

Lower bounds of the negation-limited circuit complexity

Shao-Chin Sung¹

Keisuke Tanaka¹

1 Introduction

1.1 Background and motivation

We do not know much about the complexities of combinational circuits (i.e., circuits with AND, OR, and NEGATION gates) for explicitly defined functions. Even a superlinear lower bound for the size of combinational circuits is not known. The complexities of monotone circuits (i.e., combinational circuits *without* NEGATION gates) for many explicitly defined functions are well understood. For example, exponential lower bounds for the size of monotone circuits are known [8, 2, 7]. Exponential gaps between monotone and combinational circuit complexity are also shown [11, 7]. So, we cannot generally derive strong lower bounds for the combinational circuit complexity using those bounds for the monotone circuit complexity.

In this situation, there is no doubt that it is necessary to understand the effect of NEGATION gates in order to obtain strong lower bounds for combinational circuit complexity. This is a motivation for the study of *negation-limited circuit complexity*, the complexity for circuits in which the number of NEGATION gates are restricted.

Markov [6] gave the number of NEGATION gates which is necessary and sufficient to compute a system of boolean functions. Especially, he showed that $\lceil \log(n+1) \rceil$ NEGATION gates are sufficient to compute *any* system of boolean functions (all logarithms and exponents in this paper are base two). In [5], Fischer constructed a polynomial size circuit that contains only $\lceil \log(n+1) \rceil$ NEGATION gates, and inverts n input variables. Owing to this result, for *any* n -input boolean function f , if there exists a polynomial size combinational circuit for f , there also exists a polynomial size circuit with only $\lceil \log(n+1) \rceil$ NEGATION gates. Tanaka and Nishino [9], and Beals, Nishino, and Tanaka [3] improved the result of Fischer, and also gave lower bounds for the negation-limited circuit complexity of several functions.

1.2 Definitions and preliminaries

Let $\tilde{x} = \{x_1, \dots, x_n\}$ be the inputs. Let $f = (f^1, \dots, f^m)$ be an n -input m -output *boolean function* $\{0, 1\}^n \rightarrow \{0, 1\}^m$. We denote by $C(f)$ the *circuit complexity* of f , i.e., the size (number of gates) of the smallest circuit of AND, OR, and NEGATION gates with inputs x_1, \dots, x_n and outputs $f^1(\tilde{x}), \dots, f^m(\tilde{x})$.

We call a circuit including at most r NEGATION gates an r -*circuit*. We denote by $C^r(f)$ the size of the smallest r -circuit computing f . If a function f cannot be computed

¹School of Information Science, Japan Advanced Institute of Science and Technology, Tatsunokuchi, Ishikawa 923-12, Japan. (son,tanaka)@jaist.ac.jp

with only r NEGATION gates, then $C^r(f)$ is undefined. When r is bounded, an r -circuit is said to be *negation-limited*. Especially, when $r = 0$, an r -circuit is said to be *monotone*.

A theorem of Markov [6] precisely determines the number r of NEGATION gates necessary and sufficient to compute f . A *chain* C in the boolean lattice $\{0, 1\}^n$ is an increasing sequence $a^1 < \dots < a^k \in \{0, 1\}^n$. The *decrease* of f on C is the number of $i \leq k$ such that $f^j(a^{i-1}) > f^j(a^i)$ for some $1 \leq j \leq m$. We define $d(f)$ to be the maximum decrease of f on any chain C . Markov has shown that $\lceil \log(d(f) + 1) \rceil$ NEGATION gates are necessary and sufficient to compute any f . Thus, $C^r(f)$ is always defined for $r \geq \lceil \log(d(f) + 1) \rceil$.

Let $|\tilde{x}|$ denote the number of ones in \tilde{x} . We define the n -input *parity* function as a function which returns one iff $|\tilde{x}|$ is odd, the n -input k -th *threshold* function as a function which returns one iff $|\tilde{x}| \geq k$ for $1 \leq k \leq n$, and the *majority* function as the $\lceil n/2 \rceil$ -th threshold function.

1.3 Main results

We first consider the complexity of negation-limited inverters. We show an upper bound $d + 3\lceil \log(n + 1) \rceil$ on depth for negation-limited inverters, by constructing an inverter with size $O(ns + n^2)$, where d and s is, respectively, the depth and the size of a sorting network with optimal depth. This upper bound matches the lower bound shown by Tanaka and Nishino [9]. Under a natural assumption, we show a superlinear lower bound $\Omega(n \log n)$ on size of depth-optimal negation-limited inverters when we ignore the depth of NEGATION gates.

Next, we consider the relationship between the number of NEGATION gates and the size of circuits. We show that there is a polynomial size circuit with $\log(n + 1)$ NEGATION gates, from which the removal of one NEGATION gate *must* cause an exponential growth on the size of circuit. This partially answers an open problem presented by Fischer [5].

2 Negation-limited inverters

Let $n + 1$ be a power of two, and let $b(n) = \log(n + 1)$. The inverter is an n -input n -output boolean function $I_n = (I_n^1, \dots, I_n^n)$, where $I_n^i(\tilde{x}) = \neg x_i$ for all $1 \leq i \leq n$. A theorem of Markov implies that $b(n)$ NEGATION gates are necessary and sufficient to compute I_n . Tanaka and Nishino [9] showed the following properties of NEGATION gates in any $b(n)$ -circuit for I_n .

1. There exists a path that goes through all $b(n)$ NEGATION gates.

For $1 \leq \alpha \leq b(n)$, we denote the α -th NEGATION gate by N_α on such a path. Let z_α and y_α , respectively, be the functions computed at the input and output of N_α , i.e., $z_\alpha = \neg y_\alpha$.

2. $z_1 z_2 \dots z_r$ is the binary representation of $|\tilde{x}|$.
3. On any path between any two NEGATION gates or any NEGATION gate and any output, there are at least one AND gate and at least one OR gate.

Observe that, $|\tilde{x}| + y_1(\tilde{x})2^{b(n)-1} + y_2(\tilde{x})2^{b(n)-2} + \dots + y_{b(n)}(\tilde{x}) = n$. From the above properties, the lower bound on depth for negation-limited inverters.

Lemma 1 (Tanaka and Nishino [9]) *Let $n + 1$ is a power of 2. Any negation-limited inverter must have depth at least $d_{MAJ} + 3b(n)$, where d_{MAJ} is the optimal depth of monotone circuit for the majority function.*

2.1 Upper bound on depth

In the previous results [5, 9, 3], they first sort the n inputs x_1, \dots, x_n by a sorting network, and the outputs are fed to a subcircuit M_n shown in [5]. M_n uses $b(n)$ NEGATION gates, and has size $O(n)$ and depth $4b(n)$. As Fischer's inverter, our inverter using $n+1$ sorting networks in parallel. Instead of the subcircuit M_n , we use a subcircuit M'_n which obtained by eliminating all gates above the last NEGATION gate in M_n . M'_n has n inputs and $b(n)$ outputs (of NEGATION gates).

M'_1 consists of one NEGATION gate, and outputs the negation of its input. M'_n uses $b(n)$ NEGATION gates, and has size $O(n)$ and depth $3b(n) - 2$. For $1 \leq \alpha \leq b(n)$, NEGATION gate N_α is in depth $3\alpha - 2$ in M'_n . That is, for $1 \leq \alpha \leq b(n)$, as the previous results $y_\alpha(\tilde{x})$ are computed in depth $d + 3\alpha - 2$ in our inverter. Since we are constructing an inverter in depth $d + 3b(n)$ and $y_{b(n)}(\tilde{x})$ are computed in depth $d + 3b(n) - 2$, $I_n^i(\tilde{x})$ must be computed by depth two with $y_{b(n)}(\tilde{x})$ and monotone functions over $\tilde{x} \cup \{y_1(\tilde{x}), \dots, y_{b(n)-1}(\tilde{x})\}$.

Let $T^k(t) = 1$ if $t \geq k$, otherwise 0 for some integer k and t , and let $t_0^i = |\tilde{x}| - x_i$, $t_\alpha^i = t_0^i + y_1(\tilde{x})2^{b(n)-1} + \dots + y_\alpha(\tilde{x})2^{b(n)-\alpha}$ for $1 \leq \alpha \leq b(n)$. Then, $T^k(t_0^i)$ is the k -th threshold function over $\tilde{x} - \{x_i\}$, and $I_n^i(\tilde{x}) = T^n(t_{b(n)}^i)$.

Theorem 2 *Let s be the size of sorting network with the optimal depth d . There exists a negation-limited inverter with the depth $d + 3b(n)$ can be constructed in size $O(ns + n^2)$.*

Proof. In parallel, we construct $n+1$ sorting network, S_0, S_1, \dots, S_n . S_0 sort the inputs in \tilde{x} , and S_i sort the inputs in $\tilde{x} - \{x_i\}$ for $1 \leq i \leq n$. The outputs of S_0 are fed to the subcircuit M'_n . As outputs of S_i , $T^k(t_0^i)$'s are computed in depth d for $1 \leq k \leq n$. As outputs of M'_n , $y_\alpha(\tilde{x})$'s are computed in depth $d + 3\alpha - 2$ for $1 \leq \alpha \leq b(n)$. Since $T^k(t_\alpha^i) = T^k(t_{\alpha-1}^i) \vee y_\alpha(\tilde{x}) \wedge T^{k-2^{b(n)-\alpha}}(t_{\alpha-1}^i)$, $I_n^i(\tilde{x})$ can be computed from $y_\alpha(\tilde{x}), \dots, y_{b(n)}(\tilde{x})$ and all $T^k(t_{\alpha-1}^i)$'s for $n - 2^{b(n)-\alpha+1} < k \leq n$. By using $2^{b(n)-\alpha-1}$ gates all $T^k(t_\alpha^i)$ for $n - 2^{b(n)-\alpha} < k \leq n$ can be obtained in depth $d + 3\alpha$, from $y_\alpha(\tilde{x})$ and $T^{k'}(t_{\alpha-1}^i)$ for $n - 2^{b(n)-\alpha+1} < k' \leq n$. Thus, $I_n^i(\tilde{x}) = T^n(t_{b(n)}^i)$ for all $1 \leq i \leq n$ are computed in depth $d + 3b(n)$.

Finally, there are $n+1$ sorting networks that each has size s , a subcircuit M'_n with size $O(n)$, and $2n - 2$ gates for computing $I_n^i(\tilde{x})$ from all $T^k(t_0^i)$ and $y_1(\tilde{x}), \dots, y_{b(n)}(\tilde{x})$ for each $1 \leq i \leq n$. Hence, the circuit has size $O(ns + n^2)$ and depth $d + 3b(n)$. ■

Using the AKS sorting networks (see [1]) in our construction, we have the following corollary.

Corollary 3 *Let d_{AKS} be the depth of the AKS sorting network. A negation-limited inverter with depth $d_{AKS} + 3b(n)$ can be constructed with size $O(n^2 \log n)$.* ■

2.2 Superlinear Lower bound on size

Here, we consider the negation-limited inverters under the following natural assumption.
Assumption A: The optimal depth of monotone circuit for the majority function is not less than that for any other threshold function. Under such an assumption, the following corollary is obtained from Lemma 1 and Theorem 2.

Corollary 4 *Let $n+1$ is a power of 2. The optimal depth of any negation-limited inverter is $d_{MAJ} + 3b(n)$, under Assumption A.* ■

Next, we consider the size of depth-optimal negation-limited inverters for $n + 1$ is a power of 2, under Assumption A. We change, in this section, our circuit model from the previous works. Namely, in the new model we ignore the size and depth of the NEGATION gates. This is a natural formulation, since the new model can be considered as the model of circuits with basis $\{\text{AND}, \text{OR}, \text{NAND}, \text{NOR}\}$, where we can interpret circuits with a limited number of NAND and NOR gates as standard negation-limited circuits. An $\Omega(n \log n)$ lower bound is shown for any depth-optimal negation-limited inverters in this model.

In any depth-optimal negation-limited inverter of this model, N_1 is in depth $d_{\mathcal{MAJ}}$, that is, N_α in depth $d_{\mathcal{MAJ}} + 2\alpha - 2$ for all $1 \leq \alpha \leq b(n)$ and the circuit has depth $d_{\mathcal{MAJ}} + 2b(n)$. We find n disjoint paths with no NEGATION gate from n gates in depth $d_{\mathcal{MAJ}} + 1$ or $d_{\mathcal{MAJ}} + 2$ to the n output gates. Each of these paths has $2b(n) - 1$ gates on it.

We say for two assignments π and π' that $\pi \geq \pi'$ iff $x_i|_\pi \geq x_i|_{\pi'}$ for all $1 \leq i \leq n$. For any functions $g(\tilde{x})$ and $g'(\tilde{x})$ and a set of assignments A , we say that $g(\tilde{x}) = g'(\tilde{x})$ over A iff $g(\pi) = g'(\pi)$ for all $\pi \in A$. Let $A_{\alpha,\beta} \subseteq \{0,1\}^n$ be a set of assignment that for all $\pi \in A_{\alpha,\beta}$, $|\pi| \bmod 2^{b(n)-\alpha} \equiv \beta$, for all $1 \leq \alpha \leq b(n)$ and $0 \leq \beta < 2^{b(n)-\alpha}$.

Lemma 5 Suppose there exists a gate G which computes a function $g(\tilde{x})$, that $g(\tilde{x}) = I_n^i(\tilde{x})$ over $A_{\alpha,\beta}$. For $2 \leq \alpha \leq b(n)$ and $0 \leq \beta \leq 2^{b(n)-\alpha}$,

1. There are at least one path from N_α to G with no NEGATION gate except N_α .
2. On each of such paths, there are at least one AND gate and at least one OR gate.
3. If G is in depth $d_{\mathcal{MAJ}} + 2\alpha$, then there are exactly one such a path.

Proof. 1. Suppose there are no such a path from N_α to G with no NEGATION gates except N_α . Then, g is a monotone function on x_1, \dots, x_n and $y_\gamma(\tilde{x})$ for all $\gamma \neq \alpha$. There exists an assignment $\pi \in A_{\alpha,\beta}$ that $|\pi| = \beta < n$ and $x_i|_\pi = 0$. Then, we have $y_\alpha(\pi) = 1$ and $g(\pi) = I_n^i(\pi) = 1$. For such an assignment π , another assignment $\pi' \in A_{\alpha,\beta}$ that $\pi' \geq \pi$, $|\pi'| = |\pi| + 2^{b(n)-\alpha} > 0$ and $x_i|_{\pi'} = 1$. We have $y_\alpha(\pi') = 0$ and $y_\gamma(\pi) = y_\gamma(\pi')$ for all $\gamma \neq \alpha$. By the monotonicity of g , we have $g(\pi') \geq g(\pi) = 1$. However, $1 = g(\pi') \neq I_n^i(\pi') = 0$.

2. Suppose on one of such paths, all gates (including G) except N_α are AND gates. There exists an assignment $\pi'' \in A_{\alpha,\beta}$, that $|\pi''| = \beta + 2^{b(n)-\alpha}$ and $x_i|_{\pi''} = 0$, since $\beta + 2^{b(n)-\alpha} < 2^{b(n)} - 1 = n$. Then, we have $y_\alpha(\pi'') = 0$. However, since all gates including except N_α are AND gates on such path, $y_\alpha(\pi'') = 0$ implies that $g(\pi'') = 0$. Again, $0 = g(\pi'') \neq I_n^i(\pi'') = 1$. For case that on such path all gates except N_α are OR gates can be prove similarly.

3. Since N_α is in depth $d_{\mathcal{MAJ}} + 2\alpha - 2$ and G in depth $d_{\mathcal{MAJ}} + 2\alpha$, on such path from N_α to G , there are one NEGATION gate, N_α , and including G exactly one AND gate and one OR gate. Thus, there are at most 2 such paths from N_α to G . Suppose there are 2 such paths from N_α to G . That is, both predecessors of G have a common predecessor, N_α . If G is an AND gate (OR gate), then both predecessors of G are OR gates (AND gates). There exist an assignment $\pi \in A_{\alpha,\beta}$ that $|\pi| = \beta + 2^{b(n)-\alpha} > 0$ and $x_i|_\pi = 1$. Since $y_\alpha(\pi) = 1$, we have $1 = g(\pi) \neq I_n^i(\pi) = 0$. \blacksquare

Let G be a gate in depth $d_{\mathcal{MAJ}} + 2\alpha$ which computes function g with $g(\tilde{x}) = I_n^i(\tilde{x})$ over $A_{\alpha,\beta}$ ($2 \leq \alpha \leq b(n)$ and $0 \leq \beta < 2^{b(n)-\alpha}$). From Lemma 5, there exists exactly one path from N_α to G that consists of N_α , and including G exactly one AND gate and

one OR gate. Let G' be the gate between N_α and G on such path. Thus, G' is in depth $d_{MAJ} + 2\alpha - 1$, since N_α is in depth $d_{MAJ} + 2\alpha - 2$ and G is in depth $d_{MAJ} + 2\alpha$. Let H_1 be the predecessor of G other than G' , and H_2 be the predecessor of G' other than N_α . We denote the function that H_i computes by $h_i(\tilde{x})$ for $1 \in \{1, 2\}$. Note that $h_1(\tilde{x})$ and $h_2(\tilde{x})$ are monotone functions over $\tilde{x} \cup \{y_\gamma(\tilde{x}) \mid \text{for } \gamma < \alpha\}$, since there no path from N_α to H_i for $i \in \{1, 2\}$.

Lemma 6 *Suppose G is an OR gate and G' is an AND gate. That is, $g(\tilde{x}) = h_1(\tilde{x}) \vee (h_2(\tilde{x}) \wedge y_\alpha(\tilde{x}))$. Then, $h_1(\tilde{x}) \wedge y_\alpha(\tilde{x}) = 0$ over $A_{\alpha, \beta}$.*

Proof. Suppose there exist an assignment $\pi \in A_{\alpha, \beta}$ such that $h_1(\pi) = y_\alpha(\pi) = 1$. It implies that $g(\pi) = I_n^i(\pi) = 1$ and $x_i|_\pi = 0$. Note that $y_\alpha(\pi) = 1$ implies that $|\pi| \leq n - 2^{b(n)-\alpha}$. There exists an assignment $\pi' \in A_{\alpha, \beta}$ that $\pi' \geq \pi$, $|\pi'| = |\pi| + 2^{b(n)-\alpha}$ and $x_i|_{\pi'} = 1$. Then, we have $y_\alpha(\pi') = 0$ and $y_\gamma(\pi') = y_\gamma(\pi)$ for $\gamma \neq \alpha$. By the monotonicity of h_1 , we have $h_1(\pi') = 1$. Thus, we have $1 = g(\pi') \neq I_n^i(\pi') = 0$. ■

By the duality of AND and OR, the following lemma is obtained.

Lemma 7 *Suppose G is an AND gate and G' is an OR gate. That is, $g(\tilde{x}) = h_1(\tilde{x}) \wedge (h_2(\tilde{x}) \vee y_\alpha(\tilde{x}))$. Then, $h_1(\tilde{x}) \vee y_\alpha(\tilde{x}) = 1$ over $A_{\alpha, \beta}$.* ■

From Lemma 6 and Lemma 7, we obtain the following lemma immediately.

Lemma 8 $h_2(\tilde{x}) = I_n^i(\tilde{x})$ over $A_{\alpha-1, \beta'}$, where $\beta' \in \{\beta, \beta + 2^{b(n)-\alpha}\}$.

Proof. Note that $A_{\alpha-1, \beta} = \{\pi \mid \pi \in A_{\alpha, \beta} \wedge y_\alpha(\pi) = 1\}$, and $A_{\alpha-1, \beta+2^{b(n)-\alpha}} = \{\pi \mid \pi \in A_{\alpha, \beta} \wedge y_\alpha(\pi) = 0\}$. Thus, if G is an OR gate, from Lemma 6 $h_2(\tilde{x}) = I_n^i(\tilde{x})$ on $A_{\alpha-1, \beta}$. Otherwise, if G is an AND gate, from Lemma 7, $h_2(\tilde{x}) = I_n^i(\tilde{x})$ on $A_{\alpha-1, \beta+2^{b(n)-\alpha}}$. ■

Lemma 9 *There exists a path from a gate in depth $d_{MAJ} + 1$ or $d_{MAJ} + 2$ to the i -th output gate with $2b(n) - 1$ gates, for all $1 \leq i \leq n$.*

Proof. For each $1 \leq i \leq n$, start with a path with one gate in depth $d_{MAJ} + 2b(n)$ that computes I_n^i over $A_{b(n), 0} = \{0, 1\}^n$, i.e., the i -th output gate. Such path can be extended by using Lemma 5 and Lemma 8 as follow.

For $2 \leq \alpha \leq b(n)$ and $0 \leq \beta < 2^{b(n)-\alpha}$, let G be a gate in depth $d_{MAJ} + 2\alpha$ that at the bottom of such path and computes a function g with $g(\tilde{x}) = I_n^i(\tilde{x})$ on $A_{\alpha, \beta}$. From Lemma 5, there exists a gate G' that is a predecessor of G and a successor of N_α . From Lemma 8, there exists a gate H that is a predecessor of G' other than N_α , such that H computes a function h with $h(\tilde{x}) = I_n^i(\tilde{x})$ over $A_{\alpha-1, \beta'}$, where $\beta' \in \{\beta, \beta + 2^{b(n)-\alpha}\}$. Then, we extend the path by including 2 gates, G' and H , to it. Again, from Lemma 5, H is in depth $d_{MAJ} + 2\alpha - 2$ for $\alpha \geq 3$. Otherwise, if $\alpha = 2$, i.e., in the last extension, depth of H is $d_{MAJ} + 1$ or $d_{MAJ} + 2$. That is, H has a successor in depth $d_{MAJ} + 3$ and there exists a path from N_1 to H (since $h(\tilde{x})$ is not a monotone function over x_1, \dots, x_n).

In each extension, 2 gates are included in the bottom of the path. After $b(n) - 1$ extension, a path from a gate in depth $d_{MAJ} + 1$ or $d_{MAJ} + 2$ to the i -th output gate with $2b(n) - 1$ gates are found. The gate at the bottom of such path computes a function g that $g(\tilde{x}) = I_n^i(\tilde{x})$ over $A_{1, \beta}$, where $0 \leq \beta < 2^{b(n)-1}$. ■

From this lemma, for each $1 \leq i \leq n$, we find a path from a gate in depth $d_{MAJ} + 1$ or $d_{MAJ} + 2$ to the i -output gate. Let P_i be the path to the i -th output gate, and

$G_1^i, G_2^i, \dots, G_{2^{b(n)}-1}^i$ be gates on P_i , such that G_1^i is at the bottom of P_i whose depth is $d_{\mathcal{MAJ}} + 1$ or $d_{\mathcal{MAJ}} + 2$, and for $2 \leq k < 2^{b(n)} - 1$, G_k^i whose depth is $d_{\mathcal{MAJ}} + k + 2$ is a successor of G_{k-1}^i . Thus, for $1 \leq \alpha \leq b(n)$, $G_{2^\alpha-1}^i$ is a gate that computes $I_n^i(\tilde{x})$ over $A_{\alpha,\beta}$ for some $0 \leq \beta < 2^{b(n)-\alpha}$, and for $1 \leq \alpha \leq b(n) - 1$, $G_{2^\alpha}^i$ is a gate that is a successor of $G_{2^\alpha-1}^i$ and N_α .

Lemma 10 P_1, \dots, P_n are disjoint.

Proof. Suppose P_i and P_j are sharing a gate G . Note that P_i and P_j must share G at the same position. That is, if $G = G_l^i = G_m^j$, then $l = m$. Otherwise there exists a path from N_1 to the i -th or j -th output gate with length longer than $2^{b(n)} - 1$.

Suppose $G = G_{2^\alpha-1}^i = G_{2^\alpha-1}^j$ for some $1 \leq \alpha \leq b(n)$. Let $g(\tilde{x})$ be the function that computed by G . Then, there exist an $1 \leq \alpha \leq b(n)$ and $0 \leq \beta, \beta' < 2^{b(n)-\alpha}$, $g(\tilde{x}) = I_n^i(\tilde{x})$ over $A_{\alpha,\beta}$, and $g(\tilde{x}) = I_n^j(\tilde{x})$ over $A_{\alpha,\beta'}$. It is obvious that $\beta \neq \beta'$, since there exists an assignment $\pi \in A_{\alpha,\beta}$ that $x_i|_\pi \neq x_j|_\pi$. Thus, assume without loss of generality that $\beta < \beta'$. For an assignment $\pi \in A_{\alpha,\beta}$ that $x_i|_\pi = 0$ and $x_j|_\pi = 1$. Then, we have $g(\pi) = I_n^i(\pi) = 1$. There exist an assignment $\pi' \in A_{\alpha,\beta'}$ that $\pi' \geq \pi$, i.e., $x_j|_{\pi'} \geq x_j|_\pi = 1$. Note that g is a monotone function on x_1, \dots, x_n and $y_\gamma(\tilde{x})$ for all $\gamma < \alpha$. Thus, we have $g(\pi') \geq g(\pi) = 1$. However, $1 = g(\pi') \neq I_n^j(\pi') = 0$.

Suppose $G = G_{2^\alpha}^i = G_{2^\alpha}^j$ for some $1 \leq \alpha \leq b(n) - 1$. Since N_α is a predecessor of G , the predecessor of G other than N_α is also shared by P_i and P_j , that is $G_{2^\alpha-1}^i = G_{2^\alpha-1}^j$. ■

Thus, we have the following theorem and corollary.

Theorem 11 Let $n + 1$ is a power of 2. Any depth-optimal negation-limited inverter has size at least $2n \log(n + 1) + 3n - 4$, under Assumption A.

Proof. From Lemma 9 and Lemma 10, $n(2^{b(n)} - 1) = 2n \log(n + 1) - n$ gates are found above the bottom NEGATION gate, N_1 . Below N_1 , the majority function is computed by monotone subcircuit as input of N_1 . There are at least $4(n - 1)$ gates in such a subcircuit (see [4]). ■

3 An exponential gap with the removal of one NEGATION gate

In this section, we show the relationships between the number of NEGATION gates and the size of circuits. The result of Fischer show that there is only a small gap between the size of a combinational circuit and that of a circuit which includes only $\lceil \log(n + 1) \rceil$ NEGATION gates for any boolean function. On the other hand, Tardos [11] showed that there is a monotone function F_n whose monotone and combinational circuit complexities have an exponential gap. Namely, the following proposition is shown.

Proposition 12 Let $n + 1$ be a power of two, then there exists an integer t ($0 \leq t \leq \log(n + 1) - 1$) such that $C^t(F_n)/C^{t+1}(F_n) = \exp(\Omega(n^{1/6-o(1)}))$.

Notice that in Proposition 12 we cannot determine the value of the integer t . Actually, t can range over $\log(n + 1)$ different values. Recently, Tanaka and Nishino [10] construct a function H_n and show the following Proposition, where t can range over only two different values.

Proposition 13 *Let $n+1$ be a power of two, then there exists an integer t ($\log(n+1)-2 \leq t \leq \log(n+1) - 1$) such that $C^t(H_n)/C^{t+1}(H_n) = \exp(\Omega(n^{1/6-o(1)}))$.*

In this paper we show another function K_n , which is n -input two-output, and show that the following Theorem, where t can be determined uniquely.

Theorem 14 *Let $n+1$ be a power of two, then*

$$\frac{C^{(\log(n+1)-1)}(K_n)}{C^{\log(n+1)}(K_n)} = \exp(\Omega(n^{1/6-o(1)})).$$

From the theorem above, we show that there is an optimal circuit with $\log(n+1)$ NEGATION gates, from which the removal of one NEGATION gate *must* cause an exponential growth.

Tardos pointed out that there is a polynomial time computable function F_n whose monotone circuit complexity is exponential. This function the so-called Lovász ϑ function introduced by Lovász to study the Shannon-capacity of graphs, and is known to be polynomial time computable. Tardos showed the following proposition.

Proposition 15 $C^0(F_n) = 2^{\Omega(n^{1/6-o(1)})}$.

Proposition 15 is obtained immediately from Proposition 12. Now, we define the n -input two-output function $K_n = (K_n^1, K_n^2)$ as follows:

$$K_n^1(w_1, \dots, w_{m-1}, x_1, \dots, x_{m+2}) = w_1 \oplus \dots \oplus w_{m-1} \oplus F_{m+2}(x_1, \dots, x_{m+2}), \text{ and}$$

$$K_n^2(w_1, \dots, w_{m-1}, x_1, \dots, x_{m+2}) = \neg K_n^1(w_1, \dots, w_{m-1}, x_1, \dots, x_{m+2})$$

where $n+1$ is a power of two and $m = (n-1)/2$.

Since F_{m+2} is monotone, the maximum decrease $d(K_n)$ is $m = (n-1)/2$. So, $\log(n+1) - 1$ NEGATION gates are necessary and sufficient to compute K_n by the theorem of Markov. From [3], the following lemma is easily shown.

Lemma 16 $C^{\log(n+1)}(K_n) \leq 2C(K_n) + O(n \log n)$.

Since F_{m+2} is known to be polynomial time computable, $C(K_n)$ is bounded by some polynomial in n , so is $C^{\log(n+1)}(K_n)$. This lemma can be proved by a similar argument as in [9, 3].

Lemma 17 *Let $r = \log(n+1) - 1$. Consider any r -circuit Δ which computes K_n . Label the NEGATION gates N_1, \dots, N_r in such a way that the input to N_α does not depend on the outputs of any of the NEGATION gates $N_{\alpha+1}, \dots, N_r$ (such a labeling exists since the circuit is a directed acyclic graph). Let z_α be the function computed at the input of N_α . Then $z_1 z_2 \dots z_r$ is the binary representation of $|\{w_1, \dots, w_{m-1}, F_{m+2}\}|$.*

Proof. Since $\{w_1, \dots, w_{m-1}\} \cap \{x_1, \dots, x_{m+2}\} = \emptyset$, the values of F_{m+2} can be changed independently of w_1, \dots, w_{m-1} . We can regard the value of $F_{m+2}(x_1, \dots, x_{m+2})$ as a new variable w_m which is independent of w_1, \dots, w_{m-1} . F_{m+2} is a *non-constant* monotone function over $\{x_1, \dots, x_{m+2}\}$, and Δ includes only $r = \log(n+1) - 1$ NEGATION gates, which are necessary and sufficient to compute the m -input parity function and its complement simultaneously. Thus, we obtain the lemma by a similar argument as in the proof of Lemma 5.1 in [3]. ■

Now, we obtain the following lemma, by applying Proposition 15 to a $(\log(n+1) - 1)$ -circuit computing K_n .

Lemma 18 $C^{(\log(n+1)-1)}(K_n) = \exp(\Omega(n^{1/6-o(1)}))$.

Proof. Consider the subcircuit computing z_1 in a $(\log(n+1) - 1)$ -circuit computing K_n . This subcircuit is monotone and computes the majority function over $\{w_1, \dots, w_{m-1}, F_{m+2}\}$. By fixing $(m-1)/2$ variables in $\{w_1, \dots, w_{m-1}\}$ to ones and fixing the other variables in $\{w_1, \dots, w_{m-1}\}$ to zeros, we can get the function $F_{m+2}(x_1, \dots, x_{m+2})$ at the output of the subcircuit. Combining this with Proposition 15, we have

$$C^{(\log(n+1)-1)}(K_n) \geq C^0(F_{m+2}(x_1, \dots, x_{m+2})) = 2^{\Omega(m^{1/6-o(1)})} = 2^{\Omega(n^{1/6-o(1)})}. \quad \blacksquare$$

From Lemma 16 and 18, we obtain Theorem 14.

References

- [1] M. Ajtai, J. Komlós, and E. Szemerédi. An $O(n \log n)$ sorting network. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, pages 1–9, Boston, Massachusetts, 25–27 April 1983.
- [2] N. Alon and R. B. Boppana. The monotone circuit complexity of Boolean functions. *Combinatorica*, 7(1):1–22, 1987.
- [3] Robert Beals, Tetsuro Nishino, and Keisuke Tanaka. More on the complexity of negation-limited circuits. In *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing*, pages 585–595, Las Vegas, Nevada, 29 May–1 June 1995.
- [4] Paul E. Dunne. *The Complexity of Boolean Networks*. Academic Press, London, 1988.
- [5] Michael J. Fischer. Lectures on network complexity. Technical Report YALEU/DCS/TR-1104, Department of Computer Science, Yale University, June 1974, Revised 1977, 1996. Revised April 1977, April 1996.
- [6] A. A. Markov. On the inversion complexity of a system of functions. *Journal of the ACM*, 5(4):331–334, October 1958.
- [7] Ran Raz and Avi Wigderson. Monotone circuits for matching require linear depth. *Journal of the ACM*, 39(3):736–744, July 1992.
- [8] A. A. Razborov. Lower bounds for the monotone complexity of some Boolean functions. *Soviet Math. Dokl.*, 31(2):354–357, 1985.
- [9] Keisuke Tanaka and Tetsuro Nishino. On the complexity of negation-limited Boolean networks (preliminary version). In *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing*, pages 38–47, Montréal, Québec, Canada, 23–25 May 1994.
- [10] Keisuke Tanaka and Tetsuro Nishino. A relationship between the number of negations and the circuit size. To appear in *IEICE Transactions on Information and Systems*, 1996.
- [11] É. Tardos. The gap between monotone and non-monotone circuit complexity is exponential. *Combinatorica*, 7(4):141–142, 1987.