

Better Simulation of Exponential Threshold Weights by Polynomial Weights

Kazuyuki Amano^{*†} Akira Maruoka^{*}

November 3, 2004

Abstract

We give an explicit construction of depth two threshold circuit with polynomial weights and $\tilde{O}(n^5)$ gates that computes an arbitrary threshold function. We also give the construction of such circuits with $O(n^3/\log n)$ gates computing the COMPARISON and CARRY functions, and that with $O(n^4/\log n)$ gates computing the ADDITION function. These improve the previously known constructions on its size and simplicity.

Keywords threshold circuit, constant depth, addition, comparison

1 Introduction

A linear threshold function $f(X)$ is a Boolean function with input $X = (x_1, \dots, x_n) \in \{0, 1\}^n$ such that

$$f(X) = \text{sgn}[F(X)] = \begin{cases} 1, & \text{if } F(X) \geq 0; \\ 0, & \text{otherwise,} \end{cases}$$

where

$$F(X) = w_0 + \sum_{i=1}^n w_i x_i.$$

The coefficients w_i are called the *weights* of the threshold function. It is well known that the weights of a threshold function can be restricted to integers with absolute values less than $2^{O(n \log n)}$ without changing the set of realizable functions [9] (or see [10, Theorem 3.3.9]). A gate that computes a linear threshold function is called a *threshold gate*. A *threshold circuit* is a circuit consisting entirely of threshold gates.

^{*}Graduate School of Information Sciences, Tohoku University, Aoba 6-6-05, Aramaki, Sendai 980-8579 Japan. Email: {ama|maruoka}@ecei.tohoku.ac.jp. The work was supported in part by Grant-in-Aid for Scientific Research on Priority Areas "New Horizons in Computing" from MEXT of Japan.

[†]Corresponding Author.

The relationship between the computational power of threshold circuits of small depth with exponential weights and that with polynomial weights has been widely investigated (see, e.g., [8, 11] for surveys). If one restrict the weights of the threshold gates to be integers of polynomial magnitude, then we have exponential lower bounds on the size of depth two circuits [3, 6]. However, for unrestricted weights, we have no strong lower bounds on the size of a depth two threshold circuit for an explicit function in NP.

In this paper, we develop a new and simplified simulation of a depth one threshold circuit with unbounded weights (i.e., a linear threshold function with possibly exponential weights) by a depth two threshold circuit with polynomial weights. Throughout the paper, we define the *size* of a circuit to be the number of gates in it. Goldmann, Håstad and Razborov showed in [4] that any linear threshold function can be computed by a depth two threshold circuit of polynomial size and polynomial weights. Goldmann and Karpinski [5] gave an explicit construction of such a circuit. The construction was then simplified by Hofmeister [7]. Unfortunately, the size of the constructed circuit is still quite large. (Their circuit consists of $O(n^4 \log^3 n)$ subcircuits each having $O(n^2 p^2)$ gates where p is the $O(n^3 \log n)$ -th prime number¹.) In this paper, we further simplify the construction of such a circuit. Precisely, we give an explicit construction of depth two threshold circuit with polynomial weights and $\tilde{O}(n^5)$ gates that computes an arbitrary linear threshold function. Here we use the “ \tilde{O} ” (soft O) notation, which ignores the polylogarithmic factors.

In this paper, we also give explicit constructions of depth two threshold circuits with polynomial weights that compute the “comparison” and “addition” functions. The comparison function is the Boolean function of two n -bit integers X and Y whose output is 1 iff $X > Y$. Note that the comparison function can be computed by a single threshold gate with exponential weights, but not by a gate with polynomial weights. The addition function outputs all the bits of the sum of two n -bit numbers.

Siu and Bruck [12] showed that both functions can be computed by a depth two threshold circuit with polynomial size and polynomial weights. Alon and Bruck [1] presented the constructions of such circuits. In fact, they constructed depth two circuits with a threshold gate at the top, and parity gates at the bottom. The size of their circuit for the comparison is $O(n^4)$, and that for the addition is $O(n^5)$. Since a parity gate can be replaced by $O(n)$ threshold gates with unit weights, their construction yields a depth two threshold circuit of size $O(n^5)$ for the comparison, and that of size $O(n^6)$ for the addition. Recently, we learned that Bohossian et al. [2] have presented a construction of depth two threshold circuit with $\tilde{O}(n^4)$ gates for the comparison.

In this paper, we further improve these constructions on its size and simplicity. The size of our circuit for the comparison is $O(n^3 / \log n)$ and that for the addition is $O(n^4 / \log n)$.

¹The estimation of the number of gates in their circuit described here (i.e., $\tilde{O}(n^{12})$) is larger than that described in [7] (i.e., $\tilde{O}(n^8)$). This is because we believe that we need to use $O(n^3 \log n)$ many prime numbers instead of $O(n \log n)$ primes, which was claimed in [7], if we follow their construction.

2 Construction for General Threshold Functions

For two integers $a \leq b$, $[a, b]$ denotes the set of integers $\{a, a + 1, \dots, b\}$. The set $[1, n]$ is simply denoted by $[n]$. For a set S , $\#S$ denotes the cardinality of S .

Given a linear combination $F(X) = w_0 + \sum_{i \in [n]} w_i x_i$ with $w_i \in \mathbb{Z}$ and $|w_i| \leq 2^{O(n \log n)}$. In the following, we describe the construction of depth two threshold circuit with small weights that computes the sign of $F(X)$.

Let L be the minimum integer such that $|w_i| < 2^L$ for every i . Note that $L = O(n \log n)$. Define $F^{(0)}(X) = F(X)$. For $l \in [L]$, define a linear combinations $F^{(l)}$ and $E^{(l)}$ as follows:

$$\begin{aligned} w_i^{(l)} &= \begin{cases} \lfloor w_i/2^l \rfloor, & \text{if } w_i \geq 0, \\ \lceil w_i/2^l \rceil, & \text{otherwise,} \end{cases} \\ F^{(l)}(X) &= w_0^{(l)} + \sum_{i \in [n]} w_i^{(l)} x_i, \\ E^{(l)}(X) &= F^{(l-1)}(X) - 2F^{(l)}(X). \end{aligned}$$

Note that if we represent the weight w_i by a binary sequence $s_i, w_{i,1}, \dots, w_{i,L}$ such that $w_i = (-1)^{s_i} \sum_{j \in [L]} w_{i,j} 2^{j-1}$, then $E^{(l)}$ can also be represented by

$$E^{(l)}(X) = (-1)^{s_0} w_{0,l} + \sum_{i \in [n]} (-1)^{s_i} w_{i,l} x_i. \quad (1)$$

Let $E_{max} = |\max_{l \in [L]} \max_{X \in \{0,1\}^n} E^{(l)}(X)|$. From Eq. (1), it is obvious that $E_{max} \leq n + 1$. For simplicity of presentation, we assume that $|F(X)| \geq E_{max} + 1$ for every input X . (The other case can be dealt with easily by considering a linear combination $2n(2F(X) + 1)$ instead of $F(X)$.) The construction due to Hofmeister [7] is based on the following equality:

$$F(X) \geq 0 \Leftrightarrow \bigvee_{l \in [L]} (F^{(l)}(X) \in [0, E_{max}] \wedge F^{(l-1)}(X) \notin [-E_{max}, E_{max}]).$$

The following lemma, which is the key to our construction, shows that the sign of $F(X)$ can be computed more efficiently.

Lemma 1 $F(X)$ is positive iff $F^{(l)}(X) \in [E_{max} + 1, 3E_{max}]$ for some $l \in [0, L - 1]$.

Proof. First, we show that if $F(X)$ is positive, then $F^{(l)}(X) \in [E_{max} + 1, 3E_{max}]$ for some $l \in [0, L - 1]$. Since $F^{(0)}(X) = F(X) \geq E_{max} + 1$ and $F^{(L)}(X) = 0$, it is sufficient to show that $F^{(l)}(X) > 3E_{max}$ implies $F^{(l+1)}(X) \geq E_{max} + 1$. This is clear since if $F^{(l)}(X) > 3E_{max}$, then

$$F^{(l+1)}(X) = \frac{F^{(l)}(X) - E^{(l+1)}(X)}{2} \geq \frac{3E_{max} + 1 - E_{max}}{2} > E_{max}.$$

We now show that if $F(X)$ is negative, then $F^{(l)}(X) \notin [E_{max} + 1, 3E_{max}]$ for every $l \in [0, L - 1]$. Since $F^{(0)}(X) = F(X) \leq -(E_{max} + 1)$ and $F^{(L)}(X) = 0$, it is sufficient to show that

1. If $F^{(l)}(X) \leq -(E_{max} + 1)$, then $F^{(l+1)}(X) \leq E_{max}$,
2. If $F^{(l)}(X) \in [-E_{max}, E_{max}]$, then $F^{(l+1)}(X) \in [-E_{max}, E_{max}]$.

If $F^{(l)}(X) \leq -(E_{max} + 1)$, then

$$F^{(l+1)}(X) = \frac{F^{(l)}(X) - E^{(l+1)}(X)}{2} \leq \frac{-E_{max} - 1 + E_{max}}{2} < 0,$$

which implies the first statement. For the second statement, we observe that if $|F^{(l)}(X)| \leq E_{max}$, then

$$|F^{(l+1)}(X)| = \left| \frac{F^{(l)}(X) - E^{(l+1)}(X)}{2} \right| \leq \frac{E_{max} + E_{max}}{2} = E_{max}.$$

□

The rest of the construction is similar to that of Hofmeister [7]. The following lemma is a slight modification from the lemma used in their construction. This can easily be proved by using the *Chinese Remainder Theorem*.

Lemma 2 [7, Lemma 2] *Let $a \leq b$ be two non-negative integers. Let $b < p_1 < p_2 < \dots$ be prime numbers and let s be the minimum integer which satisfies $p_1 \cdots p_s \geq 2 \cdot Z_{max} + 1$. Then for every $Z \in \mathbb{Z}$ with $|Z| \leq Z_{max}$, it holds that:*

1. $Z \in [a, b] \Rightarrow Z \bmod p_i \in [a, b]$ for all p_i ,
2. $Z \notin [a, b] \Rightarrow Z \bmod p_i \in [a, b]$ for less than $s \cdot ((b - a) + 1)$ many p_i .

□

Let $p_1 < \dots < p_r$ be r consecutive prime numbers. The value of r will be chosen later. We choose p_1 such that $3E_{max} < 4n < p_1$ in order to guarantee that no distinct integers in $[E_{max} + 1, 3E_{max}]$ can be equivalent modulo p_i for every i . Let s be the smallest integer such that $p_1 \cdots p_s > (n + 1)2^L$. Note that $s = O(n)$.

For $l \in [0, L - 1]$ and $i \in [r]$, we define a linear combination $F_i^{(l)}$ as follows:

$$F_i^{(l)}(X) = (w_0^{(l)} \bmod p_i) + \sum_{j \in [n]} (w_j^{(l)} \bmod p_i) x_j.$$

Let $\text{TEST}_{l,i}(X)$ be a Boolean function that outputs 1 iff $F_i^{(l)}(X) \bmod p_i \in [E_{max} + 1, 3E_{max}]$. By Lemmas 1 and 2, we have

$$\begin{aligned} F(X) \geq 0 &\Rightarrow \sum_{l \in [0, L-1]} \sum_{i \in [r]} \text{TEST}_{l,i}(X) \geq r, \\ F(X) < 0 &\Rightarrow \sum_{l \in [0, L-1]} \sum_{i \in [r]} \text{TEST}_{l,i}(X) \leq 2E_{max} \cdot L \cdot s. \end{aligned}$$

If we choose r such that $r > 2E_{max} \cdot L \cdot s$, e.g., $r = O(E_{max} \cdot n^2 \log n)$ will suffice, then $F(X)$ is positive if and only if the sum of the values of $rL = O(E_{max} \cdot n^3 \log^2 n)$ test functions is at least r . Since $F_i^{(l)}(X) < (n+1)p_i$ for every input X , $\text{TEST}_{l,i}(X)$ can be represented as the sum of $O(n)$ linear threshold functions

$$\sum_{k \in [0, n]} ("F_i^{(l)}(X) \geq (E_{max} + 1) + kp_i" + "F_i^{(l)}(X) \leq 3E_{max} + kp_i" - 1).$$

Here and hereafter, we use the notation of the form " $F(X) \geq a$ " that denotes the Boolean function whose value is 1 if $F(X) \geq a$ holds and is 0 otherwise. Putting them all together, we can construct a depth two threshold circuit with at most $O(nrL) = O(E_{max} \cdot n^4 \log^2 n) = \tilde{O}(n^5)$ gates that computes $f(X) = \text{sgn}[F(X)]$. Remark that the total number of wires in the resulting circuit is $\tilde{O}(n^6)$ and the weight of each wire is at most $O(np_r) = O(E_{max} \cdot n^3 \log^2 n) = \tilde{O}(n^4)$. Here we use the prime number theorem, which says that $p_r = O(r \log r)$.

3 More Economical Construction for Simple Functions

The size of the circuit constructed in the previous section is $\tilde{O}(E_{max} \cdot n^4)$, which depends on the value E_{max} of the target function. Hence, it is interesting to consider functions having small value of E_{max} , e.g., $E_{max} = O(1)$. As examples of such functions, we consider the COMPARISON and CARRY functions.

For $X = (x_n, \dots, x_1) \in \{0, 1\}^n$, we consider X as the integer $\sum_{i \in [n]} 2^{i-1} x_i$. The CARRY function is a Boolean function with two n -bit inputs X and Y that outputs 1 iff $X + Y \geq 2^n$, or equivalently $\sum_{i \in [n]} (x_i + y_i) 2^{i-1} \geq 2^n$. The COMPARISON function is a Boolean function with two n -bit inputs X and Y that outputs 1 iff $X > Y$, or equivalently $\sum_{i \in [n]} (x_i - y_i) 2^{i-1} > 0$. Since $E_{max} = O(1)$ for both functions, the construction described in the previous section yields circuits with $\tilde{O}(n^4)$ gates. We remark that the construction of a circuit for COMPARISON by Bohossian et al. [2] can be obtained in this fashion.

In the following, we show that the number of gates in circuits for these functions can be further reduced. Namely, we give explicit constructions of circuits for CARRY and COMPARISON which use only $O(n^3 / \log n)$ gates.

First, we describe a construction of a circuit for the CARRY function. Let $n < p_1 < \dots < p_r$ be r consecutive prime numbers. The value of r will be chosen later. Let s be the smallest integer such that $p_1 \cdot \dots \cdot p_s > 2^{n+1}$. Note that $s = O(n / \log n)$.

For $l \in [n]$ and $i \in [r]$, let $m_{l,i}$ be an integer satisfying

$$\sum_{j \in [l, n]} (2^{j-l} \bmod p_i) + 1 - (2^{n+1-l} \bmod p_i) = m_{l,i} p_i.$$

Such an integer always exists since $\sum_{j \in [l, n]} 2^{j-l} + 1 - 2^{n+1-l} = 0$. For $i \in [r]$ and

$l \in [n]$, let $\text{CHK}_{l,i}(X, Y)$ be a Boolean function that outputs 1 iff

$$\sum_{j \in [l, n]} (2^{j-l} \bmod p_i)(x_j + y_j) - (2^{n+1-l} \bmod p_i) = m_{l,i} p_i.$$

Below we will show that

$$\text{CARRY}(X, Y) = 1 \Rightarrow \sum_{l \in [n]} \sum_{i \in [r]} \text{CHK}_{l,i}(X, Y) \geq r, \quad (2)$$

$$\text{CARRY}(X, Y) = 0 \Rightarrow \sum_{l \in [n]} \sum_{i \in [r]} \text{CHK}_{l,i}(X, Y) \leq sn. \quad (3)$$

To show these inequalities, it is convenient to consider the following two expressions of the function CARRY:

$$\text{CARRY}(X, Y) \equiv \bigvee_{l \in [n]} \left("x_l + y_l = 2" \wedge \bigwedge_{j \in [l+1, n]} "x_j + y_j = 1" \right), \quad (4)$$

and

$$\text{CARRY}(X, Y) \equiv \bigvee_{l \in [n]} \left(" \sum_{j \in [l, n]} 2^{j-l}(x_j + y_j) = 2^{n+1-l} " \right). \quad (5)$$

The correctness of these expressions is obvious. It should be remarked that if we define $\text{EX}_l(X, Y) \equiv "x_l + y_l = 2" \wedge \bigvee_{j \in [l+1, n]} "x_j + y_j = 1"$ and $\text{SUM}_l(X, Y) \equiv \sum_{j \in [l, n]} "2^{j-l}(x_j + y_j) = 2^{n+1-l}"$, then $\text{EX}_l(X, Y) \rightarrow \text{SUM}_l(X, Y)$ for every $l \geq 1$ but $\text{SUM}_l(X, Y) \not\rightarrow \text{EX}_l(X, Y)$ for every $l \neq 1$. In fact,

$$\text{EX}_l(X, Y) \equiv \overline{\text{SUM}_1(X, Y)} \cdots \overline{\text{SUM}_{l-1}(X, Y)} \cdot \text{SUM}_l(X, Y),$$

and hence $\text{CARRY}(X, Y) \equiv \bigvee_{l \in [n]} \text{EX}_l(X, Y) \equiv \bigvee_{l \in [n]} \text{SUM}_l(X, Y)$.

Eq. (2) can be easily derived from Eq. (4) as follows:

$$\begin{aligned} \text{CARRY}(X, Y) = 1 & \\ \Rightarrow \exists l \in [n] \quad "x_l + y_l = 2" \wedge \bigwedge_{j \in [l+1, n]} "x_j + y_j = 1" & \quad (\text{From Eq. (4)}) \\ \Rightarrow \exists l \in [n] \forall i \in [r] \quad \text{CHK}_{l,i}(X, Y) = 1. & \end{aligned}$$

By using Eq. (5) instead of Eq. (4), we can derive Eq. (3) as follows:

$$\begin{aligned} \text{CARRY}(X, Y) = 0 & \\ \Rightarrow \forall l \in [n] \quad \sum_{j \in [l, n]} 2^{j-l}(x_j + y_j) - 2^{n+1-l} \neq 0 & \quad (\text{From Eq. (5)}) \end{aligned}$$

$$\begin{aligned}
&\Rightarrow \forall l \in [n] \quad \#\left\{i \in [r] \mid \sum_{j \in [l, n]} 2^{j-l}(x_j + y_j) - 2^{n+1-l} \equiv 0 \pmod{p_i}\right\} \leq s \quad (\text{By Lemma 2}) \\
&\Rightarrow \#\left\{(l, i) \in [n] \times [r] \mid \sum_{j \in [l, n]} (2^{j-l} \bmod p_i)(x_j + y_j) - (2^{n+1-l} \bmod p_i) \equiv 0 \pmod{p_i}\right\} \\
&\quad \leq sn \\
&\Rightarrow \#\left\{(l, i) \in [n] \times [r] \mid \sum_{j \in [l, n]} (2^{j-l} \bmod p_i)(x_j + y_j) - (2^{n+1-l} \bmod p_i) = m_{l,i} p_i\right\} \leq sn \\
&\Leftrightarrow \sum_{l \in [n]} \sum_{i \in [r]} \text{CHK}_{l,i}(X, Y) \leq sn.
\end{aligned}$$

If we choose r such that $r > sn$, e.g, some $r = O(n^2/\log n)$ will suffice, then $\text{CARRY}(X, Y) = 1$ if and only if the sum of the values of $rn = O(n^3/\log n)$ test functions is at least r . Since a Boolean function of the form “ $F(x) = y$ ” is equal to “ $F(x) \geq y$ ” + “ $F(x) \leq y$ ” - 1, we can construct a depth two threshold circuit of size $O(n^3/\log n)$ that computes CARRY . The total number of wires in the resulting circuit is $O(n^4/\log n)$ and the weight of each wire is at most $O(np_r) = O(n^3)$.

For the COMPARISON function, we use

$$\text{COMPARISON}(X, Y) \equiv \bigvee_{l \in [n]} \left(\text{“}x_l - y_l = 1\text{”} \wedge \bigwedge_{j \in [l+1, n]} \text{“}x_j - y_j = 0\text{”} \right)$$

instead of Eq. (4), and use

$$\text{COMPARISON}(X, Y) \equiv \bigvee_{l \in [n]} \left(\text{“} \sum_{j \in [l, n]} 2^{l-j}(x_j - y_j) = 1\text{”} \right)$$

instead of Eq. (5). The rest of the construction is analogous to that for the CARRY function. The size of the circuit is $O(n^3/\log n)$.

Finally, we sketch the construction of circuit that computes the addition of two n -bit integers based on our circuit for the carry function. For $X = (x_n, \dots, x_1)$ and $Y = (y_n, \dots, y_1)$, the $\text{ADDITION}(X, Y)$ outputs $Z = (z_{n+1}, \dots, z_1)$ such that $X + Y = Z$, or equivalently $\sum_{i \in [n]} (x_i + y_i)2^{i-1} = \sum_{i \in [n+1]} z_i 2^{i-1}$.

The k -th bit of the output of ADDITION is given by $z_k = x_k \oplus y_k \oplus c_k$ where c_k denotes the output of $\text{CARRY}(x_{k-1} \dots x_1, y_{k-1} \dots y_1)$. To compute z_k , we slightly modify the definition of our test functions for CARRY . For $t \in [0, 2]$, $l \in [k-1]$ and $i \in [r]$, let $\text{CHK}_{l,i,t}(X, Y)$ be a Boolean function that outputs 1 iff

$$\sum_{j \in [l, k-1]} (2^{j-l} \bmod p_i)(x_j + y_j) - (2^{k-l} \bmod p_i) + 4kp_i(x_k + y_k) = m_{l,i} p_i + 4kp_i t,$$

where $m_{l,i}$ is an integer satisfying

$$\sum_{j \in [l, k-1]} (2^{j-l} \bmod p_i) + 1 - (2^{k-l} \bmod p_i) = m_{l,i} p_i.$$

Note that if $x_k + y_k \neq t$, then $\text{CHK}_{l,i,t}(X, Y) = 0$ for every l and i . It is easy to check that the k -th bit of the output of ADDITION is 1 iff

$$\sum_{t \in [0,2]} \sum_{l \in [k-1]} \sum_{i \in [r]} (-1)^t \text{CHK}_{l,i,t}(X, Y) + (r + sn) "x_k + y_k = 1" \geq r.$$

Hence, each bit of the output of ADDITION can be computed by a depth two threshold circuit with polynomial weights and $O(n^3/\log n)$ gates. Thus, the total number of gates in our circuit for ADDITION is $O(n^4/\log n)$.

References

- [1] N. Alon, J. Bruck, *Explicit Constructions of Depth-2 Majority Circuits for Comparison and Addition*, SIAM J. Disc. Math. **7(1)** (1994) 1–8
- [2] V. Bohossian, M.D. Riedel and J. Bruck, *Trading Weight Size for Circuit Depth: An LT2 Circuit for Comparison*, Tech. Report of PARADISE, ETR028 (1998) (Available at <http://www.paradise.caltech.edu/~riedel/research/lt2comp.html>)
- [3] J. Forster, M. Krause, S.V. Lokam, R. Mubarakzjanov, N. Schmitt and H.U. Simon, *Relations Between Communication Complexity, Linear Arrangements, and Computational Complexity*, Proc. of 21st FSTTCS, LNCS **2245** (2001) 171–182
- [4] M. Goldmann, J. Håstad, A.A. Razborov, *Majority Gates vs. General Weighted Threshold Gates*, Computational Complexity **2** (1992) 277–300
- [5] M. Goldmann, M. Karpinski, *Simulating Threshold Circuits by Majority Circuits*, SIAM J. Comput. **27(1)** (1998) 230–246
- [6] A. Hajnal, W. Maass, P. Pudlák, M. Szegedy and G. Turán, *Threshold Circuits of Bounded Depth*, J. Comput. Syst. Sci., **46(2)** (1993) 129–154
- [7] T. Hofmeister, *A Note on the Simulation of Exponential Threshold Weights*, Proc. of the 2nd COCOON, LNCS **1090** (1996) 136–141
- [8] M. Krause and I. Wegener, *Circuit Complexity*, in “Boolean Functions Vol.II”, Eds. Y. Crama and P. Hammer (2004)
- [9] S. Muroga, *Threshold Logic and its Applications*, John Wiley, New York (1971)
- [10] I. Parberry, *Circuit Complexity and Neural Networks*, The MIT Press, London, England (1994)
- [11] A.A. Razborov, *On Small Depth Threshold Circuits*, Proc. of the 3rd SWAT, LNCS **621** (1992) 42–52
- [12] K.I. Siu and J. Bruck, *On the Power of Threshold Circuits with Small Weights*, SIAM J. Disc. Math. **4(3)** (1991) 423–435