Energy-Efficient Threshold Circuits Computing Mod Functions

Akira Suzuki Kei Uchizawa** Xiao Zhou

Graduate School of Information Sciences, Tohoku University
Aramaki-aza Aoba 6-6-05, Aoba-ku, Sendai, 980-8579, Japan.
Email: {a.suzuki, uchizawa, zhou}@ecei.tohoku.ac.jp

Abstract

We prove that the modulo function \( \text{MOD}_m \) of \( n \) variables can be computed by a threshold circuit \( C \) of energy \( e \) and size \( s = O(e(n/m)\log(n/e)) \) for every integer \( e \geq 2 \), where the energy \( e \) is defined to be the maximum number of gates outputting “1” over all inputs to \( C \), and the size \( s \) is defined to be the number of gates in \( C \). Our upper bound on the size \( s \) almost matches the known lower bound \( s = \Omega(e(n/m)^{1/e}) \).

1 Introduction

Neuronal signals play fundamental role in information processing of the brain. A neuron emitting a signal is said to be “firing.” Recent biological studies report the following fact about the energy consumption of the neuronal firing: the energy cost of a neuronal firing is high while energy supplied to the brain is limited, and hence neural networks must have low firing activity (Attwell & Laughlin, 2001; Lennie, 2003). Consequently, many neuroscientists consider that the metabolic limit must influence the way in which information is processed, and the brain has countered this metabolic constraint by adopting energy-efficient circuit designs (Földiak, 2003; Laughlin & Sejnowski, 2003; Olshausen & Field, 2004; Vinje & Gallant, 2000). Uchizawa, Douglas and Maass consider the problem posed above from the view point of theoretical computer science, and introduce a new complexity measure called the energy complexity of threshold circuits (Uchizawa et al., 2006), where a threshold circuit, is a combinatorial circuit consisting of threshold gates, and is a theoretical model of neural circuit (Minsky & Papert, 1988; Parberry, 1994; Sima & Orponen, 2003; Siu et al., 1995). Based on the biological fact above, the energy \( e \) of a threshold circuit \( C \) is defined as the maximum number of threshold gates outputting “1” over all inputs to \( C \). In previous research, several facts are known on the computational power of threshold circuits with small energy (Uchizawa et al., 2006, 2009a; Uchizawa & Takimoto, 2008; Uchizawa et al., 2009b). Particularly, Uchizawa et al. (2006) find a non-trivial circuit structure that benefits energy-efficiency, and provide threshold circuits of polynomial size and energy \( O(\log(n)) \) for a fairly large class of Boolean functions of \( n \) variables. However, their construction is not specialized for a particular task, and hence it sometimes gives a redundant circuit.

In this paper, we consider one of the fundamental and well-studied Boolean functions in the theory of circuit complexity, the modulo function, as a particular task. The modulo function \( \text{MOD}_m \) of \( n \) variables for two positive integers \( m \) and \( n \) is defined as follows: \( \text{MOD}_m(x) = 0 \) if the number of “1”s in an input \( x \in \{0,1\}^n \) is a multiple of \( m \) and, otherwise, \( \text{MOD}_m(x) = 1 \). Although the modulo function may be far from real tasks that neural networks in the brain perform, we believe that considering such a simple and fundamental task makes an important step for understanding what circuit structure benefits the energy-efficiency of threshold circuits. Uchizawa et al. (2009b) proved that size and energy of a threshold circuit computing the modulo function cannot be simultaneously small: Any threshold circuit \( C \) of energy \( e \) computing \( \text{MOD}_m \) of \( n \) variables has size

\[
\text{(1)}
\]

\[
\begin{align*}
\text{size } s &= \Omega\left( e\left(\frac{n}{m}\right)^{1/e} \right).
\end{align*}
\]

We prove in this paper that \( \text{MOD}_m \) of \( n \) variables can be computed by a threshold circuit of energy \( e \) and size

\[
\text{(2)}
\]

\[
\begin{align*}
\text{size } s &= O\left( e\left(\frac{n}{m}\right)^{1/(e-1)} \right)
\end{align*}
\]

for every integer \( e \geq 2 \). Comparing the right-hand side of Eq. (1) with one of Eq. (2), we can find the difference between the terms only in the exponent of \( n/m \). Thus, our upper bound almost matches the lower bound, and implies that there exists a tight tradeoff between size and energy of threshold circuits computing modulo function. We obtain the result by construction of the desired threshold circuits, and hence it exhibit a circuit design of energy-efficient threshold circuits.

In addition, we consider an extreme case where threshold circuits have energy \( e = 1 \). In this case, we prove that any threshold circuit \( C \) computing the\( \text{PARITY} \) of \( n \) variables must have an exponential number of gates in \( n \). On the other hand, Eq. (2) implies that \( \text{PARITY} \) (i.e., \( \text{MOD}_2 \)) can be computed by a threshold circuit of size \( s = O(n) \) and energy \( e = 2 \). Thus, we know from these facts that there exists a significant gap of computational power between threshold circuits of \( e = 1 \) and ones of \( e = 2 \).

The rest of the paper is organized as follows. In Section 2, we define some terms on threshold circuits and the modulo function. In Section 3, we first provide our main theorem. We then give a technical lemma, and prove the theorem using the lemma. In
Section 4, we prove the technical lemma given in Section 3. In Section 5, we give the lower bound for threshold circuits of energy one. In Section 6, we conclude with some remarks.

2 Preliminaries

A threshold circuit $C$ is a combinatorial circuit of threshold gates, and is expressed by a directed acyclic graph. Let $n$ be the number of input variables to $C$. Then each node of in-degree 0 in $C$ corresponds to one of the $n$ input variables $x_1, x_2, \ldots, x_n$, and the other nodes correspond to threshold gates. We define the size $s(C)$ of a threshold circuit $C$ as the number of threshold gates in $C$.

Let $g_1^C, g_2^C, \ldots, g_{s(C)}^C$ be the gates in a threshold circuit $C$. For each gate $g_i^C$, $1 \leq i \leq s(C)$, let $z(x) = (z_1(x), z_2(x), \ldots, z_k(x)) \in \{0, 1\}^k$ be the $k$ inputs of $g_i^C$ with weights $w_1, w_2, \ldots, w_k$, and a threshold $t_i$ for $x \in \{0, 1\}^n$. Then the output $g_i^C(z(x))$ of the gate $g_i^C$ is defined as follows:

$$g_i^C(z(x)) = \left( \sum_{j=1}^{k} w_j z_j(x) - t_i \right),$$

where $\text{sign}(z) = 1$ if $z \geq 0$ and $\text{sign}(z) = 0$ if $z < 0$. Simply, $g_i^C(z(x))$ is denoted by $g_i^C[x]$. Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function of $n$ variables. Let $g^C_n$ be a gate of out-degree 0 in $C$, and let the output $g^C_n[x]$ of $g_n$ be the output $C[x]$ of $C$. Thus, $C[x] = g_n^C[x]$ for every input $x \in \{0, 1\}^n$. The gate $g^C_n$ is called the top gate of $C$. A threshold circuit $C$ computes a Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ if $C(x) = f(x)$ for every input $x \in \{0, 1\}^n$.

We define the energy $e(C)$ of a threshold circuit $C$ as

$$e(C) = \max_{x \in \{0, 1\}^n} s(C) \sum_{i=1}^{s(C)} g_i^C[x].$$

Thus, the energy $e(C)$ is the maximum number of gates outputting “1” over all inputs $x \in \{0, 1\}^n$ to $C$. Trivially, we have $0 \leq e(C) \leq s(C)$.

For an input variable $x = (x_1, x_2, \ldots, x_n) \in \{0, 1\}^n$, we define $|x|$ as the hamming weight of the inputs $x$, that is,

$$|x| = \sum_{i=1}^{n} x_i.$$

Then, for an integer $m \geq 2$, the modulus function $\text{MOD}_m$ of $n$ variables is defined as follows: For every input variable $x = (x_1, x_2, \ldots, x_n) \in \{0, 1\}^n$,

$$\text{MOD}_m(x) = \begin{cases} 1 & \text{if } |x| \text{ is not a multiple of } m; \\ 0 & \text{otherwise.} \end{cases}$$

If $n \leq m - 1$, then $\text{MOD}_m(x) = 1$ for all inputs $x$ except $x = (0, 0, \ldots, 0)$. Thus, a circuit consisting of a single threshold gate with weight one for all the inputs and threshold one computes $\text{MOD}_m$. One may thus assume that $n \geq m$ in the remainder of the paper.

3 Energy-Efficient Circuits

Our main result is the following theorem that yields an energy-efficient threshold circuit computing the modulus function.

**Theorem 1.** Let $m, n$ be any two positive integers, and let $e \geq 2$ be any integer. Then there is a threshold circuit computing $\text{MOD}_m$ of $n$ variables such that its energy is at most $e$ and its size is at most

$$(e - 1) \left( \frac{n + 1}{m} \right)^{1/(e-1)} = O\left( e \left( \frac{n}{m} \right)^{1/(e-1)} \right). \quad (3)$$

Uchizawa et al. (2009b) prove that the size $s$ and energy $e$ of a threshold circuit $C$ computing $\text{MOD}_m$ of $n$ variables cannot be simultaneously small, as described in the following theorem.

**Theorem 2** (Uchizawa et al. 2009b). Let $C$ be a threshold circuit computing the function $\text{MOD}_m$ of $n$ variables. Then the size $s$ and energy $e$ of $C$ satisfy

$$\frac{n}{m} + 1 \leq \frac{1}{\sqrt{2\pi e}} \left( \frac{2c \cdot s}{e} \right)^e \quad (4)$$

where $c \approx 2.718$ is a constant.

By a simple modification of Eq. (4), we can obtain from Theorem 2 the following lower bound on the size of threshold circuits computing $\text{MOD}_m$ of $n$ variables.

**Corollary 1.** Let $C$ be any threshold circuit of energy $e$ computing $\text{MOD}_m$ of $n$ variables. Then

$$s(C) = \Omega\left( e \left( \frac{n}{m} \right)^{1/e} \right). \quad (5)$$

Observe the asymptotic terms in the right-hand side of Eqs. (3) and (5). We can find the difference between the terms only in the exponent of $n/m$: the term in Eq. (3) has $1/(e-1)$, while the term in Eq. (5) has $1/e$. Hence, the upper bound in Theorem 1 almost matches the lower bound in Corollary 1.

In the rest of the section, we prove Theorem 1. We say that a threshold circuit $C$ is regular if the inputs of every gate in $C$ includes all the inputs $x_1, x_2, \ldots, x_n$ with weight ones. In other words, every gate in $C$ receives all the unweighted inputs $x_1, x_2, \ldots, x_n$. The following technical lemma plays key role in our proof.

**Lemma 1.** Let $m, n, n'$ be positive integers such that $n \geq n' + 1$. Let $C'$ be a regular threshold circuit computing $\text{MOD}_{m'}$ of $n'$ variables. Then, there is a regular threshold circuit $C$ computing $\text{MOD}_m$ of $n$ variables such that $e(C) \leq e(C') + 1$ and

$$s(C) \leq s(C') + \frac{n + 1}{\left\lceil \frac{n + 1}{m} \right\rceil m} - 1.$$

We will prove the lemma in the next section. Using the lemma, we prove Theorem 1 below.

**Proof of Theorem 1.** Let $e$ be an arbitrary integer at least 2. We prove the theorem by constructing a regular threshold circuit $C$ computing $\text{MOD}_m$ of $n$ variables such that $e(C) \leq e$ and

$$s(C) \leq (e - 1) \left( \frac{n + 1}{m} \right)^{1/(e-1)}, \quad (6)$$

where $e \approx 2.718$ is a constant.
We provide our construction by induction on \( e \geq 2 \). That is, we construct a threshold circuit of energy \( e + 1 \) from a threshold circuit of energy \( e \). We start from the case of \( e = 2 \) as the basis.

**Basis:** \( e = 2 \).

Consider a regular threshold circuit \( C' \) consisting of a single threshold gate \( g \) with threshold \( t = 1 \) and \( m - 1 \) input variables. Clearly, \( e(C') = 1 \), \( s(C') = 1 \), and \( C' \) computes \( \text{MOD}_m \) of \( n' = m - 1 \) variables. Therefore, Lemma 1 implies that there is a regular threshold circuit \( C \) computing \( \text{MOD}_m \) of \( n \) variables such that \( e(C) \leq e(C') + 1 \) and

\[
s(C) \leq s(C') + \left( \frac{n + 1}{m} \right) - 1.
\]

Since \( e(C') = 1 \), we have \( e(C) \leq e(C') + 1 = 2 = e \). Since \( s(C') = 1 \), we have

\[
s(C) \leq s(C') + \left( \frac{n + 1}{m} \right) - 1
= \left( \frac{n + 1}{m} \right) - 1
= (e - 1) \left[ \frac{n + 1}{m} \right]^{1/(e-1)}.
\]

**Inductive Step:** \( e \geq 3 \).

By the induction hypothesis, there is a regular threshold circuit \( C' \) computing \( \text{MOD}_m \) of \( n' = m\gamma^{e-1} - 1 \) variables for each positive integer \( \gamma \) where \( e(C') \leq e \) and

\[
s(C') \leq (e - 1) \left[ \frac{n' + 1}{m} \right]^{1/(e-1)}
\leq (e - 1) \left[ \frac{(m\gamma^{e-1} - 1) + 1}{m} \right]^{1/(e-1)}
\leq (e - 1) \gamma.
\]

We will construct a regular threshold circuit \( C \) computing \( \text{MOD}_m \) of \( n \) variables, and show that \( C \) has the energy

\[
e(C) \leq e + 1
\]

and the size

\[
s(C) \leq e \left[ \frac{n + 1}{m} \right]^{1/e}.
\]

Since \( C' \) computes \( \text{MOD}_m \) of \( n' = m\gamma^{e-1} - 1 \) variables, by Lemma 1 there is a regular threshold circuit \( C \) computing \( \text{MOD}_m \) of \( n \) variables such that

\[
e(C) \leq e(C') + 1 = e + 1
\]

and

\[
s(C) \leq s(C') + \left( \frac{n + 1}{m\gamma^{e-1}} \right) - 1
= \left( \frac{n + 1}{m\gamma^{e-1}} \right) - 1.
\]

We choose

\[
\gamma = \left[ \frac{n + 1}{m} \right]^{1/e},
\]

then \( \gamma \geq (n + 1)/m \), and hence

\[
\left[ \frac{n + 1}{m\gamma^{e-1}} \right] - 1 \leq \gamma.
\]

Therefore, by Eqs. (7), (10) and (11), we have

\[
s(C) \leq s(C') + \left[ \frac{n + 1}{m\gamma^{e-1}} \right] - 1
\leq (e - 1)\gamma + \gamma
\leq e\gamma
= e \left[ \frac{n + 1}{m} \right]^{1/e}.
\]

\[\blacklozenge\]

### 4 Proof of Lemma 1

In the section, we prove Lemma 1.

Let \( m, n, n' \) be positive integers such that \( n \geq n' + 1 \). Let \( C' \) be a regular threshold circuit computing \( \text{MOD}_m \) of \( n' \) variables, and \( s = s(C') \). We denote by \( g_1, g_2, \ldots, g_s \) the threshold gates in \( C' \). One may assume without loss of generality that \( g_1, g_2, \ldots, g_s \) are topologically ordered with respect to the underlying directed acyclic graph of \( C' \), and that each gate \( g_i \), \( 1 \leq i \leq s \), receives exactly \((i - 1) + n' \) inputs from the outputs of the gates \( g_1, g_2, \ldots, g_{i-1} \) and the \( n' \) inputs \( x_1, x_2, \ldots, x_{n'} \). If there is some gate \( g_i' \), \( 1 \leq i \leq s \), such that \( g_i' \) has no input from the output of \( g_i \), then one connects input of \( g_i' \) with weight 0 for the output of \( g_i \). Therefore, for each index \( i \), \( 1 \leq i \leq s \), let \( w_{i,1}, w_{i,2}, \ldots, w_{i,i-1} \) be the weights of the gate \( g_i' \) for the outputs of the gates \( g_1, g_2, \ldots, g_{i-1} \), respectively, and denote by \( t_i \) the threshold of \( g_i \). Since \( C' \) is regular, each of the gates \( g_1, g_2, \ldots, g_s \) has weight ones for the \( n' \) input variables. Thus, the output of the gate \( g_i' \) for each input \( x' \in \{0, 1\}^{1/n} \) can be recursively computed by the following threshold function:

\[
g_i'[x'] = \begin{cases} 
\text{sign}(|x'| - t_i') & \text{if } i = 1; \\
\text{sign} \left( |x'| + \sum_{j=1}^{i-1} w_{i,j} g_j'[x'] - t_i' \right) & \text{otherwise}.
\end{cases}
\]

We show that, for any positive integer \( n \geq n' + 1 \), \( \text{MOD}_m \) of \( n \) variables can be computed by a regular threshold circuit \( C \) of energy \( e(C) \leq e(C') + 1 \) and size \( s(C) \leq s(C') + \beta \), where

\[
\beta = \left[ \frac{n + 1}{\alpha m} \right] - 1
\]

and

\[
\alpha = \left[ \frac{n' + 1}{m} \right].
\]

We construct the desired threshold circuit \( C \) from \( C' \), as described below.

To obtain \( C \), we add new input variables \( x_{n'+1}, x_{n'+2}, \ldots, x_n \) to \( C' \), and connect each of the new input variables to each of the gates \( g_1, g_2, \ldots, g_s \) with weight one. Besides, for each index \( i \), \( 1 \leq i \leq \beta \), we add a new threshold gate \( g_i \) with weight one.
for the inputs \( x_1, x_2, \ldots, x_n \) and a threshold \( \alpha m_i \) to \( C' \), and connect the output of the gate \( g_i \) to the gates \( g_i', g_2', \ldots, g_s' \) with weight \(-\alpha m_i\). For each index \( i, 1 \leq i \leq s \), we denote by \( g_i \) the gate in \( C \) that corresponds to the gate \( g_i' \) in \( C' \), and denote by \( \mathbf{x} = (x_1, x_2, \ldots, x_n) \in \{0, 1\}^n \) an input to \( C \). Then, the output of the gate \( g_i \) for an input \( \mathbf{x} \in \{0, 1\}^n \) is now represented as

\[
g_i[\mathbf{x}] = \begin{cases} 
\text{sign}\left(\left|\mathbf{x}\right| - \frac{\beta}{j=1} \alpha m_j \cdot \hat{g}_j[\mathbf{x}] - t_i'\right) & \text{if } i = 1; \\
\text{sign}\left(\left|\mathbf{x}\right| + \sum_{j=1}^{i-1} w_{ij} g_j[\mathbf{x}] - \frac{\beta}{j=1} \alpha m_j \cdot \hat{g}_j[\mathbf{x}] - t_i'\right) & \text{otherwise.}
\end{cases}
\]

Moreover, for each index \( i, 2 \leq i \leq \beta \), we connect the output of the gate \( \hat{g}_i \) to the gates \( \hat{g}_1, \hat{g}_2, \ldots, \hat{g}_{i-1} \) with weight \(-\alpha m_i\). Thus, we have

\[
\hat{g}_i[\mathbf{x}] = \begin{cases} 
\text{sign}\left(\left|\mathbf{x}\right| - \frac{\beta}{j=1} \alpha m_j \cdot \hat{g}_j[\mathbf{x}] - \alpha m_i\right) & \text{if } 1 \leq i \leq \beta - 1; \\
\text{sign}\left(\left|\mathbf{x}\right| - \alpha m_i\right) & \text{if } i = \beta.
\end{cases}
\]

for \( \mathbf{x} \in \{0, 1\}^n \). Clearly, \( C \) is a regular circuit, and

\[
s(C) \leq s(C') + \beta = s(C') + \left[\frac{n + 1}{\left\lceil \frac{n+1}{m} \right\rceil m}\right] - 1.
\]

Below we prove that \( C \) computes \( \text{MOD}_m \) of \( n \) variables, and \( e(C) \leq e(C') + 1 \).

Let \( \mathbf{x} \in \{0, 1\}^n \) be an arbitrary input to \( C \). Note that \( 0 \leq |\mathbf{x}| \) and

\[
|\mathbf{x}| \leq n \leq \alpha m \cdot \left[\frac{n + 1}{\alpha m}\right] - 1 \leq \alpha m(\beta + 1) - 1
\]

for any input \( \mathbf{x} \in \{0, 1\}^n \). Let

\[
i^* = \left\lceil \frac{|\mathbf{x}|}{\alpha m} \right\rceil,
\]

then trivially

\[
\alpha m i^* \leq |\mathbf{x}| \leq \alpha m(i^* + 1) - 1.
\]

We prove the following claim.

**Claim 1.** The following (i), (ii) and (iii) hold.

(i) \( \hat{g}_i[\mathbf{x}] = 0 \) for each \( i, i^* + 1 \leq i \leq \beta \);

(ii) \( \hat{g}_i[\mathbf{x}] = 1 \) if \( i = i^* \);

(iii) \( \hat{g}_i[\mathbf{x}] = 0 \) for each \( i, 1 \leq i \leq i^* - 1 \).

In other words, if \( 0 \leq |\mathbf{x}| \leq \alpha m - 1 \), none of \( g_1, g_2, \ldots, g_s \) outputs one; otherwise, only the gate \( \hat{g}_{i^*} \) outputs one.

**Proof of Claim.** For each index \( i, 1 \leq i \leq \beta \), let

\[
p_i(\mathbf{x}) = \begin{cases} 
|\mathbf{x}| - \frac{\beta}{j=1} \alpha m_j \cdot \hat{g}_j[\mathbf{x}] - \alpha m_i & \text{if } 1 \leq i \leq \beta - 1, \\
|\mathbf{x}| - \alpha m_i & \text{if } i = \beta.
\end{cases}
\]

Clearly, \( p_i(\mathbf{x}) \) is the value in the sign function of the right hand side of Eq. (14) for \( \mathbf{x} \in \{0, 1\}^n \), that is, \( \hat{g}_i[\mathbf{x}] = \text{sign}(p_i(\mathbf{x})) \). We evaluate \( p_i(\mathbf{x}) \), and prove (i), (ii) and (iii).

(i) \( \hat{g}_i[\mathbf{x}] = 0 \) for each \( i, i^* + 1 \leq i \leq \beta \).

If \( i \leq \beta - 1 \), then by Eqs. (15) and (16)

\[
p_i(\mathbf{x}) \leq \alpha m(i^* + 1) - 1 - \frac{\beta}{j=1} \alpha m_j \cdot \hat{g}_j[\mathbf{x}] - \alpha m_i \leq \alpha m(i^* + 1 - i) - 1 \leq -1.
\]

If \( i = \beta \), then by Eqs. (15) and (16) we similarly have

\[
p_i(\mathbf{x}) = |\mathbf{x}| - \alpha m_i \leq \alpha m(i^* + 1) - 1 - \alpha m_i \leq -1.
\]

Since \( i^* + 1 \leq \beta \), Eqs. (14), (17) and (18) imply that \( \hat{g}_i[\mathbf{x}] = \text{sign}(p_i(\mathbf{x})) = 0 \).

(ii) \( \hat{g}_i[\mathbf{x}] = 1 \) if \( i = i^* \).

In this case, we have \( 1 \leq i^* \leq \beta \). By (i) above, if \( i^* \leq \beta - 1 \),

\[
\frac{\beta}{j=1} \alpha m_j \cdot \hat{g}_j[\mathbf{x}] = 0,
\]

and hence we have by Eqs. (15) and (16)

\[
p_i(\mathbf{x}) = |\mathbf{x}| - \alpha m_i \geq \alpha m(i^* + 1) - \alpha m_i = 0.
\]

Thus Eq. (14) implies that \( \hat{g}_{i^*}[\mathbf{x}] = \text{sign}(p_i(\mathbf{x})) = 1 \).

(iii) \( \hat{g}_i[\mathbf{x}] = 0 \) for each \( i, 1 \leq i \leq i^* - 1 \).

In this case, we have \( 2 \leq i + 1 \leq i^* - 1 \), and hence

\[
\frac{\beta}{j=1} \hat{g}_j[\mathbf{x}] = 1,
\]

By (ii) above, we have \( g_{i^*}[\mathbf{x}] = 1 \), and hence

\[
- \frac{\beta}{j=1} \alpha m_j \cdot \hat{g}_j[\mathbf{x}] \leq -\alpha m i^* \cdot \hat{g}_{i^*}[\mathbf{x}] = \alpha m i^*.
\]

Since \( i + 1 \leq \beta \), we have \( i \leq \beta - 1 \). Therefore, by Eqs. (16) and (19)

\[
p_i(\mathbf{x}) \leq |\mathbf{x}| - \alpha m i^* - \alpha m_i.
\]
By Eqs. (15) and (20), we have
\[ p_i(x) \leq am(i^* + 1) - 1 - ami^* - ami \]
\[ \leq am - 1 - ami \]
\[ \leq -1 \]
and hence Eq. (14) implies that \( \hat{g}_i[x] = \text{sign}(p_i(x)) = 0. \)

We are now ready to prove the lemma by the claim. There are the following two cases to consider.

**Case 1:** \( 0 \leq |x| \leq \alpha m - 1. \)

In this case, the claim implies that none of \( \hat{g}_1, \hat{g}_2, \ldots, \hat{g}_n \) outputs one. Besides, we have

\[ \alpha m - 1 = \left\lfloor \frac{n' + 1}{m} \right\rfloor m - 1 \leq n'. \]

Therefore, Eqs. (12) and (13) imply that, for every index \( i, 1 \leq i \leq s, \) the output of \( g_i \) for \( x \in \{0,1\}^n \) equals to the output of \( g_i' \) for an input \( x' \in \{0,1\}^{n'} \) such that \( |x'| = |x| \). Thus, the number of gates outputting one is at most \( c. \) Since \( C' \) computes \( \text{MOD}_n, \)
\( C(x) \) equals to \( \text{MOD}_m(x). \)

**Case 2:** \( \alpha m \leq |x| \leq \alpha m(\beta + 1) - 1. \)

In this case, the claim implies that only the gate \( \hat{g}_i^* \) of \( \hat{g}_1, \hat{g}_2, \ldots, \hat{g}_n \) outputs one, and hence Eq. (13) implies that, for every index \( i, 1 \leq i \leq s, \) the output of \( g_i \) can be represented as

\[ g_i[x] = \text{sign}\left(|x| + \sum_{j=1}^{i-1} w_{ij} g_j[x] - '\alpha mi^* - i'\right). \]

Eq. (15) implies that

\[ 0 \leq |x| - '\alpha mi^* \leq \alpha m - 1, \]

and hence, for every index \( i, 1 \leq i \leq s, \) we have that \( g_i(x) \) for \( x \in \{0,1\}^n \) equals to the output of \( g_i' \) for an input \( x' \in \{0,1\}^{n'} \) such that \( |x' - '\alpha mi^* = |x'. \) Thus, at most \( c \) gates of the gates \( g_1, g_2, \ldots, g_s \) output one, and consequently the number of gates outputting one in \( C' \) is at most \( c + 1. \) The circuit \( C' \) computes \( \text{MOD}_m \)
\( \text{of} \ n' \text{variables, and} \ |x| - '\alpha mi^* \text{is a multiple of} \ m \text{if and only if} \ |x'| \text{is a multiple of} \ m. \text{Hence,} \ C(x) \text{equals to} \ \text{MOD}_m(x). \)

5 Circuits of Energy One

In this section, we consider an extreme case where threshold circuits have energy \( e = 1. \) While we know from Theorem 1 that \( \text{PARITY} \) (i.e., \( \text{MOD}_2 \)) of \( n \) variables can be computed by a threshold circuit of size \( s = O(n) \) and energy \( e = 2, \) we can prove that any threshold circuit of energy \( e = 1 \) computing \( \text{PARITY} \) of \( n \) variables must have an exponential number of gates in \( n, \) as follows.

**Theorem 3.** If a threshold circuit \( C \) of energy one computes \( \text{PARITY} \) of \( n \) variables, then the size \( s \) of \( C \) is at least \( 2^n - 1. \)

**Proof.** Let \( C \) be a threshold circuit of size \( s \) and energy \( e = 1 \) that computes \( \text{PARITY} \) of \( n \) variables. We denote by \( g_1, g_2, \ldots, g_s \) the threshold gates in \( C', \) and let \( g_s \) be the top gate of \( C. \) Let \( X_0 = \{ z \in \{0,1\}^n | \ |z| \text{ is even} \}, \) and \( n_0 \) be the cardinality of \( X_0. \) Clearly, \( n_0 = 2^{n-1}. \) We prove that \( s \geq n_0 = 2^{n-1} \) as follows.

For the sake of contradiction, assume that \( s \leq n_0 - 1. \) Since the top gate \( g_s \) outputs zero for any input \( z \in X_0, \) we have, for each input \( z \in X_0, \) either exactly one of \( g_1, g_2, \ldots, g_{s-1} \) outputs one or none of the gates outputs one. Since \( s \leq n_0 - 1, \) the pigeon hole principle implies that there exists a pair of inputs \( x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in X_0 \) that satisfies one of the following conditions:

(i) there exists only an index \( k, 1 \leq k \leq s - 1, \) such that the gate \( g_k \) outputs one for each of the inputs \( x \) and \( y. \)

(ii) none of the gates \( g_1, g_2, \ldots, g_s \) outputs one for each of the inputs \( x \) and \( y. \)

For each of (i) and (ii), we derive a contradiction as follows.

We next consider (i), and derive a contradiction in a similar way to (i). Let the top gate \( g_s \) have weights \( w_1, w_2, \ldots, w_n \) for the \( n \) input variables and...
a threshold \( t \). Since none of the gates outputs one for \( x \) and \( y \), we clearly have
\[
\sum_{i=1}^{n} w_i x_i - t < 0 \quad \text{and} \quad \sum_{i=1}^{n} w_i y_i - t < 0.
\]
Thus,
\[
\sum_{i=1}^{n} w_i x_i + \sum_{i=1}^{n} w_i y_i - 2t < 0. \quad (26)
\]
Let \( j \) be an index such that \( x_j \neq y_j \), then consider a pair of inputs \( x' \) and \( y' \) obtained from \( x \) and \( y \) by switching the \( j \)th components of the inputs as in Eqs (25) and (24). Clearly, \( |x'| \) and \( |y'| \) are both odd. Thus, the top gate \( q_s \) outputs one for each of \( x' \) and \( y' \), which implies that
\[
\sum_{i=1}^{n} w_i x_i - w_j x_j + w_j y_j - t \geq 0
\]
and
\[
\sum_{i=1}^{n} w_i y_i - w_j y_j + w_j x_j - t \geq 0.
\]
Thus,
\[
\sum_{i=1}^{n} w_i x_i + \sum_{i=1}^{n} w_i y_i - 2t \geq 0. \quad (27)
\]
We obtain a contradiction from Eqs. (26) and (27). Q.E.D.

Theorems 1 and 3 imply that there exists a significant gap of computational power between threshold circuits of \( e = 1 \) and ones of \( e = 2 \).

6 Conclusions

In the paper, we design energy-efficient threshold circuits computing the modulus function \( \text{MOD}_n \), and show that \( \text{MOD}_n \) of \( n \) variables can be computed by a threshold circuit of size \( s = O(e(n/m)^{1/(e-1)}) \) and energy \( e \) for any integer \( e \geq 2 \). The upper bound on the size \( s = O(e(n/m)^{1/(e-1)}) \) almost matches the known lower bound \( \Omega(e(n/m)^{1/e}) \). We also show that any threshold circuit of energy \( e = 1 \) needs at least \( 2^{n-1} \) threshold gates to compute \( \text{PARITY} \) of \( n \) variables.

A Boolean function \( f : \{0,1\}^n \rightarrow \{0,1\} \) is called symmetric if \( f(x) \) depends only on the number of 1s in \( x \) for every input \( x \in \{0,1\}^n \). Thus, the modulus function is symmetric. A generalization of the result to symmetric functions remains open.

Acknowledgments

We would like to thank Takao Nishizeki for his fruitful discussion and the referees for their helpful comments.

References


