 1 \leq t \leq n,\ f(A_{t-1}) \neq f(A_t)\}$ かつ $r_1 < \cdots < r_k$ であるとする. $f$ は, この表記法によって一意に表現できる.

**補題 1** *$\mathcal{F}_n$ 内の $r$ 個の NOT ゲート $N_1, \ldots, N_r$ から集合 $\{1, \ldots, r\}$ への全単射 $\sigma$ が存在して, $z_{\sigma(N_1)}, \ldots, z_{\sigma(N_r)}$ は以下の条件を満足する: 各 $i$ $(1 \leq i \leq r)$ に対し, $z_i$ のみが $y_1, \ldots, y_{i-1}$ の値と, AND ゲート, OR ゲートのみを用いた $\mathcal{F}_n$ の部分回路によって計算される. さらに, $z_i$ は $X_n$ 上の対称関数であり, その spectrum は,*

$$s(z_i) = (d_{\frac{(m+1)}{2^i}}, d_{\frac{2(m+1)}{2^i}}, d_{\frac{3(m+1)}{2^i}}, \ldots, d_{\frac{(2^i-1)(m+1)}{2^i}})$$

*である.* □

$\#_1(X_n)$ が $k$ で割り切れるとき, かつそのときに限り 1 を出力するような **modular 関数** を $MOD_n^k(X_n)$ で表す. $n = k2^{rm} - k$ とする. $MOD_n^k$ は対称関数であり, $|g(MOD_n^k)| = n/k$ なの

で, 補題 1 を適用することにより, $MOD_n^k$ を計算する最適な $r_m$-circuit $\mathcal{M}_n$ に関して, 以下の系が得られる.

**系 1** $r_m = \log(n/k+1)$ とする. このとき, $\mathcal{M}_n$ 内の $r_m$ 個の $NOT$ ゲート $N_1, \ldots, N_{r_m}$ から集合 $\{1, \ldots, r_m\}$ への全単射 $\sigma$ が存在して, $z_{\sigma(N_1)}, \ldots, z_{\sigma(N_{r_m})}$ は以下の条件を満足する: 各 $i$ $(1 \leq i \leq r_m)$ に対し, $z_i$ のみが $y_1, \ldots, y_{i-1}$ の値と, $AND$ ゲート, $OR$ ゲートのみを用いた $\mathcal{M}_n$ の部分回路によって計算される. さらに, $z_i$ は $X_n$ 上の対称関数であり, その *spectrum* は,

$$s(z_i) = (\frac{n+k}{2^i} - k + 1,\ \frac{2(n+k)}{2^i} - k + 1,\ \frac{3(n+k)}{2^i} - k + 1,\ \ldots,\ \frac{(2^i-1)(n+k)}{2^i} - k + 1)$$

である. □

$\#_1(X_n)$ が奇数のとき, かつそのときに限り 1 を出力するような **parity 関数** を $PARITY_n(X_n)$ で表す. $n = 2^{r_p+1} - 1$ とする. $PARITY_n$ を計算する最適な $r_p$-circuit を $\mathcal{P}_n$ で表す. $PARITY_n$ は対称関数であり, $|g(PARITY_n)| = (n-1)/2$ なので, $PARITY_n$ を計算する最適な $r_p$-circuit に関しても, 系 1 と同様な系が成り立つ. ただし, $r_p = \log((n-1)/2+1)$ とし, かつ,

$$s(z_i) = (\frac{n+1}{2^i},\ \frac{2(n+1)}{2^i},\ \frac{3(n+1)}{2^i},\ \ldots,\ \frac{(2^i-1)(n+1)}{2^i})$$

とする.

また, $PARITY_n$ の否定 (すなわち $\#_1(X_n)$ が偶数のとき, かつそのときに限り 1 を出力するような関数) を $\overline{PARITY}_n(X_n)$ で表す. $n = 2^{r_{\overline{p}}+1} - 2$ とする. $\overline{PARITY}_n$ は対称関数であり, $|g(\overline{PARITY}_n)| = n/2$ なので, $\overline{PARITY}_n$ を計算する最適な $r_{\overline{p}}$-circuit に関しても, 系 1 と同様な系が成り立つ. ただし, $r_{\overline{p}} = \log(n/2+1)$ とし, かつ,

$$s(z_i) = (\frac{n+2}{2^i} - 1,\ \frac{2(n+2)}{2^i} - 1,\ \frac{3(n+2)}{2^i} - 1,\ \ldots,\ \frac{(2^i-1)(n+2)}{2^i} - 1)$$

とする.

さらに, $G_n^k(X_n) = T_n^k(x_1, \ldots, x_n) \oplus x_1 \oplus \cdots \oplus x_n$, $n = 2^{r_g+1}$ とする. $G_n^k$ は対称関数であり, $|g(G_n^k)| = n/k$ なので, $G_n^k$ を計算する最適な $r_g$-circuit に関しても, 系 1 と同様な系が成り立つ.

## 4 対称関数の否定数限定回路計算量

$\mathcal{M}_n$ のサイズおよび深さの上界に関しては, 以下の結果が知られている [2, 5, 6].

**主張 1** *1.* $C^{r_m}(MOD_n^k) = O(n \log n)$.

*2.* $D^{r_m}(MOD_n^k) = O(\log n)$. □

なお, 主張 1 の二式中の $O$-notation に隠れている定数係数は, [1] の単調 sorting 回路に依存しているため, かなり大きい値である.

補題 1 を用いると, $\mathcal{M}_n$ のサイズおよび深さの下界に関して, 以下の定理および系が得られる.

**定理 1**

$$C^{r_m}(MOD_n^k) \geq 4n + 3\log(n+k) - 5k - c. \quad \square$$

$F_n$ は $g(F_n) = (d_1, \ldots, d_m)$ であるような $X_n$ 上の任意の対称関数であり, また, $r = \log(m+1)$ であったことに注意する. 定理 1 の証明と同様な方法で, 一般に, 以下の結果が得られる.

**定理 2**

$$C^r(F_n) \geq C^m(T_n^{d_{(m+1)/2}}) + 3\log(m+1) - c. \quad \square$$

特に, parity 関数については, 以下の結果が得られる. ここで, $r_{\overline{p}} = \log(n+2) - 1$, $r_m = \log(n+k) - k$ であったことに注意する.

**系 2** *1.* $C^{r_p}(PARITY_n) \geq 4n + 3\log(n+1) - c.$

*2.* $C^{r_{\overline{p}}}(\overline{PARITY}_n) \geq 4n + 3\log(n+2) - c.$ $\square$

一方, 対称関数を計算する否定数限定回路の深さについては, 以下の結果が得られる.

**定理 3**

$$D^{r_m}(MOD_n^k) \geq 4\log(n+k) - k - c. \quad \square$$

**定理 4**

$$D^r(F_n) \geq D^m(T_n^{d_{(m+1)/2}}) + 3\log(m+1) - c. \quad \square$$

**系 3** *1.* $D^{r_p}(PARITY_n) \geq 4\log(n+1) - c.$

*2.* $D^{r_{\overline{p}}}(\overline{PARITY}_n) \geq 4\log(n+2) - c.$ $\square$

次に, $\mathcal{M}_n$ のサイズが超線形下界をもつような場合を紹介する. そのために, 以下のような制約を考える.

> **制約 A**: $\mathcal{M}_n$ 内において, $N_1, \ldots, N_l$ のいずれかからの path が存在するようなゲートの出力では, 必ず対称関数が計算されている.

**定理 5** 制約 $A$ を満たす $\mathcal{M}_n$ のサイズは $\Omega(((n-k)\log(n-k))/k)$ である. □

$r=\log(m+1)$ であり, かつ, $\mathcal{F}_n$ は $F_n$ を計算する最適な $r$-circuit であったことに注意する. また, $A_i \in \{0,1\}^n$ $(0 \leq i \leq n)$ かつ $A_0 < \cdots < A_n$ であった.

**定理 6** 制約 $A$ を満たす $\mathcal{F}_n$ のサイズは, $C^m(T_n^{q_1}, T_n^{q_2}, \ldots, T_n^{q_k})$ 以上である. ただし, $\{q_1, \ldots, q_k\} = \{q \mid 1 \leq q \leq n,\ F(A_{q-1}) \neq F(A_q)\}$ とする. □

## 5 否定数と回路サイズの関係について

本節では, NOT ゲートの個数と回路サイズの関係について考察する. Tardos [8] は, 単調回路の複雑さが $2^{\Omega(n^{1/6-o(1)})}$ であるような, 多項式時間計算可能な単調関数 $f_n$ の存在を示した. すなわち, 次の命題が成り立つ [4].

**主張 2** 以下の条件を満たす $t$ $(0 \leq t \leq \lceil \log(n+1) \rceil - 1)$ が存在する:

$$\frac{C^t(f_n)}{C^{t+1}(f_n)} = \exp(\Omega(n^{1/6-o(1)})). \quad \square$$

$n = 2^{r_h+2}-1$, $m=(n-1)/2$ とする. $r_h = \log(n+1)-2$ であることに注意する. ここで, 次のような $n$ 変数関数 $h_n$ を考える:

$$h_n(x_1, \ldots, x_{m+2}, w_1, \ldots, w_{m-1}) = f_{m+2}(x_1, \ldots, x_{m+2}) \oplus w_1 \oplus \cdots \oplus w_{m-1}.$$

以下の主張は [6] より自明である.

**主張 3**

$$C^{r_h+2}(h_n) \leq 2C(h_n) + O(n(\log n)^2). \quad \square$$

$C(h_n)$ は, 明らかに $n$ の多項式で上から押えられる. $h_n$ を計算する最適な $r_h$-circuit を $\mathcal{H}_n$ で表す. 補題 1 と同様の議論により, 以下の補題が得られる.

**補題 2** $\mathcal{H}_n$ 内の $r_h$ 個の *NOT* ゲート $N_1, \ldots, N_{r_h}$ から集合 $\{1, \ldots, r_h\}$ への全単射 $\sigma$ が存在して, $z_{\sigma(N_1)}, \ldots, z_{\sigma(N_{r_h})}$ は以下の条件を満足する: 各 $i$ $(1 \leq i \leq r_h)$ に対し, $z_i$ のみが $y_1, \ldots, y_{i-1}$ の値と, *AND* ゲート, *OR* ゲートのみを用いた $\mathcal{H}_n$ の部分回路によって計算される. さらに, $z_i$ は $\{f_{m+2}(x_1, \ldots, x_{m+2}), w_1, \ldots, w_{m-1}\}$ 上の対称関数であり, その *spectrum* は,

$$s(z_i) = (\frac{m+1}{2^i}, \frac{2(m+1)}{2^i}, \frac{3(m+1)}{2^i}, \ldots, \frac{(2^i-1)(m+1)}{2^i})$$

である.

**証明.** 各 $x_i$ $(1 \leq i \leq m+2)$ は, すべての $w_j$ $(1 \leq j \leq m-1)$ と独立なので, 関数値 $f_{m+2}(x_1, \ldots, x_{m+2})$ は, すべての $w_j$ $(1 \leq j \leq m-1)$ と独立な変数 $w_m$ とみなすことができる. このとき, $h_n(w_1, \ldots, w_{m-1}, w_m) = PARITY_m(w_1, \ldots, w_{m-1}, w_m)$, $m = 2^{r_h+1} - 1$ であり, $\mathcal{H}_n$ は $r_h$ 個の NOT ゲートを含む. よって, 系 1 を $\mathcal{H}_n$ に適用することにより, 補題 2 が証明できる. □

**主張 4**

$$C^{r_h}(h_n) = \exp(\Omega(n^{1/6-o(1)})).$$

**証明.** $\mathcal{H}_n$ 内には $N_1, \ldots, N_{r_h}$ 以外の NOT ゲートが存在しないので, $f_{m+2}(x_1, \ldots, x_{m+2})$ は単調部分回路で計算されなくてはならない. よって 補題 2 より, $z_1$ を計算する部分回路のサイズは, 少なくとも $C^m(z_1(f_{m+2}(x_1, \ldots, x_{m+2}), w_1, \ldots, w_{m-1}))$ である.

$w_1, \ldots, w_{m-1}$ のうちの $(m-1)/2$ 個の変数を 1 に固定し, 残りの変数を 0 に固定する部分割り当てを $\pi$ とする. このとき, [8] より,

$$\begin{aligned} C^m(z_1(f_{m+2}(x_1, \ldots, x_{m+2}), w_1, \ldots, w_{m-1})) &\geq C^m(z_1|^\pi(f_{m+2}(x_1, \ldots, x_{m+2}), w_1, \ldots, w_{m-1})) \\ &= C^m(T_m^{(m+1)/2}|^\pi(f_{m+2}(x_1, \ldots, x_{m+2}), w_1, \ldots, w_{m-1})) \\ &= C^m(f_{m+2}(x_1, \ldots, x_{m+2})) \\ &= 2^{\Omega(m^{1/6-o(1)})} \\ &= 2^{\Omega(n^{1/6-o(1)})}. \quad \square \end{aligned}$$

最後に, 主張 3 と 4 より, 以下の定理を得る.

**定理 7** $t = \log(n+1) - 2$, または $t = \log(n+1) - 1$ のどちらかのときに以下が成り立つ.

$$\frac{C^t(h_n)}{C^{t+1}(h_n)} = \exp(\Omega(n^{1/6-o(1)})). \quad \square$$

**参考文献**


[1] AJTAI, M., KOMLÓS, J., AND SZEMERÉDI, E. An $O(n \log n)$ sorting network. In *Proceedings of the 15th Annual ACM Symposium on the Theory of Computing* (1983), pp. 1–9.

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

[3] MARKOV, A. A. On the inversion complexity of a system of functions. *J. ACM 5* (1958), 331–334.

[4] NISHINO, T., AND TANAKA, K. On the negation-limited circuit complexity of clique functions. To appear in *IEICE Trans. on Information and Systems*, Dec. 1993.

[5] SANTHA, M., AND WILSON, C. Limiting negations in constant depth circuits. *SIAM J. Comput. 22*, 2 (Apr. 1993), 294–302.

[6] TANAKA, K., AND NISHINO, T. On the complexity of negation-limited Boolean networks. In *Proceedings of the 26th Annual ACM Symposium on the Theory of Computing* (May 1994), pp. 38–47.

[7] 田中 圭介, 西野 哲朗, Parity 関数を計算する否定数限定回路の複雑さについて, 夏の LA シンポジウム, 蓼科, 1994 年 7 月 (「情報基礎理論ワークショップ論文集」に掲載予定).

[8] TARDOS, É. The gap between monotone and non-monotone circuit complexity is exponential. *Combinatorica 7*, 4 (1987), 141–142.