# Simulating Threshold Circuits by Majority Circuits [1] (Revised Version)

**Mikael Goldmann**[2]

**Marek Karpinski**[3]

**TR–94–030**

**August, 1994**

**Abstract**

We prove that a single threshold gate with arbitrary weights can be simulated by an explicit polynomial-size depth 2 majority circuit. In general we show that a depth $d$ threshold circuit can be simulated uniformly by a majority circuit of depth $d+1$. Goldmann, Håstad, and Razborov showed in [10] that a non-uniform simulation exists. Our construction answers two open questions posed in [10]: we give an explicit construction whereas [10] uses a randomized existence argument, and we show that such a simulation is possible even if the depth $d$ grows with the number of variables $n$ (the simulation in [10] gives polynomial-size circuits only when $d$ is constant).

[1] A preliminary version of this paper appeared in Proc. 25th ACM STOC (1993), pp. 551–560.

[2] Laboratory for Computer Science, MIT, Cambridge MA 02139, Email: `migo@theory.lcs.mit.edu`. This author's work was done at Royal Institute of Technology in Stockholm, and while visiting the University of Bonn

[3] Department of Computer Science, University of Bonn, 53117 Bonn, and International Computer Science Institute, Berkeley, California, Email: `marek@cs.bonn.edu`. Supported in part by Leibniz Center for Research in Computer Science, by the DFG Grant KA 673/4–1, and by the ESPRIT BR Grant 7097 and ECUS030.

# 1 Introduction

A threshold gate is a fairly simple device that computes a weighted sum of its input and compares it to a threshold value and outputs 1 or 0 depending on the outcome of the comparison. A threshold circuit is an acyclic network of threshold gates. The *size* of a circuit is the number of wires.

Small weight threshold gates are a restricted type of threshold gates. In this case the magnitude of the (integer) weights of the gate is polynomially bounded. The corresponding circuits are called small depth threshold circuits. It is easy to see that a majority gate can simulate a small weight threshold gate by simply duplicating input wires and adding some constant inputs. This only leads to a polynomial increase in the number of wires. Hence, depth $d$ polynomial-size majority circuits are equivalent to depth $d$ polynomial-size, small weight threshold circuits.

Threshold circuits have been shown to be surprisingly powerful. It is implicit in work by Beame, Cook, and Hoover [4] that integer division can be carried out by polynomial-size threshold circuits of constant depth. Allender [1] (inspired by Toda [28]) shows that any function in $\mathrm{AC}^0$ can be computed by depth 3 majority circuits of quasi-polynomial size. Yao [33] extends this to all of $\mathrm{ACC}^0$ (see also [5]).

There are some strong lower bounds for majority circuits of very small depth. Hajnal et al. [11] prove exponetial lower bounds on the size of depth 2 majority circuits computing "inner product mod 2." These results were extended in [13] to depth 3 majority circuits where the gates on the bottom level have very small fanin, and recently super-polynomial bounds were proved for depth 3 majority circuits where the gates on the bottom level are arbitrary gates of fan-in $n^{1-\epsilon}$ [22]. For depth 3 majority circuits with no extra restrictions, no super-polynomial lower bounds are known. Siu, Roychowdhury, and Kailath proved super-linear lower bounds on the number of wires in constant-depth majority circuits computing parity [27]. Recently Impagliazzo, Paturi, and Saks extended the results of [27] to constant-depth threshold circuits (with large weights) computing parity [15].

If one considers threshold circuits with arbitrary weights, even less is known. There is no super-polynomial lower bound for depth 2 threshold circuits computing some function in NP. As we mentioned above, such bounds exist for majority circuits [11]. It is therefore interesting to explore the power of large weights in threshold circuits.

It is well known that a single threshold gate is strictly more powerful than a single small-weight threshold gate. Also, it was recently shown that depth 2, polynomial-

size threshold circuits are more powerful than depth 2, polynomial-size, small-weight threshold circuits [10].

On the other hand, it was proved by Chandra, Stockmeyer, and Vishkin [8] that addition of $n$ binary encoded integers can be performed by constant depth majority circuits (see also [20]). This implies that depth $d$, polynomial-size threshold circuits can be simulated by depth $O(d)$, polynomial-size, small-weight threshold circuits.

In [24] Siu and Bruck gave a non-constructive proof that depth $d$ threshold circuits can be simulated by depth $2d+1$ majority circuits. Alon and Bruck gave a uniform construction in [3] achieving this. Goldmann, Håstad, and Razborov showed in [10] that any function computed by a depth $d$, polynomial-size threshold circuit is computable by a depth $d+1$, polynomial-size majority circuit (note that for $d = 1, 2$ this is optimal). Two open questions were posed in [10]: Can one make an explicit construction, and can one make it work also for non-constant depth? ([10] uses a probablilistic argument, and the blowup in size is super-polynomial if the depth grows with the number of variables.) We give positive answers to both questions.

For a thourough survey of complexity theoretic results on threshold circuits, see [21]

# 2 Preliminaries

It will be convenient to work over $\{1, -1\}$ rather than $\{0, 1\}$. An $n$-variable Boolean function thus maps $\{1, -1\}^n$ to $\{1, -1\}$. This is a simple transformation, and does not affect the power of threshold gates. A threshold gate computes its output as the sign of a linear form:

$$g(x) = sign\left(w_0 + \sum_{i=1}^{n} w_i x_i\right),$$

where the $w_i$ are the *weights*. We assume that the argument to the sign function is nonzero for all $x \in \{1, -1\}^n$. The following well known result by Muroga [16] gives a bound on the magnitude of the weights.

**Theorem 1 ([16, Theorem 9.3.2.1])** *Let $f(x)$ be an arbitrary $n$-variable threshold function. Then $f(x)$ can be written as*

$$f(x) = sign\left(w_0 + \sum_1^n w_i x_i\right),$$

*where for all $i = 0, \ldots, n$,*

$$w_i \in \mathbb{Z} \quad \text{and} \quad |w_i| \leq 2^{-n}(n+1)^{(n+1)/2}.$$

**Remark 1** *A recent result by Håstad [12] gives a lower bound on the weights required for a particular threshold function. The lower bound nearly matches the upper bound in Theorem 1.*

A threshold circuit is a directed acyclic graph the nodes of which are either threshold gates or input variables. We allow multiple output nodes, and a circuit is evaluated in topological order. For a given circuit $C$, $f_C$ is the function computed by $C$. The size of a circuit is the number of wires.

A family of circuits $\{C_n\}$ is said to compute a function $f\colon \{1,-1\}^* \to \{1,-1\}^*$ provided $f \restriction_{\{1,-1\}^n} = f_{C_n}$ for all $n$.

**Definition 1** *We use the following notation from [6].*

- *$LT_d$ is the class of functions computable by depth $d$ polynomial-size threshold circuits.*
- *$\widehat{LT}_d$ is the class of functions computable by depth $d$ polynomial-size threshold circuits with polynomially bounded integer weights.*

Note that if we allow a gate to have multiple wires from an input (i.e., the underlying structure is a *multi*-graph), then depth $d$, polynomial-size majority circuits can compute any function in $\widehat{\mathrm{LT}}_d$.

We introduce also uniform classes of threshold circuits. In doing so we can use the threshold circuit descriptions, e.g. similar to the "Direct Connection Language" of Ruzzo [23] (see also [9]).

Let $BIN$ be the set of binary encodings of the positive integers. A threshold circuit $C_n$ with $n$ inputs is described by an edge-labeled multi-graph $(V_n, E_n)$. $V_n = I_n \dot{\cup} G_n$, where $I_n = \{1, x_1, \ldots, x_n\}$ is the set of inputs (note that the constant "1" is included in $I_n$), and $G_n = \{g_1, \ldots, g_s\}$ is the set of gates. The edges in $E_n$ are tuples $(v, g, e, k, s) \in V_n \times G_n \times BIN \times BIN \times \{1, -1\}$ with the following interpretation: the edge goes from $v$ to $g$, $e$ is the index among the $(v, g)$-edges (i.e., it's the $e$th edge from $v$ to $g$), and the weight of the edge is $s \cdot 2^k$. There is no need to assign a threshold value to the gates in $G_n$. We give them all threshold 0 and by having an appropriate weight assigned to the constant input 1 any threshold can be achieved. Also, an edge with weight $w$ can be split into about $\log w$ edges the weights of which are powers of 2. We use $\overline{C_n}$ to denote the description of $C_n$.[4]

To define uniformity, let $\mathcal{C} = \{C_n\}$ be a sequence of circuits, and for each $C_n$ let $G_n$ and $E_n$ be the corresponding gates and edges. $\mathcal{C}$ defines the language $L_{\mathcal{C}} = L_G \cup L_E$, where $L_G = \{\, (n, g) \mid g \in G_n \,\}$ and $L_E = \{\, (n, v, g, e, k, s) \mid (v, g, e, k, s) \in E_n \,\}$.

**Definition 2** *A function is in $L$–uniform $LT_d$ if there is a sequence $\mathcal{C}$ of depth $d$ threshold circuits with polynomial-size descriptions, such that there is a Turing machine that accpets $L_{\mathcal{C}}$ in linear space.*

*A function is in $L$–uniform $\widehat{LT}_d$ if there is a sequence $\mathcal{C}$ of depth $d$ small-weight threshold circuits with polynomial-size descriptions, such that there Turing machine that accpets $L_{\mathcal{C}}$ in linear space.*

The reason for the terminology "$L$–uniform" is that the description of a circuit of the above type can be generated in space that is logarithmic in the size of the description.

We call a sequence of circuits $P$–uniform if the description of the $n$th circuit can be generated in polynomial time on input $1^n$ (cf., e.g. [9]).

We define the following operator.

**Definition 3** *The operator* rem *is defined as follows. For integers $a$ and $b$,*

$$a \ rem \ b = c,$$

[4]The case of majority circuits is when the weights are only allowed to be 1 or $-1$. We then drop $k$ from the edges and the weight of an edge is simply $s$.

*where $c$ is the unique integer such that*

$$a \equiv c \pmod{b} \quad \textit{and} \quad -b/2 < c \leq b/2.$$

Our construction uses the following function of one integer variable $y$.

$$\begin{aligned} M_j^{m,p}(y) &= \frac{1}{2}\,sign\left(y + jp - m + \frac{1}{2}\right) \\ &\quad -\frac{1}{2}\,sign\left(y + jp - 2m + \frac{1}{2}\right) \\ &\quad +\frac{1}{2}\,sign\left(y + jp + m - \frac{1}{2}\right) \\ &\quad -\frac{1}{2}\,sign\left(y + jp + 2m - \frac{1}{2}\right) \end{aligned}$$

The function $M_j^{m,p}(y)$ has some nice properties.

**Lemma 2** *If $p > 4m$ then for any integers $y$ and $j$ the following is true.*

*If $y + jp = y \text{ rem } p$ and $m \leq |y \text{ rem } p| < 2m$, then $M_j^{m,p}(y) = sign\,(y \text{ rem } p)$. In all other cases $M_j^{m,p}(y) = 0$.*

PROOF. Assume that $y + jp = y \text{ rem } p$. It is easy to see that the first two terms contribute 1 if $m \leq y + jp < 2m$ and 0 otherwise. Similarly, the last two terms contribute $-1$ if $-2m < y + jp \leq -m$ and 0 otherwise. Thus, we have $M_j^{m,p}(y) = sign\,(y - jp)$ when $m \leq |y - jp| < 2m$ and $M_j^{m,p}(y) = 0$ otherwise.

When $y + jp \neq y \text{ rem } p$ then $|y - jp| \geq 2m$, and thus $M_j^{m,p}(y) = 0$. $\square$

# 3 The Idea Behind the Construction

Let $f$ be an arbitrary threshold gate given by

$$f(x) = sign\,(F(x)),$$

where

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

Since we have integer weights, and we require that the argument of '$sign$' is nonzero, we have $|F(x)| \geq 1$ for all $x$.

In the next section we will build a parametrized *approximator* for $f$. For a fix input, the approximator is good for randomly chosen parameters. To show the intuition behind the construction, we build an approximator $\varphi$ for $f$ that computes correctly for a random input.

In the construction it will be convenient to use rational weights. Any circuit we construct will have weights of the form $w/2$, where $w$ is an integer. By multiplying all weights in the circuit by 2 we get integer weights, and the increase in the magnitude of the weights is just a factor 2.

To describe the construction we need a couple of parameters that we call $W$ and $m$. It will be convenient to assume the following:

$$W \geq \max\{w_{max}(f), 2^n\}, \tag{1}$$

$$10n \leq m \leq W. \tag{2}$$

The parameter $m$ controls how good the approximator is. If $m$ is big, then the approximator is good, but the weights in the approximator are polynomial in $m$.

Let us look at a fixed input $x$. Assume that $2^l \leq |F(x)| < 2^{l+1}$. Given this information, we can use less precision in the weights $w_i$. Set

$$F_{(l)}(x) = \lfloor w_0 m/2^l \rfloor + \sum_{i=1}^{n} \lfloor w_i m/2^l \rfloor x_i.$$

If we disregard the error introduced by the floor operation, we will have

$$m \leq |F_{(l)}(x)| < 2m.$$

It is plausible that for most values of $F(x)$, the truncation error will not matter. Note that $sign\,(F(x)) = sign\left(F_{(l)}(x)\right)$. To get the weights small, we just look at $F_{(l)}(x)$ modulo some small prime $p > m^2$.

We are now ready to construct a small gadget $\varphi^{(l)}(x)$ that implements the computation described above.

$$\begin{aligned} w_i^{(l)} &= \lfloor w_i m/2^l \rfloor \ rem\ p, \\ \Phi_{(l)}(x) &= w_0^{(l)} + \sum_{i=1}^{n} w_i^{(l)} x_i, \\ \varphi_{(l)}(x) &= \sum_{j=-n-1}^{n+1} M_j^{m,p}\left(\Phi_{(l)}(x)\right). \end{aligned} \tag{3}$$

Let us establish some properties of $\varphi_{(l)}$ as defined by (3).

**Proposition 3** *For $p > m^2$ the following holds.*

1. *For any $x$, $\left|\varphi_{(l)}(x)\right| \in \{0,1\}$.*
2. *If $\left|F_{(l)}(x) \text{ rem } p\right| \notin [m, 2m)$ then $\varphi_{(l)}(x) = 0$.*
3. *If $m \leq \left|F_{(l)}(x)\right| < 2m$ then $\varphi_{(l)}(x) = sign\left(F_{(l)}(x)\right)$.*

PROOF. All statments follow from Lemma 2. The first one is immediate. The second follows by the observation that $F_{(l)}(x) \equiv \Phi_{(l)}(x) \pmod p$.

For the third statement we have the following. Assume that $m \leq \left|F_{(l)}(x)\right| < 2m$. We then have

$$\Phi_{(l)}(x) \text{ rem } p = F_{(l)}(x).$$

Let $j_0$ be the integer that satisfies

$$\Phi_{(l)}(x) \text{ rem } p = \Phi_{(l)}(x) + j_0 p.$$

Since $\left|\Phi_{(l)}(x)\right| \leq (n+1)(p-1)/2$, $j_0$ occurs in the sum in (3). The third statement now follows from Lemma 2. $\square$

It is tempting to set

$$\varphi(x) = \sum_l \varphi_{(l)}(x), \tag{4}$$

and hope that $\varphi(x) = sign\,(F(x)) = f(x)$. The idea is that there is always an $l$ such that $2^l \leq |F(x)| < 2^{l+1}$. If there was no error introduced by the floor operations, we would have $m \leq \left|F_{(l)}(x)\right| < 2m$ and $sign\left(F_{(l)}(x)\right) = sign\,(F(x))$. By Proposition 3, $\varphi_{(l)}(x) = sign\left(F_{(l)}(x)\right)$ and for all other $l$ we would probably have $\varphi_{(l)}(x) = 0$. Then we would have $\varphi(x) = \varphi_{(l)}(x) = sign\,(F(x)) = f(x)$.

**Remark 2** *We know that $|F(x)| \leq (n+1)W$. Thus, it is sufficient to sum over $l$ such that $0 \leq l \leq \log((n+1)W)$ in (4).*

The problems with (4) are of course that the floor operation sometimes introduces *truncation errors* (e.g., when $2^l \leq F(x)$ but $F_{(l)}(x) < m$), and sometimes the "wrong" $l$ gives a nonzero contribution to the sum (a *modular error*).

Equation (4) is not such a bad idea though, because it works for most $x$, or rather, for most values of $F(x)$.

# 4 The Approximator

To get an approximator based on the ideas in the previous section we want to spread the value $F(x)$ in some random fashion. This was done in [10] by considering $sign\,(\alpha F(x))$ for a randomly chosen integer $\alpha \in \{1, 2, \ldots, 2^{2n}\}$. Since $\alpha > 0$ one has $sign\,(F(x)) = sign\,(\alpha F(x))$. It was shown that for any $x$, the approximator would compute $sign\,(\alpha F(x))$ correctly with high probability. By taking many independent $\alpha$'s and taking the sign of the average, one gets an approximator that behaves well on all inputs. If the range of $\alpha$ was smaller, we could get an explicit approximator by taking the average over all $\alpha$'s.

We will modify the construction. Our approximator will depend on two parameters, and for any input, the approximator will be good with high probability if the parameters are chosen at random. In our case the probability space is small enough that we may take the average over all possible choices of parameter values.

We will modify the construction. Just like in [10] we will use a multiplier $\alpha$, but it will be much smaller. For a random $\alpha$, the probability of a truncation error is small. To handle the modular errors, we will also choose the prime $p$, used in the construction, randomly, and the probability that we get a modular error for a random $p$ is small.

**Definition 4** *We define the following sets. Let*

$$\begin{aligned} [m] &= \{1, 2, \ldots, m\}, \\ \mathcal{P}R^m &\text{ is the set of the first } m^2 \text{ primes} \\ &\text{that are greater than } m^2. \end{aligned}$$

*When $\alpha$ and $p$ are chosen randomly, they are picked as a pair $(\alpha, p) \in [m] \times \mathcal{P}R^m$ according to the uniform distribution.*

Instead of looking at the weights $w_i$, we make the approximator for weights $\alpha w_i$. Thus, instead of looking at $F(x)$ we look at $\alpha F(x)$ but this works since $sign\,(\alpha F(x)) = sign\,(F(x)) = f(x)$. We call the corresponding truncated linear form $F^{\alpha}_{(l)}(x)$, that is

$$F^{\alpha}_{(l)}(x) = \lfloor \alpha w_0 m/2^l \rfloor + \sum_{i=1}^{n} \lfloor \alpha w_i m/2^l \rfloor x_i.$$

Now we are ready to define the parametrized approximator $\varphi^{\alpha,p}(x)$.

$$\begin{aligned}
w_i^{(l)} &= \left\lfloor \alpha w_i m/2^l \right\rfloor \; rem\; p \\
\Phi^{\alpha,p}_{(l)}(x) &= w_0^{(l)} + \sum_{i=1}^{n} w_i^{(l)} x_i \\
\varphi^{\alpha,p}_{(l)}(x) &= \sum_{j=-n-1}^{n+1} M_j^{m,p}(\Phi^{\alpha,p}_{(l)}(x)) \\
\varphi^{\alpha,p}(x) &= \sum_{l=0}^{\lfloor 3\log W \rfloor + 1} \varphi^{\alpha,p}_{(l)}(x), \qquad (5)
\end{aligned}$$

where the upper bound of the last summation follows from an argument analogous to Remark 2, the assumptions (1) and (2), and the fact that $\alpha \leq m$.

The following proposition is the $(\alpha, p)$-version of Proposition 3. The proof is completely analogous.

**Proposition 4** *For $p > m^2$ the following holds.*

1. *For any $x$, $\left|\varphi^{\alpha,p}_{(l)}(x)\right| \in \{0,1\}$.*
2. *If $\left|F^{\alpha}_{(l)}(x) \; rem\; p\right| \notin [m, 2m)$ then $\varphi^{\alpha,p}_{(l)}(x) = 0$.*
3. *If $m \leq \left|F^{\alpha}_{(l)}(x)\right| < 2m$ then $\varphi^{\alpha,p}_{(l)}(x) = sign\left(F^{\alpha}_{(l)}(x)\right)$.*

**Corollary 5** *If we assume (1) and (2), then for all $x \in \mathbb{Z}^n$ we have $\varphi^{\alpha,p}(x) \in \mathbb{Z}$ and $|\varphi^{\alpha,p}(x)| \leq 2 + 3\log W$.*

PROOF. It is not hard to see that statement 1 of Proposition 4 holds even for $x \in \mathbb{Z}^n$. The corollary follows since we sum over at most $2 + 3\log W$ different $l$ in (5). $\square$

For any $x$ there are usually $\alpha$'s and $p$'s such that we get truncation errors or modular errors. We will show that for any fixed $x$ most pairs $(\alpha, p)$ do not give such errors.

**Definition 5**

1. *We say that $\alpha$ is* bad *for $x$ if there is some $l$ such that $\left||\alpha F(x)| - 2^l\right| \leq 2^{l+1} n/m$. Otherwise $\alpha$ is* good *for $x$.*
2. *We say that $p$ is* bad *for $x$ and $\alpha$ if there is an $l$ such that $\left|F^{\alpha}_{(l)}(x)\right| \geq 2m$ but $\left|F^{\alpha}_{(l)}(x) \text{ rem } p\right| < 2m$. Otherwise $p$ is* good *for $x$ and $\alpha$.*
3. *We call a pair $(\alpha, p)$* bad *for $x$ if $\alpha$ is bad for $x$, or if $p$ is bad for $x$ and $\alpha$. Otherwise $(\alpha, p)$ is* good *for $x$.*

We will show that when a pair $(\alpha, p)$ is good for $x$, then $\varphi^{\alpha,p}(x) = f(x)$. We will also show that a for any fixed $x$, a random pair $(\alpha, p)$ is likely to be good.

First we show that $\varphi^{\alpha,p}(x) = f(x)$ when $(\alpha, p)$ is good.

**Proposition 6** *Let $x$ be an arbitrary fixed input. The following is true. if $(\alpha, p)$ is good for $x$, then $\varphi^{\alpha,p}(x) = f(x)$.*

PROOF (SKETCH). If $(\alpha, p)$ is good for $x$ then, by the definition of "good," there will not be any truncation errors or modular errors. Thus, the only contribution we get in (5) is the contribution from the "right" $l$, which is $sign\,(\alpha F(x))$. $\square$

We will show that for any fixed $x$ most $\alpha$'s are good, and for any fixed $x$ and $\alpha$ most $p$'s are good.

**Lemma 7** *If $W$ and $m$ satisfy (1) and (2), then for any $x$*

$$\Pr\left[\alpha \text{ is bad for } x\right] < (16 \log^2 W)/m.$$

PROOF. Let $r = |F(x)|$. We want to show that for most $\alpha$ we have $\left|2^l - \alpha r\right| > 2^{l+1}n/m$ for all $l$.

Look at a fixed $l$, if there is any $\alpha$ which is bad with respect to $l$, then $r$ must satisfy the following equations.

$$r < 2^{l+1}, \tag{6}$$
$$r > 2^{l-1}/m. \tag{7}$$

The bad interval for $\alpha$ has length $2^{l+2}n/(rm)$. If $r$ and $l$ do not satisfy (7), then all $\alpha$'s are too small to be bad. On the other hand, if $r$ and $l$ satisfy (7), there are at most $8n$ different $\alpha$'s that fit in the bad interval.

For any $r$, there are less than $2\log m$ different $l$ that satisfy (6) and (7). Thus, any $x$ has at most $16n\log m$ bad $\alpha$. The lemma follows by our assumption that (1) and (2) hold. □

**Lemma 8** *If $W$ and $m$ satisfy (1) and (2), then for any $x$ and $\alpha$*

$$\Pr\left[p \text{ is bad for } x \text{ and } \alpha\right] < (16\log^2 W)/m.$$

PROOF. Once again consider a fixed $l$ first, and assume that for input $x$ and multiplier $\alpha$ we have $|F^{\alpha}_{(l)}(x)| \geq 2m$ but $\left|F^{\alpha}_{(l)}(x) \text{ rem } p\right| < 2m$ for $4m\log W$ of the primes. By the pigeon hole principle we must have more than $\log W$ primes that give the same remainder $k$, such that $|k| < 2m$. By the Chinese remainder theorem, $F^{\alpha}_{(l)}(x)$ is uniquely determined modulo the product of those primes. That product is greater than $m^{2\log W}$. Since we assume (1) and (2),

$$\begin{aligned}\left|F^{\alpha}_{(l)}(x)\right| &\leq |m\alpha F(x)| \\ &\leq m^2(n+1)W \\ &\ll m^{2\log W}.\end{aligned}$$

This implies that $k = F^{\alpha}_{(l)}(x)$ which means that $\left|F^{\alpha}_{(l)}(x)\right| < 2m$, and we have a contradiction. Since there are at most $2 + 3\log W < 4\log W$ different $l$, the lemma follows. □

Lemma 7 and Lemma 8 imply the following lemma.

**Lemma 9** *If $W$ and $m$ satisfy (1) and (2), then for an arbitrary fixed input $x$,*

$$\Pr\left[(\alpha, p) \text{ is bad for } x\right] \leq (32 \log^2 W)/m.$$

We conclude this section by showing how the approximator allows us to simulate a single threshold gate (with large weights) by a depth 2, small-weight, threshold circuit. This is a constructive version of Theorem 7.8 from [10].

**Theorem 10** $LT_1 \subsetneq \widehat{LT}_2$.

PROOF. We will prove the inclusion. That it is strict follows from the fact that parity is in $\widehat{\mathrm{LT}}_2 \setminus \mathrm{LT}_1$. Assume $n \geq 100$, smaller inputs are handled by writing the function on disjuntive normal form.

We are given a threshold gate

$$f(x) = sign\left(w_0 + \sum_{i=1}^{n} w_i x_i\right).$$

Let $W = \max\{w_{max}(f), 2^n\}$ be the bound used in the construction, and set the parameter $m = 128 \log^3 W$ (observe that $W$ and $m$ satisfy (1) and (2)). Consider the following function:

$$g(x) = sign\left(\sum_{(\alpha,p)} \varphi^{\alpha,p}(x)\right).$$

We claim two things: $f(x) = g(x)$ for all $x \in \{1, -1\}^n$, and $g(x)$ can be computed by a depth 2, polynomial-size, threshold circuit with polynomially bounded weights.

The correctness of the construction follows from

$$\mathrm{E}\left[f(x)\varphi^{\alpha,p}(x)\right] > 0, \tag{8}$$

where $x$ is arbitrary and fixed, and we take expectation over the uniform distribution on pairs $(\alpha, p)$. Let us prove (8).

$$\begin{aligned}
&\mathrm{E}\left[f(x)\varphi^{\alpha,p}(x)\right] \\
&\quad \geq \Pr\left[(\alpha,p) \text{ good}\right] \\
&\qquad -(2 + 3\log W)\Pr\left[(\alpha,p) \text{ bad}\right] \\
&\quad \geq 1 - \frac{1}{4\log W} - \frac{2 + 3\log W}{4\log W} \\
&\quad > 0,
\end{aligned}$$

where the first inequality follows from Corollary 5 and the second inequality follows from Lemma 9. This shows that $f(x) = g(x)$ for all $x$.

Now, to implement $g(x)$ as a circuit, let us look at a very schematic picture of what $g(x)$ does.

$$g(x) = sign\left(\sum_{\alpha,p,l,j} \frac{1}{2} sign\left(F^{(l)}_{(\alpha,p)}(x)\cdots\right)\cdots\right).$$

Since we only have two levels of $sign$-functions, and one is the outmost operator, $g(x)$ can be computed by a depth 2 threshold circuit. The size is the total number of terms in the summations (recall that each $F^{(l)}_{(\alpha,p)}(x)$ has fan-in $n \leq \log W$). There are $m^3 = O\left(\log^9 W\right)$ pairs $(\alpha, p)$, and $O(\log W)$ different $l$. This gives a total size of $O(\log^{12} W)$.

As for the weights, they are not necessarily integers, but if we multiply them by two they are. The only weights that are not $\pm 1$ are the $w_1^{(l)}, \ldots, w_n^{(l)}$ and $w_0^{(l)} + jp$ weights. All the $w_i^{(l)}$ are reduced modulo some prime $p$ that is among the first $2m^2 = O(\log^6 W)$ primes. This implies that $p \leq O(\log^7 W)$. Since $-(n+1) \leq j \leq n+1$, the weights are all of magnitude $O(\log^8 W)$.

If we assume Muroga's bound on weights to hold for the original threshold gate $f$, then $\log W \leq O(n \log n)$, and hence we have a polynomial-size, polynomial-weight threshold circuit of depth 2 that computes $f(x)$. Actually, we only need to have $\log W$ polynomial in $n$. $\square$

# 5 Extending the Construction to Circuits

In the previous section we showed that a single threshold gate can be simulated by a polynomial-size majority circuit. We will now generalize this to show that a depth $d$, polynomial-size, threshold circuit can be simulated by a depth $d+1$, polynomial-size, majority circuit.

In [10] Goldmann, Håstad, and Razborov introduced a circuit class that mixes small and large weights.

**Definition 6** *$\widetilde{LT}_d$ is the class of functions computable by depth $d$, polynomial-size, circuits where the top gate has polynomially bounded weights.*

We will show the following theorem.

**Theorem 11** *For any depth $d$, possibly depending on $n$, $\widetilde{LT}_d = \widehat{LT}_d$.*

*Moreover, given a $\widetilde{LT}_d$ circuit, for input size $n$, with weights bounded by $2^{p(n)}$ for some polynomial $p$, there is an explicit $\widehat{LT}_d$ circuit that computes the same function.*

PROOF. Let us look at a circuit $C$ for an $\widetilde{\mathrm{LT}}_d$-function. For simplicity, assume that the weights at the top gate are all 1. Let the top gate be given by

$$g(x) = sign\left(\sum_{i=1}^{t} C_i(x)\right),$$

where the $C_i$ are depth $d-1$ threshold circuits. Let $s$ be the size of $C$. For each circuit $C_i$ we construct an approximator $\Gamma_k^{\alpha,p}$. Below we describe how this is done.

Let $W = \max\{w_{max}(C), 2^s\}$. Let $C_k$ be one of the subcircuits of $g$. Let the gates of $C_k$ be $f_1, \ldots, f_r$, where $r \leq s$. The fan-in of any $f_i$ is trivially bounded by $\log W$, and all gates have their weights bounded by $W$. Set the parameter $m$ of the previous section as follows.

$$m = 256 s\, t \log^3 W.$$

For $(\alpha, p) \in [m] \times \mathcal{P}R^m$, construct a gate approximator $\varphi_i^{\alpha,p}$ for each gate $f_i$. Now, connect the approximators in the same way as the gates. That is, if the output of $f_i$ is the $k$'th input to $f_j$, then the output of $\varphi_i^{\alpha,p}$ is the $k$'th input to $\varphi_j^{\alpha,p}$. We call the constructed "circuit" $\Gamma_k^{\alpha,p}$. Note that for any fixed input $x$, if $(\alpha, p)$ is simultaneously good for all $\varphi_i^{\alpha,p}$ of $\Gamma_k^{\alpha,p}$, then $\Gamma_k^{\alpha,p}(x) = C_k(x)$.

**Lemma 12** *For any fixed input $x$, if $(\alpha, p)$ is chosen uniformly at random from $[m] \times \mathcal{P}R^m$, then $\Pr\left[\Gamma_k^{\alpha,p}(x) \neq C_k(x)\right] \leq (8t \log W)^{-1}$.*

PROOF. We know that each gate $f_i$ of $C_k$, has fan-in bounded by $\log W$, and will give the correct output if $(\alpha, p)$ is good. By Lemma 9, the probability that $(\alpha, p)$ is bad is $(8s\, t \log W)^{-1}$ by the choice of $m$. Since there are at most $s$ gates in $C_k$, the lemma follows. $\square$

We say that $(\alpha, p)$ is good for $x$ and $\Gamma_k^{\alpha,p}$, if it is good for all gate approximators $\varphi_i^{\alpha,p}$ of $\Gamma_k^{\alpha,p}$ simultaneously.

What happens when $(\alpha, p)$ is bad for $\Gamma_k^{\alpha,p}$? The magnitude of the output of $\Gamma_k^{\alpha,p}$ is bounded by the maximum output of the approximator of the top gate of $C_k$. Using Corollary 5, we have for all $x$ and all $(\alpha, p)$,

$$|\Gamma_k^{\alpha,p}(x)| \leq 2 + 3 \log W. \tag{9}$$

Since the corollary holds even when the inputs to the top gate are integers, this bound holds even when some other approximator in $\Gamma_k^{\alpha,p}$ fails.

If we combine Lemma 12 and (9) we get

**Lemma 13** *For any fixed input $x$, if $(\alpha, p)$ is chosen uniformly at random from $[m] \times \mathcal{P}R^m$, then $|\mathrm{E}[\Gamma_k^{\alpha,p}(x)] - C_k(x)| \leq \frac{1}{2t}$.*

Do the same for all the circuits $C_i$ to get approximators $\Gamma_i^{\alpha,p}$. Consider the following function:

$$h(x) = sign\left(\sum_{i=1}^{t} \sum_{(\alpha,p)} \Gamma_i^{\alpha,p}(x)\right).$$

Observe that this is equivalent to

$$h(x) = sign\left(\mathrm{E}\left[\sum_i \Gamma_i^{\alpha,p}(x)\right]\right). \tag{10}$$

We claim the following.

**Proposition 14** *For all inputs $x$, $h(x) = g(x)$.*

PROOF. We will prove this by showing that for any fixed $x$,

$$\left|\mathrm{E}\left[\sum_{i=1}^{t} \Gamma_i^{\alpha,p}(x)\right] - \sum_{i=1}^{t} C_i(x)\right| \leq 1/2. \tag{11}$$

This is sufficient by (10) and the fact that $\left|\sum_{i=1}^{t} C_i(x)\right| \geq 1$. The inequality (11) follows by straightforward application of Lemma 13. $\square$

An argument analogous to that in the previous section shows that $g(x)$ can be implemented as a depth $d$ threshold circuit. We call the circuit $\widehat{C}$. It is not hard to see that each wire in $C$ corresponds to a polynomially (in $\log W$) many wires in $\widehat{C}$.

To get integer weights in the circuit it is sufficient to multiply all weights by 2. The weights all have magnitude bounded by order of the largest prime used multiplied by $s$. The largest prime in $\mathcal{P}R^m$ has size $O(m^2 \log m)$, so the weights are all $O(s^3 t^2 \log^6 W(\log(st) + \log\log W))$. This completes the proof of Theorem 11.

Just as before, the construction is polynomial in $n$ as long as $\log W$ is polynomial in $n$. By Theorem 1, this is always possible. $\square$

# 6 Uniform Computations

The constructions given in this paper in addition to be explicit, preserve also the uniformity conditions of the classes of circuits. The constructions of Section 4 and 5 yield the following.

**Theorem 15** *Given any $f$–uniform class of threshold circuits $\{C_n\}$ of depth $d$ and polynomial size, $f \in \{L, P\}$. There exists an algorithm running in logspace that given a description of a circuit $\overline{C}_n$ of depth $d$ and a polynomial size will output the description of a majority circuit $\overline{C}'_n$ of depth $d+1$ and a polynomial size such that $f_{C_n} = f_{C'_n}$.*

We have also an immediate corollary:

**Corollary 16**

$$\begin{aligned} L\text{–uniform } LT_d &\subseteq L\text{–uniform } \widehat{LT}_{d+1} \\ P\text{–uniform } LT_d &\subseteq P\text{–uniform } \widehat{LT}_{d+1} \ . \end{aligned}$$

$\square$

# 7 Conclusions and Open Problems

Our results entail the first explicit constructions for the optimal depth, polynomial size majority circuits for the number of basic functions including, among others,

*powering* (depth 3), *integer multiplication* and *integer division* (depth 3), see [26] and [4].

More generally, our results entail the *uniformity* of the classes of majority circuits simulating the corresponding classes of *threshold circuits*. We look at the following functions.

ADDITION: given two $n$-bit numbers, compute their sum.

MULTIPLE ADDITION: given $n$ $n$-bit numbers, compute their sum.

MULTIPLICATION: given two $n$-bit numbers, compute their product.

MULTIPLE MULTIPLICATION: given $n$ $n$-bit numbers, compute their product.

DIVISION: given a $2n$-bit numbers $x$ and an $n$-bit number $y$, compute $\lfloor x/y \rfloor$.

SQUARING: given an $n$-bit number $x$, compute $x^2$.

POWERING: given an $n$-bit numbers $x$ and a $\log n$-bit number $y$, compute $x^y$.

COMPARISON: given two $n$-bit numbers $x$ and $y$, decide if $x \geq y$.

MAXIMUM: given $n$ $n$-bit numbers, output the largest one.

SORTING: given $n$ $n$-bit numbers, output them in sorted order.

The following table surveys the uniform upper bounds known before and stemming from the present paper and compares it with the best known (nonuniform) lower bounds. Most of the constructions follow from non-uniform versions in [26] and [25] (see also [21]). The uniform constructions for ADDITION,COMPARISON, and SORTING follow from [3].

| Function | Uniform Depth Upper Bound | Lower Bound |
|---|---|---|
| ADDITION | 2,$L$–uniform | 2 |
| MULTIPLE ADDITION | 2,$L$–uniform | 2 |
| MULTIPLICATION | 3,$L$–uniform | 3 [11] |
| MULTIPLE MULTIPLICATION | 4,$L$–uniform | 3 [11] |
| DIVISION | 3,$P$–uniform | 3 [32] |
| SQUARING | 3,$L$–uniform | 3 [32] |
| POWERING | 3,$P$–uniform | 2 [32] |
| COMPARISON | 2,$L$–uniform | 2 [24] |
| MAXIMUM | 3,$L$–uniform | 2 |
| SORTING | 3,$L$–uniform | 3 [25] |

We conclude with the list of open problems:

1. If the original circuit is monotone, our construction yields a non-monotone majority circuit. It is an open question if an arbitrary monotone threshold gate can be simulated by constant depth monotone majority circuits of polynomial size.

2. Alternating Turing machines are closely connected to circuits with AND-gates and OR-gates, and counting Turing machines are connected to majority circuits. Is there a reasonable machine model that has such a relationship to threshold circuits? If so, what would be the corresponding notion of uniformity, and would our simulation still work?

3. Any strong lower bounds for depth two threshold circuits or depth three majority circuits computing some explicit function?

# Acknowledgement

We are grateful to Johan Håstad and Ingo Wegener for many valuable comments on earlier versions of this paper. We also thank Jens Lagergren, Sasha Razborov, and

Avi Wigderson for several helpful discussions on the topic of this paper.

# References

[1] E. Allender. A note on the power of threshold circuts. In *Proc. 30th IEEE Symposium on Foundations of Computer Science*, pages 580–584, 1989.

[2] N. Alon and R. B. Boppana. The monotone circuit complexity of boolean functions. *Combinatorica*, 7:1–22, 1987.

[3] N. Alon and J. Bruck. Explicit constructions of depth-2 majority circuits for comparison and addition. Technical Report RJ 8300 (75661), IBM Research Division, August 1991. To appear in *SIAM J. Disc. Math.*

[4] P. W. Beame, S. A. Cook, and H. J. Hoover. Log depth circuits for division and related problems. In *Proc. 25th IEEE Symposium on Foundations of Computer Science*, pages 1–6, 1984.

[5] R. Beigel and J. Tarui. On ACC. In *Proc. 32nd IEEE Symposium on Foundations of Computer Science*, pages 783–792, 1991.

[6] J. Bruck. Harmonic analysis of polynomial threshold functions. *SIAM J. Disc. Math.*, 3(2):168–177, May 1990.

[7] J. Bruck and R. Smolensky. Polynomial threshold functions, $AC^0$ functions and spectral norms. In *Proc. 31st IEEE Symposium on Foundations of Computer Science*, pages 632–641, 1990.

[8] A. Chandra, L. Stockmeyer, and U. Vishkin. Constant depth reducibility. *SIAM J. Comp.*, 13:423–439, 1984.

[9] S. A. Cook. A taxonomy of problems with fast parallel algorithms. *Information and Control*, 64:2–22, 1985.

[10] M. Goldmann, J. Håstad, and A. Razborov. Majority gates vs. general weighted threshold gates. *Computational Complexity*, 2:277–300, 1992.

[11] A. Hajnal, W. Maass, P. Pudlák, M. Szegedy, and G. Turán. Threshold circuits of bounded depth. In *Proc. 28th IEEE Symposium on Foundations of Computer Science*, pages 99–110, 1987.

[12] J. Håstad. On the size of weights for threshold gates. Manuscript, 1992. To appear in SIAM. J. Disc. Math.

[13] J. Håstad and M. Goldmann. On the power of small-depth threshold circuits. *Computational Complexity*, 1(2):113–129, 1991.

[14] T. Hofmeister and P. Pudlak. A Proof that Division Is Not in $TC_2^0$. *Research Report No. 447* (1992), Dept. of Computer Science, Univ. of Dortmund, 1992.

[15] R. Impagliazzo, R. Paturi, and M. Saks. Size-depth trade-offs for threshold circuits. In *Proc. 25th ACM Symposium on Theory of Computing*, 1993.

[16] S. Muroga. *Threshold Logic and its Applications*. Wiley-Interscience, 1971.

[17] P. Orponen. Neural networks and complexity theory. In *Proc. 17th International Symposium on Mathematical Foundations of Computer Science*, pages 50–61. Springer-Verlag, 1992. Lecture Notes in Computer Science 629.

[18] I. Parberry. A primer on the complexity theory of neural networks. In *Formal Techniques in Artificial Intelligence: A Sourcebook*. Elsevier, 1990.

[19] I. Parberry and G. Schnitger. Parallel computation with threshold functions. *Journal of Computer and System Sciences*, 36(3):278–302, June 1988.

[20] N. Pippenger. The complexity of computation by networks. *IBM J. of Research and Development*, 31(2):235–243, March 1987.

[21] A. A. Razborov. On small depth threshold circuits. In *Proc. 3rd Scandinavian Workshop on Algorithm Theory*, pages 42–52. Springer-Verlag, 1992. Lecture Notes in Computer Science 621.

[22] A. A. Razborov and A. Wigderson. $n^{\Omega(\log n)}$ lower bounds on the size of depth 3 threshold circuits with AND gates at the bottom. *Information Processing Letters*, 45(6):303–307, 1993.

[23] W. L. Ruzzo. On uniform circuit complexity. In J. Computer and System Sciences, 22:365–383, 1981. 383.

[24] K. Y. Siu and J. Bruck. On the power of threshold circuits with small weights. *SIAM J. Disc. Math.*, 4:423–435, 1991.

[25] K. Y. Siu, J. Bruck, T. Kailath, and T. Hofmeister. Depth-efficient neural networks for division and related problems. Technical Report RJ 7946, IBM Research Division, January 1991. *IEEE Trans. Information Theory*, 39:946–956, 1993.

[26] K. Y. Siu and V. Roychowdhury. On optimal depth threshold circuits for multiplication and related problems. *SIAM J. Disc. Math.*, 7:284–292, 1994.

[27] K. Y. Siu, V. Roychowdhury, and T. Kailath. Computing with optimal size threshold circuits. Technical Report, Stanford University, 1990.

[28] S. Toda. On the computational power of $PP$ and $\oplus P$. In *Proc. 30th IEEE Symposium on Foundations of Computer Science*, pages 514–519, 1989.

[29] J. Torán. An oracle characterization of the counting hierarchies. In *Proc. 3rd Annual Structure in Complexity Theory Conference*, pages 213–223, 1988.

[30] J. Torán. A combinatorial technique for separating counting complexity classes. In *Proc. 16th International Colloquium on Automata, Languages and Programming*, pages 732–744. Springer-Verlag, 1989. Lecture Notes in Computer Science 372.

[31] K. W. Wagner. The complexity of combinatorial problems with succinct input representation. *Acta Informatica*, 23:325–356, 1986.

[32] I. Wegener. Optimal Lower Bounds on the Depth of Polynomial Size Threshold Circuits for some Arithmetic Functions. *Information Processing Letters*, 46:85–87, 1993.

[33] A. C. Yao. On $ACC$ and threshold circuits. In *Proc. 31st IEEE Symposium on Foundations of Computer Science*, pages 619–627, 1990.