Lower Bounds on Threshold and Related Circuits via Communication Complexity

Vwani P. Roychowdhury, Alon Orlitsky, and Kai-Yeung Siu

Abstract—**Using communication complexity concepts and techniques, we derive linear ($\Omega(n)$) and almost-linear ($\Omega(n/\log n)$) lower bounds on the size of circuits implementing certain functions. Our approach utilizes only basic features of the gates used, hence the bounds hold for general families of gates of which the symmetric and threshold gates are special cases. Each of the bounds derived is shown to be tight for some functions and some applications to threshold circuit complexity are indicated. The results generalize and in some cases strengthen recent results.**

Index Terms—**Linear/almost-linear circuit-size lower bounds, communication complexity, threshold gates/circuits, symmetric gates/circuits, equality, comparison and inner product mod 2 Boolean functions.**

I. Introduction

LET us first describe the model, review known results, and introduce techniques and results presented in this paper.

Gates, Circuits, and Complexity

An *n-variable gate* is a physical device computing a single n-variable function. The input variables of a gate can be permuted, omitted, or repeated, hence we identify the gate with the set of functions derived by such operations. For example, the set of functions implementable by a gate computing the four-variable function $(x \wedge y) \vee (z \wedge w)$, where $\wedge$ is logical "AND" and $\vee$ logical "OR," includes functions such as $(x \wedge z) \vee (y \wedge w)$, $(x \wedge y) \vee (x \wedge y) \equiv x \wedge y$, and $(y \wedge y) \vee (y \wedge y) \equiv y$.

We usually consider a set, or a *family*, of gates. We identify the family with the union of the function sets corresponding to each of its gates.

Let $\mathcal{G}$ be a family of gates. A circuit whose gates are all from $\mathcal{G}$ is a *$\mathcal{G}$-circuit*. The *size* of a circuit is the number of gates it contains and its *depth* is the maximum number of gates along a path from an input to an output. The *$\mathcal{G}$-circuit complexity* $C_{\mathcal{G}}(f)$ of f is the size of the smallest $\mathcal{G}$-circuit that computes f. In principle, some function may not be computed by a $\mathcal{G}$-circuit. However, every gate family considered here forms a complete basis, and hence $C_{\mathcal{G}}(f)$ is always defined.

The circuit complexity of functions has many theoretic and practical applications. Therefore, several gate families have been extensively investigated. They include:

AND/OR/NOT gates ($\wedge$, $\vee$): These gates perform logical "AND" or "OR" of their, possibly negated, inputs. AND/OR/NOT gates come in two varieties: constant fan-in gates and unbounded fan-in gates. The bounds we prove apply to both.

Symmetric gates ($\mathcal{SYM}$): Gates of the form $g(\sum_{i=1}^{n} x_i)$ for arbitrary binary functions g. These gates compute some binary function of their input sum. One type of a symmetric gate is a mod_m gate. It computes a binary function of the form $g((\sum_{i=1}^{n} x_i) \bmod m)$ for some fixed integer m.

Threshold gates ($\mathcal{TH}$): Gates of the form $\mathrm{sgn}(\sum_{i=1}^{n} w_i x_i - T)$ where T is an arbitrary *threshold*, the w_i's are integer *weights*, and $\mathrm{sgn}(x)$ is 1 if $x \geq 0$ and 0 otherwise. In the analysis we distinguish between general threshold gates with arbitrary weights and threshold gates with polynomially bounded integer weights.

Generalized symmetric gates ($\mathcal{GS}$): Gates of the form $g(\sum_{i=1}^{n} w_i x_i)$ for arbitrary function g and integer weights w_i that are polynomially bounded in n. The weights are restricted to be polynomially bounded because every function can be computed by a single generalized symmetric gate if the weights are allowed to be exponentially large.

Using the above terminologies, $C_{\wedge\vee}(f)$, $C_{\mathcal{GS}}(f)$, $C_{\mathcal{SYM}}(f)$, and $C_{\mathcal{TH}}(f)$ refer to the circuit complexity of the function f when the circuit comprises AND/OR/NOT, generalized symmetric, symmetric, and threshold gates, respectively.

Note that every AND/OR/NOT gate is also a threshold gate with polynomially bounded integer weights. Moreover, any threshold gate with polynomially bounded weights as well as any symmetric gate is also a generalized symmetric gate.

Related Results and Motivation

Much research has gone into estimating $C_{\mathcal{G}}(f)$ for various functions and gate families [13]. The strongest results apply to bounded depth circuits. For constant depth AND/OR/NOT circuits and mod_p circuits (where p is prime), exponential-size lower bounds for specific functions such as the parity were established in [2], [8], [11]. For circuits of more powerful gates, less is known. In [5], an exponential lower bound on the size of depth-2 threshold circuits implementing the n-variable *Inner Product Mod 2* function (IP) was shown, where IP is defined

Manuscript received July 30, 1992. This work was supported by the Joint Services Program at Stanford University (US Army, US Navy, US Air Force) under Contract DAAL03-88-C-0011 and the Department of the Navy (NAVELEX) under Contract N00039-84-C-0211, NASA Headquarters, Center fo rAeronautics and Space Information Sciences under Grant NAGW-419-S6.

V. P. Roychowdhury is with the School of Electrical Engineering, Purdue University, West Lafayette, IN 47907 USA.

A. Orlitsky is with AT&T Bell Laboratories, Murray Hill, NJ 07974 USA.

K.-Y. Siu is with the Department of Electrical and Computer Engineering, University of California at Irvine, Irvine, CA 92717 USA.

IEEE Log Number 9216797.

0018–9448/94$04.00 © 1994 IEEE

as follows:

$$\mathrm{IP}\left(x_1,\cdots,x_{\frac{n}{2}},y_1,\cdots,y_{\frac{n}{2}}\right) = \begin{cases}1 & \text{if } \sum_{i=1}^{\frac{n}{2}} x_i \wedge y_i \text{ is odd,}\\ 0 & \text{otherwise.}\end{cases}$$

However, this bound applies only when the integer weights in the second layer are polynomially bounded. No superlinear lower bounds are known for depth-2 threshold circuits with exponentially weights in the second layer, or for depth-3 threshold circuits with polynomially bounded integer weights.

For unrestricted depth and unbounded fan-in circuits, deriving seemingly weak lower bounds, such as linear or polylogarithmic in the number of input variables, are considered challenging [13], [10]. For example, an $\Omega(\log n)$ lower bound on the size of threshold circuits computing the parity of n bits is shown in [13]. Only recently have linear/almost-linear lower bounds been established for circuits with gates of unbounded fan-in. A linear-size lower bound on circuits, where each gate computes a commutative and associative function, was given in [6]. However, the family of gates is too restrictive to apply to symmetric or threshold circuits.

Recently, an $\Omega(n/\log n)$ lower bound on the size of symmetric gate circuits computing the n-variable *equality* function was established in [10], where the equality function is defined as

$$\mathrm{EQ}\left(x_1,\cdots,x_{\frac{n}{2}},y_1,\cdots,y_{\frac{n}{2}}\right) = \begin{cases}1 & \text{if } x_i = y_i \text{ for all } 1 \le i \le \frac{n}{2},\\ 0 & \text{otherwise.}\end{cases}$$

Novel techniques such as analytic function interpolation of Boolean functions and the differential dimension were used. More recently a linear lower bound $(n/4)$ on the size of threshold circuits with arbitrary weights computing the n-variable IP was proved in [4].

Techniques and Results in this Paper

Using communication complexity concepts and techniques, we derive linear and almost-linear lower bounds on the size of circuits implementing certain functions. This approach utilizes only basic features of the gates used, hence the bounds hold for general families of gates of which the symmetric and threshold gates considered in [10], [4] are special cases. Thus communication complexity arguments serve to generalize known lower bounds and unify their proofs.

In the next section, we define the notions of *decomposition number* and *largest monochromatic rectangle* of a function. These are simple attributes useful for analyzing the communication complexity of various functions.

In Section III, we consider the family of *polynomially-rectangular* gates. These gates, which include symmetric, generalized symmetric, and threshold gates with polynomially bounded integer weights, compute functions with small decomposition numbers. We show that functions computed by small-size circuits of polynomially-rectangular gates have small decomposition numbers. It follows that functions with high decomposition numbers require circuits of proportionally large size. We then use some effective techniques to derive lower bounds on the decomposition numbers and prove almost-linear lower bounds on the circuit complexity of several functions.

In Section IV, we strengthen the results for the family of *triangular gates*. These gates, which include all threshold gates, compute functions with large monochromatic rectangles. We show that any function computed by a small circuit of triangular gates contains a large monochromatic rectangle. Therefore, functions with only small monochromatic rectangles require circuits of proportionally large size.

We shall illustrate the results using the Inner Product Mod 2 (IP) function and the Equality (EQ) function. The bounds we derive imply:

1) Any implementation of n-variable EQ or IP by generalized symmetric gates requires $\Theta(n/\log n)$ gates. Namely, if the weights are bounded by n^k, then
$$\frac{1}{4(k+1)}\frac{n}{\log n} \le C_{\mathcal{GS}}(\mathrm{EQ}),\ C_{\mathcal{GS}}(\mathrm{IP}) \le \frac{\log 3}{2k}\frac{n}{\log n}.$$
2) Any implementation of n-variable EQ or IP by symmetric gates requires $\Omega(n/\log n)$ gates:
$$C_{\mathcal{SYM}}(\mathrm{EQ}),\ C_{\mathcal{SYM}}(IP) \ge \frac{n}{4\log n}.$$
3) Any implementation of n-variable EQ or IP by AND/OR/NOT gates requires $\Theta(n)$ gates:
$$\frac{n}{2\log 3} \le C_{\wedge,\vee}(\mathrm{EQ}),\ C_{\wedge,\vee}(\mathrm{IP}) \le 2n.$$
4) Any implementation of n-variable IP by threshold gates requires $\Theta(n)$ gates.
$$\frac{1}{4}n \le C_{\mathcal{TH}}(\mathrm{IP}) \le \frac{3}{4}n + 1.$$
Both upper and lower bounds apply to threshold circuits with exponential as well as polynomially bounded integer weights.

Note that the bounds in (1), (3), and (4) are tight up to a small multiplicative factor.

Related to EQ is the n-variable *Comparison* function:

$$\mathrm{COMP}\left(x_1,\cdots,x_{\frac{n}{2}},y_1,\cdots,y_{\frac{n}{2}}\right) = \begin{cases}1 & \text{if } \sum_{i=1}^{\frac{n}{2}} 2^i x_i \ge \sum_{i=1}^{\frac{n}{2}} 2^i y_i,\\ 0 & \text{otherwise.}\end{cases}$$

II. Communication Complexity Arguments

Let $f: \{0,1\}^n \to \{0,1\}$ be an n-variable Boolean function, and let $Z = \{z_1,\cdots,z_n\}$ denote the set of variables of f. If $X \subset Z$ is a subset of variables, then an element of $\{0,1\}^{|X|}$ corresponds to a value assignment to the variables in X and is called an *X-input*.

Let $\{X, Y\}$ partition the set of variables ($X \cup Y = \{z_1,\cdots,z_n\}$ and $X \cap Y = \emptyset$). An X-input x together with a Y-input y correspond in an obvious way to an input which we call the *joint input* and will be denoted by (x, y). In the same way, the set of all inputs corresponds to the Cartesian product $\{0,1\}^{|X|} \times \{0,1\}^{|Y|}$. We can therefore associate with the function f and the partition $\{X, Y\}$ a matrix $M_{f,X,Y}$. We

shall also refer to $M_{f,X,Y}$ as the *function matrix* of f under the partition $\{X, Y\}$. It has $2^{|X|}$ rows, each indexed by an X-input, $2^{|Y|}$ columns, each indexed by an Y-input, and

$$M_{f,X,Y}(x, y) = f(x, y).$$

An $\{X, Y\}$-*rectangle* is a Cartesian product $A \times B$ where A is a set of X-inputs and B is a set of Y-inputs. The *size* of the rectangle is $|A| \cdot |B|$, the number of inputs it contains. An $\{X, Y\}$-*decomposition* is a partition of $\{0, 1\}^{|X|} \times \{0, 1\}^{|Y|}$ into $\{X, Y\}$-rectangles. The *size* of the decomposition is the number of rectangles in the partition. A set of inputs is f-*constant* if f assigns the same value to all the elements in the set. An f-*constant* $\{X, Y\}$-*decomposition* is an $\{X, Y\}$-decomposition whose rectangles are all f-constant.

The concept of rectangles plays a major role in the following *communication complexity* problem. As before, let f be an n-variable Boolean function and $\{X, Y\}$ be a partition of the variables. A person P_X knows an X-input, a person P_Y knows a Y-input, and they communicate according to a predetermined protocol in order to find the value of f on their joint input. We are interested in $\hat{C}(f, X, Y)$, the maximum number of bits P_X and P_Y must transmit for the worst input.

The following results are well known [14]:

1) Every protocol induces an $\{X, Y\}$-decomposition.
2) If the protocol always produces the correct answer, this decomposition is f-constant.
3) The maximum number of bits required by the protocol for the worst input is at least the logarithm[1] of the decomposition.

Let $\rho_{f,X,Y}$ be the smallest size of an f-constant $\{X, Y\}$-decomposition. From the above,

$$\hat{C}(f, X, Y) \geq \log \rho_{f,X,Y}. \tag{1}$$

It was shown in [1] that this bound is not far from being tight:

$$\hat{C}(f, X, Y) \leq \log^2 \rho_{f,X,Y}.$$

For that reason, several simple methods have been introduced to derive lower bounds on $\rho_{f,X,Y}$ for arbitrary f, X, and Y.

Largest f-constant rectangle: Let $L_{f,X,Y}$ be the size of the largest f-constant $\{X, Y\}$-rectangle. Clearly,

$$\rho_{f,X,Y} \geq \frac{2^n}{L_{f,X,Y}}.$$

Fooling set: An f-constant subset S of $\{0, 1\}^{|X|} \times \{0, 1\}^{|Y|}$ is an $\{X, Y\}$-*fooling set* if $(x_1, y_1), (x_2, y_2) \in S$ implies that either $f(x_1, y_2)$ or $f(x_2, y_1)$ differs from the common value of f over S. Let $F_{f,X,Y}$ be the size of the largest $\{X, Y\}$-fooling set. An f-constant $\{X, Y\}$-rectangle contains at most one element of a given $\{X, Y\}$-fooling set. Hence,

$$\rho_{f,X,Y} \geq F_{f,X,Y}.$$

[1] All logarithms are to the base 2.

Rank: The matrix representing the indicator function of a rectangle has rank 1, and ranks are subadditive under matrix addition. Melhorn and Schmidt [7] concluded that under any field

$$\rho_{f,X,Y} \geq 2 \operatorname{rank}(M_{f,X,Y}) - 1.$$

In our applications, we can choose the most advantageous partition of the input variables. We therefore define the *decomposition number* of f,

$$\rho_f = \max\{\rho_{f,X,Y} : \{X, Y\} \text{ partitions } \{x_1, \cdots, x_n\}\},$$

to be the number of rectangles needed in the variable partition that yields the strongest bound in (1). We use the methods above to derive lower bounds on the decomposition number of EQ, IP, and COMP.

Example 1: We show that the decomposition numbers of both EQ and IP are larger than $2^{\frac{n}{2}}$. In the following, $X = \{x_1, \cdots, x_{n/2}\}$ and $Y = \{y_1, \cdots, y_{n/2}\}$. Every $n/2$ bit sequence corresponds in an obvious way to an X-input and to a Y-input. We can therefore talk about the joint input (x, x) where $x \in \{0, 1\}^{n/2}$.

Equality: The set $\{(x, x) : x \in \{0, 1\}^{n/2}\}$ is an $\{X, Y\}$-fooling set of size $2^{n/2}$, implying that $\rho_{\mathrm{EQ},X,Y} \geq 2^{n/2}$. In fact, $\rho_{\mathrm{EQ}} = \rho_{\mathrm{EQ},X,Y} = 2^{n/2+1}$. A similar argument shows $\rho_{\mathrm{COMP}} = 2^{\frac{n}{2}}$.

Inner Product Mod 2: It can be shown that $M_{\mathrm{IP},X,Y}$ is a Hadamard matrix and hence has full rank over the reals. Thus $\rho_{\mathrm{IP}} \geq 2^{(n/2)+1} - 1$. □

III. Rectangular Gates

The last section was motivated by the notion that a function with a high decomposition number is "complex." To show that computing such a function requires many gates, we now show that the gates used are "simple," that is, they can be decomposed into a small number of rectangles.

A function f is *r-rectangular* for some integer r if for every partition $\{X, Y\}$ of the variables, there is an f-constant $\{X, Y\}$-decomposition consisting of at most r rectangles, namely, if

$$\rho_f \leq r.$$

Let $p : \mathcal{Z}^+ \to \mathcal{Z}$. A family $\mathcal{G}$ of functions is *p-rectangular* if for every $m \leq n$, all m-variable functions in $\mathcal{G}$ are $p(n)$-rectangular. The family is *polynomially-rectangular* if it is p-rectangular for some polynomial p. These definitions apply to gates and families of gates via their underlying functions. The next lemma, its simple proof omitted, provides a basic tool for proving that a function is r-rectangular.

Lemma 1: Let f be a Boolean function and let $\{X, Y\}$ partition the set of variables. $f(x, y)$ can be expressed as $h(g_1(x), g_2(y))$. Then

$$\rho_{f,X,Y} \leq |g_1| \cdot |g_2|$$

where $|g_i|$ is the size of the range of g_i. □

To prove that a function is r-rectangular, we apply the lemma to *all* possible partitions of the variables.

Example 2: We show that the gate families mentioned in the introduction are polynomially rectangular. In the following, $\{X, Y\}$ is an arbitrary partition of the input variables $\{z_1, \cdots, z_n\}$.

AND/OR:

$$\bigvee_{z_i \in X \cup Y} z_i = \left(\bigvee_{z_i \in X} z_i\right) \bigvee \left(\bigvee_{z_i \in Y} z_i\right),$$

hence the lemma implies that every OR gate is 4-rectangular (in fact three rectangles are sufficient). The same holds for AND gates.

Symmetric gates:

$$f(x, y) = h\left(\sum_{z_i \in X} z_i, \sum_{z_i \in Y} z_i\right),$$

hence

$$\rho_{f,X,Y} \leq (|X| + 1) \cdot (|Y| + 1) \leq \left(\frac{n}{2} + 1\right)^2.$$

Generalized symmetric gates:

$$f(x, y) = h\left(\sum_{z_i \in X} w_i z_i + \sum_{z_i \in Y} \tilde{w}_i z_i\right).$$

where the w_i's are integers bounded by some polynomial $p(n)$. The first sum attains at most $(|X|+1)\cdot p(n)$ values and likewise for the second, hence f is $(n/2) + 1)^2 \cdot p^2(n)$-rectangular. It follows that the family of generalized symmetric functions is polynomially rectangular.

Threshold gates: Since generalized symmetric functions are polynomially rectangular, it follows that the family of threshold functions with polynomially bounded integer weights is also polynomially rectangular. □

Theorem 1: Let $\mathcal{G}$ be a p-rectangular family of gates. If an $\mathcal{G}$-circuit consisting of k gates computes an n-variable Boolean function f, then

$$\rho_f \leq (p(n))^k.$$

Proof: We can label the gates in the circuit so that if $i < j$ then there is no directed path from the output of gate j to the input of gate i. Let g_j denote the function computed by gate j. We prove by induction on j that the vector-valued function $G_j = (g_1, g_2, \cdots, g_j)$ has $\rho_{G_j,X,Y} \leq (p(n))^j$ for all variable partitions $\{X, Y\}$.

The induction basis holds by definition; suppose it holds for j, and consider the $(j + 1)$st gate. Let $\{X, Y\}$ be a variable partition. There is a G_j-constant $\{X, Y\}$-decomposition consisting of at most $(p(n))^j$ rectangles. Let R be a rectangle in this decomposition. Over R, all of $g_1, \cdots, g_j$ are constant, hence the $(j+1)$st gate coincides with a $p(n)$ rectangular function of the original variables. Therefore R can be partitioned into $p(n)$ G_{j+1}-constant $\{X, Y\}$ rectangles, and the induction step follows. □

Corollary 1: Let $\mathcal{G}$ be a p-rectangular family of gates. For every n-variable function f,

$$C_{\mathcal{G}}(f) \geq \frac{\log \rho_f}{\log p(n)}.$$ □

We apply the corollary to derive a lower bound on the number of gates needed to implement the Equality and the Inner Product Mod 2 functions.

Theorem 2:

i) For circuits consisting of AND, OR, and NOT gates:

$$\frac{n}{2 \log 3} \leq C_{\wedge,\vee}(\text{EQ}),\ C_{\wedge,\vee}(\text{IP}) \leq 2n.$$

ii) For circuits consisting of generalized symmetric gates:

$$C_{\mathcal{GS}}(\text{EQ}),\ C_{\mathcal{GS}}(\text{IP}) = \Theta\left(\frac{n}{\log n}\right).$$

More specifically, if the integer weights are bounded by n^k, then

$$\frac{1}{4(k+1)} \frac{n}{\log n} \leq C_{\mathcal{GS}}(\text{EQ}),\ C_{\mathcal{GS}}(\text{IP}) \leq \frac{\log 3}{2k} \frac{n}{\log n}.$$

iii) For circuits consisting of symmetric gates:

$$C_{\mathcal{SYM}}(\text{EQ}),\ C_{\mathcal{SYM}}(\text{IP}) \geq \frac{n}{4 \log n}.$$

Proof: All six lower bounds follow from Corollary 1 as both EQ and IP have decomposition numbers of at least $2^{\frac{n}{2}}$. The upper bounds in i) follow from a simple construction.

We implement IP as a depth-3 generalized symmetric circuit (the next section shows it cannot be implemented using less than $\Omega(n)$ threshold gates).

Let $m = 2\lfloor k \log n \rfloor$. Clearly, m-variable COMP can be written as

$$\text{COMP}\left(x_1, \cdots, x_{\frac{m}{2}}, y_1, \cdots, y_{\frac{m}{2}}\right) = \text{sgn}\left(\sum_{i=1}^{m/2} 2^i (x_i - y_i)\right), \tag{2}$$

thus can be implemented by a single threshold gate with weights of at most n^k. For $i = 1, \cdots, \lceil n/m \rceil$, let

$$x^i = x_{(i-1)\cdot m/2+1}, \cdots, x_{i \cdot m/2}$$

and

$$y^i = y_{(i-1)\cdot m/2+1}, \cdots, y_{i \cdot m/2}.$$

Then,

$$\text{EQ}\,(x^i, y^i) = \text{COMP}\,(x^i, y^i) + \text{COMP}\,(y^i, x^i) - 1.$$

Hence, m-variable EQ can be implemented by a depth-2 threshold circuit with weights of magnitudes at most n^k and where the top gate is just a weighted sum of the first-level outputs (without a threshold). Finally, observe that

$$\text{EQ}\left(x_1, \cdots, x_{\frac{n}{2}}, y_1, \cdots, y_{\frac{n}{2}}\right) = \bigwedge_{i=1}^{\lceil n/m \rceil} \text{EQ}\,(x^i, y^i).$$

Since any AND is just the sum of its variables with an appropriate threshold, this gate can be combined with the second layer above to derive a depth-2 circuit for EQ of size

$2\lceil n/2k\log n\rceil+1$. When generalized symmetric gates are used instead of threshold gates, the number of gates can be reduced to $\lceil n/2k\log n\rceil+1$.

When trying to meet the lower bound for IP, we cannot use threshold gates as we did for EQ. The next section shows that any threshold circuit for IP (even with exponential weights) has at least linear size. Yet, we can use the circuit structure applied to EQ. Every $(k\log n)$-variable function, in particular $\text{IP}(x_1,\cdots,x_{k\log n/2}, y_1,\cdots,y_{k\log n/2})$, can be computed by a single generalized symmetric gate with weights of magnitudes at most n^k. Use $\lceil n/k\log n\rceil$ generalized symmetric gates to compute the partial IP's, then use a single (symmetric) gate to compute their parity. □

It is shown in [9] that COMPARISON cannot be computed by a single threshold gate with polynomially bounded integer weights. It is, however, shown in [9] that it can be computed by a depth-2 polynomial-size threshold circuit with polynomially bounded integer weights. We next establish a tight lower bound on the size of a generalized symmetric circuit computing COMPARISON and also derive a depth-3 threshold circuit with size that achieves the lower bound. It is not known whether the lower bound can be achieved by a depth-2 threshold circuit of polynomially bounded integer weights.

Theorem 3:

$$C_{\mathcal{GS}}(\text{COMP})=\Theta\left(\frac{n}{\log n}\right).$$

Proof: It is shown in Example 1 that $\rho_{\text{COMP}}=2^{(n/2)+1}$. Hence it follows from Corollary 1 that $C_{\mathcal{GS}}(\text{COMP})=\Omega(n/\log n)$. We next show that the lower bound can be met by a depth-3 threshold circuit with polynomially bounded integer weights. It is not known whether the lower bound can be met by a depth-2 threshold circuit with polynomially bounded integer weights.

Let $m=2\lceil\log n\rceil$. For $i=1,\cdots,\lceil n/m\rceil$, let

$$C_i=\text{sgn}\left(\sum_{j=(i-1)\cdot m/2+1}^{i\cdot m/2}2^j(x_j-y_j)\right),$$

and

$$\tilde{C}_i=\text{sgn}\left(\sum_{j=(i-1)\cdot m/2+1}^{i\cdot m/2}2^j(x_j-y_j)-1\right).$$

Note that both C_i and $\tilde{C}_i$ can be computed with threshold gates of polynomially bounded weights. Further,

$$C_i=1 \quad \text{iff} \sum_{j=(i-1)\cdot m/2+1}^{i\cdot m/2}2^jx_j\geq\sum_{j=(i-1)\cdot m/2+1}^{i\cdot m/2}2^jy_j,$$

and

$$\tilde{C}_i=1 \quad \text{iff} \sum_{j=(i-1)\cdot m/2+1}^{i\cdot m/2}2^jx_j>\sum_{j=(i-1)\cdot m/2+1}^{i\cdot m/2}2^jy_j.$$

Define Boolean expressions:

$$B_{\lceil n/m\rceil}=\tilde{C}_{\lceil n/m\rceil},$$

for $k=2,\cdots,\lceil n/m\rceil-1$

$$B_k=\tilde{C}_k\bigwedge_{j=k+1}^{\lceil n/m\rceil}C_j,$$

and

$$B_1=\bigwedge_{j=1}^{\lceil n/m\rceil}C_j.$$

It is straightforward to see that

$$\text{COMP}(x_1,\cdots,x_n,y_1,\cdots,y_n)=\bigvee_{j=1}^{n}B_j.$$

The first layer of our circuit for the COMP function has $O(n/\log n)$ gates computing the C_i and $\tilde{C}_i$. With these computed values as inputs, the second layer has $O(n/\log n)$ gates each computing the B_j. Finally the output gate computes the OR ($\vee$) of all the B_j's. The total number of gates is $O(n/\log n)$.□

IV. Triangular Gates

A Boolean matrix is *strictly triangular* if the entries in each row and column forms a nondecreasing sequence. In a strictly triangular Boolean matrix, the sets of 1's and 0's resemble a (possibly truncated) triangle, hence the name. A matrix is *triangular* if its rows and columns can be permuted so that the resulting matrix is strictly triangular.

Lemma 2: A Boolean matrix is triangular if and only if it contains no 2 by 2 rectangle of the form

$$\begin{matrix}0&1\\1&0\end{matrix}\quad\text{or}\quad\begin{matrix}1&0\\0&1\end{matrix}$$

(recall that a rectangle need not be contiguous).

Proof: By definition of a triangular matrix, one can permute the rows and columns so that the resulting matrix is strictly triangular. On the other hand, it is easy to verify that no 2 by 2 rectangles of the above form can be obtained by permuting the rows and columns of a strictly triangular matrix. Thus a triangular matrix cannot contain 2 by 2 rectangles of the above form.

For the other direction, permute the rows so that the rows are arranged according to increasing number of 1's in each row. Then permute the columns so that the columns are arranged according to increasing number of 1's in each column. The resulting matrix is strictly triangular for if in some column a 1 appears above a 0, then, as the numbers of 1's does not decrease with the rows, there must be another column where in the same locations a 0 appears above a 1, contradicting the noncontainment assumption. □

Some properties of triangular matrices are apparent.

Corollary 2: 1) Every submatrix of a triangular matrix is triangular.

2) Every triangular matrix contains a constant rectangle of 1/4 the size.

3) Every submatrix of a triangular matrix contains a constant rectangle of 1/4 its size.

Proof: The first property follows directly from Lemma 2. To show the second property, permute the rows/columns until one obtains a strictly triangular matrix. Consider the midpoint (x, y). If the (x, y)th element of the matrix is 0, then the rectangle above and to the left of (x, y) is all 0, otherwise, the rectangle to the right and below (x, y) is all 1. The third property follows directly from the first two properties. □

An n-variable Boolean function f is *triangular* if $M_{f,X,Y}$ is triangular for *all* $\{X, Y\}$-partitions of the variables. A family of functions is triangular if all the functions in the family are. The definition applies to gates and families of gates via the underlying functions.

Example 3: Threshold gates (and in particular AND and OR gates) are triangular. We use Lemma 2 and show the result by contradiction. Let $f(X, Y) = \text{sgn}\left(\sum_{x_i \in X} u_i x_i + \sum_{y_i \in Y} v_i y_i\right)$ and suppose that it is not triangular. It follows from Lemma 2 that there exist $x, x' \in X$ and $y, y' \in Y$ such that $f(x, y) = f(x', y') = 1$ and that $f(x, y') = f(x', y) = 0$. Then $\sum u_i x_i + \sum v_i y_i > \sum u_i x_i + \sum v_i y_i'$ while $\sum u_i x_i' + \sum v_i y_i < \sum u_i x_i' + \sum v_i j_i'$. This leads to an obvious contradiction. □

Recall that $L_{f,X,Y}$ was defined to be the size of the largest f-constant $\{X, Y\}$-rectangle. Define L_f as

$$L_f = \min\{L_{f,X,Y} : \{X, Y\} \text{ partitions } \{z_1, \cdots, z_n\}\}.$$

Theorem 4: If a circuit consisting of k triangular gates computes a function f then

$$L_f \geq \frac{2^n}{4^k}.$$

Proof: As in Theorem 1, we label the gates in the circuit so that if $i < j$ then there is no directed path from the output of gate j to the input of gate i. Let g_j denote the function computed by gate j. We prove by induction on j that the vector-valued function $G_j = (g_1, g_2, \cdots, g_j)$ has $L_{G_j,X,Y} \geq 2^n/4^k$ for all variable partitions $\{X, Y\}$.

The induction basis holds by property 2) of Corollary 2 above. Suppose it holds for j, and consider the $(j+1)$st gate. Let $\{X, Y\}$ be a variable partition. By induction hypothesis, there is a G_j-constant $\{X, Y\}$-rectangle R of size $2^n/4^k$. Over R, the outputs of the first j gates are fixed, hence the input to the $(j+1)$st gate varies only with the original inputs. It follows that over R the $(j+1)$st gate coincides with a triangular function whose inputs are the original inputs. By property 3) of Corollary 2, there must be a subrectangle of R of size $\geq |R|/4$ over which the $(j+1)$st gate has a constant output. □

Corollary 3: For every function f and every family $\mathcal{G}$ of triangular gates,

$$C_{\mathcal{G}}(f) \geq \frac{n - \log L_f}{2}.$$ □

Example 4: Let $X = \{x_1, \cdots, x_{n/2}\}$ and $Y = \{y_1, \cdots, y_{n/2}\}$. It follows from a result of Lindsey (see [12]) that the largest IP-constant $\{X, Y\}$-rectangles are of size at most $2^{n/2}$. Hence, it follows from Corollary 3 that

$$C_{\mathcal{TH}}(\text{IP}) \geq \frac{n}{4}.$$ □

The bound on $C_{\mathcal{TH}}(\text{IP})$ is tight up to a constant factor. A simple depth-3 threshold circuit with polynomially bounded integer weights can compute IP using $3/4n + 1$ gates. In a sense, the depth-3 circuit is also depth-optimal, because it is shown in [5] that every depth-2 threshold circuit for IP has exponential size if the weights at the second layer are polynomially bounded integers. It is not known whether there is a polynomial-size depth-2 threshold circuit for IP when exponential weights are allowed at the second layer.

V. Miscellaneous Applications

We briefly discuss some applications of the results and techniques discussed in the previous sections to threshold circuit complexity, and circuit complexity with various gates.

Depth-Weight Tradeoffs in Threshold Circuits

Recent results [3] have shown that any depth-d threshold circuit (with arbitrary weights) can be simulated by a depth-$(d+1)$ threshold circuit of polynomially bounded integer weights with only a polynomial factor increase in size. However, no upper or lower bounds have been shown for the degree of this polynomial factor.

One can implement the n-variable EQ using only three threshold gates with arbitrary weights in depth-2. Yet Theorem 2 gave a lower bound of $\Omega(n/\log n)$ on the size of any threshold circuit (with polynomially bounded integer weights) for EQ. We therefore have:

Corollary 4: There are n-variable Boolean functions whose threshold circuits (with polynomially bounded integer weights) have size $\Omega(n/\log n)$ times larger than the size of their depth-2 threshold circuits with arbitrary weights. □

Weighted-Sum Gates

In our discussion, we often observed that the output gate of a given threshold circuit does not always require the $\text{sgn}(\cdot)$ function usually associated with a threshold gate. A gate that computes a linear combination $\sum w_i x_i$ of its inputs (without taking a threshold) is a *weighted-sum gate*. No explicit function is known that requires super-polynomial size when implemented by a depth-2 arbitrary-weight threshold circuit with a weighted-sum gate at the output. This is a weaker case of the more difficult open problem of proving that some given function requires super-polynomial size when implemented by a depth-2 arbitrary-weight threshold circuit (with a threshold allowed in the output gate). We prove a partial result regarding weighted-sum gates in the context of the Equality and other related functions.

As mentioned earlier, the n-variable EQ can be implemented by a depth-2 circuit consisting of two threshold gates with exponential weights in the first layer and a weighted-sum gate in the second layer. We show that any circuit for EQ that consists of threshold gates with polynomially bounded integer weights at the first layer and of a weighted-sum gate at the second layer (possibly with arbitrary real weights) has exponential size.

Theorem 5: Suppose that a depth-2 circuit consisting of $p(n)$-rectangular gates in the first layer and a weighted-

sum gate (possibly with arbitrary real weights) at the output computes the n-variable EQ. Then the size of the circuit is at least $2^{n/2}/p(n)$.

Proof: Let $g_1, \cdots, g_k$ be the output functions of the k gates in the first layer of the circuit. Consider the "natural" partition $X = \{x_1, \cdots, x_{n/2}\}$ and $Y = \{y_1, \cdots, y_{n/2}\}$ of the input variables. Note that for such a partition, the corresponding function matrix $M_{\mathrm{EQ,X,Y}} = I_{2^{n/2} \times 2^{n/2}}$. Since the output function is a weighted sum of g_i's, we have

$$M_{\mathrm{EQ,X,Y}} = \sum_{i=1}^{k} w_i M_{g_i,X,Y}.$$

By subadditivity of ranks,

$$\mathrm{rank}\,(M_{\mathrm{EQ,X,Y}}) \leq \sum_{i=1}^{k} \mathrm{rank}\,(M_{g_i,X,Y}).$$

But

$$\mathrm{rank}\,(M_{\mathrm{EQ,X,Y}}) = 2^{\frac{n}{2}}$$

and for all $i \in \{1, \cdots, k\}$,

$$p(n) \geq \rho_{g_i,X,Y} \geq \mathrm{rank}\,(M_{g_i,X,Y}).$$

The theorem follows immediately from the above observations. □

Corollary 5: Suppose that a depth-2 circuit consisting of threshold gates with polynomially bounded integer weights in the first layer and a weighted-sum gate (possibly with exponential weights) at the output, computes the n-variable EQ. Then the size of the circuit is $\Omega(2^{(n/2)-\epsilon})$ for every $\epsilon > 0$.

Proof: Example 2 implies that any threshold gate with weights bounded by $p(n)$ is $((n/2)+1)^2 p^2(n)$-rectangular. □

The above result holds for any function f, (e.g., COMPARISON) for which $\mathrm{rank}\,(M_{f,X,Y})$ is exponentially large for some partition $\{X, Y\}$ of the input variables.

VI. Concluding Remarks

Several problems remain unresolved.

1) The best lower bounds for $C_{\mathcal{SYM}}(\mathrm{EQ})$ and $C_{\mathcal{SYM}}(\mathrm{IP})$ are $\Omega(n/\log n)$ while the best upper bounds are linear.
2) Is there a depth-2 threshold circuit with polynomially bounded integer weights for COMP that meets the lower bound of $\Omega(n/\log n)$?
3) The set of polynomially-rectangular gates, introduced in Section III, includes the set of generalized symmetric gates. Are the two sets the same? Recently, in [15] (see also [16]), this question was resolved by showing that there is a polynomially rectangular function that is not generalized symmetric. Similarly the set of triangular gates, introduced in Section IV, includes the set of threshold gates. Are these sets the same?

Appendix
A Lower Bound on the Differential Dimension of Boolean Functions

Smolensky [10] used the differential dimension of Boolean functions to derive lower bounds on symmetric-circuit complexity. We now show that communication complexity arguments developed in this paper can be used to derive a lower bound on the differential dimension of Boolean functions.

Let S be a finite set of points in the n-dimensional complex vector space $\mathcal{C}^n$. Let V denote the space of functions from S to $\mathcal{C}$.

Differential Dimension: The differential dimension of an analytic function $g: \mathcal{C}^n \to \mathcal{C}$ over S is the dimension of the subspace of V spanned by the restrictions to S of g and all of its partial derivatives.

Since we are concerned with functions that interpolate Boolean functions, we assume without loss of generality that $S = \{0, 1\}^n$.

Differential Dimension of Boolean Functions: The differential dimension of a Boolean function $f: \{0, 1\}^n \to \{0, 1\}$ is the minimal differential dimension over $S = \{0, 1\}^n$ of any analytic function $g: \mathcal{C}^n \to \mathcal{C}$ that interpolates f.

Let $g: \mathcal{C}^n \to \mathcal{C}$ be an analytic function and let $v \in \mathcal{C}^n$. The *shifted* function g_v is defined by: $g_v(x) = g(x - v) \forall x \in \mathcal{C}^n$.

Proposition 1: ([10]) The subspace of V spanned by all the partial derivates of all orders of g restricted to S coincides with the subspace of V spanned by all the shifts of g restricted to S. □

Thus if g interpolates a given Boolean function f, then the dimension of the space spanned by the shifts g_v for all $v \in S = \{0, 1\}^n$ gives a lower bound on the differential dimension of g.

Any function g restricted to the set $S = \{0, 1\}^n$ can be viewed as a 2^n-dimensional vector in $\mathcal{C}^n$; each coordinate of the vector is the value of g at a distinct point in S. For any $v_i \in S$, we represent the shift g_{v_i} restricted to S as a 2^n-dimensional vector, and denote it as $g_{v_i,S}$. Then the dimension spanned by the shifts $g_{v_1}, g_{v_2}, \cdots, g_{v_k}$, $v_i \in S$, is the *rank* of the following $2^n \times k$ matrix:

$$[g_{v_1,S} g_{v_2,S} \cdots g_{v_k,S}].$$

Lemma 3: The differential dimension of a Boolean function f is $\Omega(r)$, where

$$r = \max\{\mathrm{rank}\,(M_{f,X,Y}) : \{X, Y\} \text{ partitions } \{z_1, \cdots, z_n\}\}.$$

Proof: Let $\{X, Y\}$ partition $\{x_1, \cdots, x_n\}$ and let $M_{f,X,Y}$ be the corresponding function matrix. Choose $k = \mathrm{rank}\,(M_{f,X,Y})$ linearly independent columns of M_{fXY}, and let $\{y_1, y_2, \cdots, y_k\}$ be the set of Y-inputs corresponding to the chosen columns. Let $g(x, y)$ interpolate f and consider the following k shifts: $g_{(0,-y_1)}, g_{(0,-y_2)}, \cdots, g_{(0,-y_k)}$. One can show the following for the shifts $g_{(0,-y_i)}$, restricted to $S = \{0, 1\}^r$:

1) $g_{(0,-y_i)}(x, 0) = g(x, y_i) = f(x, y_i)$, is known for every $x \in \{0, 1\}^X$ and the values of $g_{(0,-y_i)}(x, y)$ might be undetermined if $y \neq 0$;

2) If the entries of the vector $g_{(0,-y_i),S}$ are arranged so that the first $2^{|X|}$ entries correspond to $(x, 0) \in \{0, 1\}^n$, then in the following $2^n \times k$ matrix

$$Y_k = [g_{(0,-y_1),S} g_{(0,-y_2),S} \cdots g_{(0,-y_k),S}],$$

the submatrix defined by the first $2^{|X|}$ rows comprises the k linearly independent columns (corresponding to Y-inputs $(y_1, \cdots, y_k)$) chosen from $M_{f,X,Y}$.

Thus rank $(Y_k) = k$. Hence by Proposition 1, the differential dimension of any function g interpolating the Boolean function f is $\Omega(\text{rank}\,(M_{f,X,Y}))$. □

The above result implies, for example, that the differential dimensions of the n-variable EQ and COMP are $\Omega(2^{n/2})$.

ACKNOWLEDGMENT

The authors would like to thank A. Wigderson for helpful discussions and for pointing out the depth of optimal realization of the EQ function discussed in Theorem 2.

REFERENCES

[1] A. V. Aho, J. D. Ullman, and M. Yanakakis, "On notions of information transfer in VLSI circuits," in *Proc. 15th Annu. ACM Symp. Theory Comput.*, 1983.

[2] M. Furst, J. B. Saxe, and M. Sipser, "Parity circuits and the polynomial time hierarchy," in *Proc. 22nd Annu. Symp. Foundations Comput. Sci.*, 1981, pp. 260–270.

[3] M. Goldmann, J. Hoastad, and A. Razborov, "Majority gates vs. general weighted threshold gates," in *Proc. 7th Annu. Conf. Structure in Complexity Theory*, 1992.

[4] H. D. Gröger and G. Turán, "On linear decision trees computing boolean functions," in *Proc. ICALP*, J. L. Albert, B. Monien, M. R. Artalejo, Eds., 1991, pp. 707–718.

[5] A. Hajnal, W. Mass, P. Pudlák, M. Szegedy, and G. Turán, "Threshold circuits of bounded depth," in *Proc. 28th Annu. Symp. Foundations Comput. Sci.*, 1987, pp. 99–110.

[6] J. Hromkovic, "Linear lower bounds on unbounded fan-in Boolean circuits," *Inform. Processing Lett.*, vol. 21, pp. 71–74, 1985.

[7] K. Melhorn and E. M. Schmidt, "Las Vegas is better than determinism in VLSI and distributed computing," in *Proc. 14th Annu. ACM Symp. Theory Comput.*, 1982.

[8] A. A. Razborov, "Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$," in *Math. Notes of the Academy of Science of the USSR, 41:4*, 1987, pp. 333–338.

[9] K. Y. Siu and J. Bruck, "On the power of threshold circuits with small weights," *SIAM J. Discrete Math.* pp. 423–435, Aug. 1991.

[10] R. Smolensky, "On interpolation by analytical functions with special properties and some weak lower bounds on the size of circuits with symmetric gates," in *Proc. 31st Annu. Symp. Foundations Comput. Sci.*, 1990, pp 628–631.

[11] ———, "Algebraic methods in the theory of lower bounds for boolean circuit complexity," in *Proc. 19th Annu. ACM Symp. Theory Comput.*, 1987, pp 77–82.

[12] J. Spencer, *Ten Lectures on the Probabilistic Method*, SIAM, 1987.

[13] I. Wegener, *The Complexity of Boolean Functions.* New York: Wiley, 1987.

[14] A. C. Yao, "Some complexity questions related to distributive computing," in *Proc. 11th Annu. ACM Symp. Theory Comput.*, 1979, pp. 209–213.