GENERALIZED LOWER BOUNDS DERIVED FROM HASTAD'S MAIN LEMMA
(Revised Version)

by

SHLOMO MORAN
Technical Report #438
November 1986
GENERALIZED LOWER BOUNDS DERIVED FROM
HASTAD'S MAIN LEMMA

(Revised Version)

by

Shlomo Moran

Department of Computer Science, the
Technion, Haifa 32000, Israel.

ABSTRACT

In [H] it is proven, among other things, that the size of any depth $k$ circuit computing the parity or the majority function is $\Omega(2^{0.1(0.3^k)^{0.1}})$. In this note we generalize the proof given there to yield similar lower bounds for arbitrary symmetric functions of $\{0,1\}^n$. This improves results in [FKPS], where it was shown that the non-existence of polynomial-size, constant-depth circuits for the majority function implies the non-existence of such circuits for other symmetric functions.

\footnote{Part of this work was done while the author was at IBM Thomas J. Watson Research Center Yorktown Heights, NY 10598}
1. INTRODUCTION

Let $S$ be a subset of $\{0,1\}^n$. $S$ is symmetric if for every $w=(w(1),..,w(n)) \in \{0,1\}^n$ and for every permutation $\pi$ of $\{1,...,n\}$, $w$ is in $S$ iff $w'=\pi(w(1),..,w(n))$ is in $S$. An integer $j$ is a boundary of a symmetric set $S$ if $1^i0^{n-i}$ is in $S$ but $1^{i+1}0^{n-i+1}$ is not, where $i=j-1$ or $i=j+1$. We show that if $cn$ is a boundary of $S$, then the size of every depth $k$ circuit recognizing $S$ is at least $2^{n(0.6b\alpha)^{1+c}}$, where $b=\min\{c,1-c\}$. For $c=0.5$ this gives the lower bounds obtained by Hastad for the parity and majority functions [H]. The proof is based on certain properties of boundaries, which enable us to generalize Hastad's proof of the lower bound for the majority function to a proof of a similar lower bound for any symmetric set with a boundary $n/2$, and then to generalize this later bound to a bound for any symmetric set with a boundary $cn$ for arbitrary $c$. One application of this result is that if the size of any depth 2 circuit recognizing a symmetric set $S$ is $\Omega(2^{n^c})$ for some $0<c<0.5$, then the size of every depth $k$ circuit recognizing $S$ is $2^{\Omega(1-(c/\log c)^{1-c})}$. This later result might not hold for non-symmetric sets; as in [H] there are examples of sets which can be recognized by a depth $k$ circuit of polynomial size, but require exponential size on depth $k-1$ circuits.

Related Results: The first to prove super-polynomial lower bounds on the size of constant depth circuits for the majority function were Furst et al. in [FSS]. Their results were later improved by Yao [Y] and Hastad [H]. Fagin et al. had shown in [FKPS] that the results in [FSS] imply super polynomial lower bound on the size of constant depth circuits for other symmetric sets (see also [DGS]). Using our terminology, the result in [FKPS] that is related to this paper can be formulated as follows: Let a polynomial $p$, an integer $d$ and an $\varepsilon>0$ be given. Then for all sufficiently large $n$, a subset of $\{0,1\}^n$ which has a boundary in the interval $[n^d,n-n^d]$ cannot be recognized by a $d$-depth, $p(n)$-size circuit. By incorporating the results of [Y] or [H] in [FKPS], it is possible to show that for any unbounded function $\alpha(n)$, for every polynomial $p$, for every constant $d$ and for all sufficiently large $n$, no $d$-depth, $p(n)$-size circuit can recognize a subset of $\{0,1\}^n$ which has a boundary in $[(\log n)^{\alpha(n)},n-(\log n)^{\alpha(n)}]$. This provides a full characterization of the symmetric functions that cannot be computed by constant-depth, polynomial-size circuits.

The above mentioned result in [FKPS] is proved there by showing that the existence of a circuit contradicting it implies a circuit of depth $d+1$ and size $q(n)$ computing the majority function on $\{0,1\}^n$, where $q$ is a polynomial depending on $p$, and $\delta$ is a constant which depends on both $d$ and $\varepsilon$; the existence of this latter circuit contradicts the result in [FSS], which implies the result.

Our technique differs from the one in [FKPS] in that we directly generalize the proof of the lower bound for the majority function given in [H] to a similar proof for arbitrary symmetric function. Consequently, the bounds
In this section we formally define boundaries of symmetric sets, and prove their properties.

Definition: Let $S$ be a symmetric subset of $(0,1)^n$. An integer $j \in \{0, n-1\}$ is a left boundary of $S$ if $j$ is in $\text{CH}(S)$ but $j-1$ is not. An integer $j \in \{0, n-1\}$ is a right boundary of $S$ if $j+1$ is in $\text{CH}(S)$ but $j+1$ is not. $j$ is a boundary of $S$ if it is either right or left boundary of $S$.

Examples: For the parity function, all even $j$'s between 0 and $n$ are boundaries. The majority function has only one (left) boundary, namely $n/2$.

Lemma 1: Let $\rho$ be a restriction satisfying $|\rho^{-1}(\ast)|=m$ and $|\rho^{-1}(1)|=l$, and let $S$ be a symmetric subset of $(0,1)^n$. Then $S'=\{S \mid \rho\}$ is a symmetric subset of $(0,1)^m$, and for each $j \in \{0, l-1\}$, $j$ is a right boundary of $S'$ iff $j+l$ is a right boundary of $S$.

Proof: For simplicity, assume that $\rho(x_1)=\cdots=\rho(x_m)=\ast$ (and $\rho(x_i)\in \{0,1\}$ for $m<i\leq n$). Consider a string
If \( w' = (w(1), \ldots, w(m)) \) is in \( \{0, 1\}^m \). Then \( w' \) is in \( S' \) iff \( w = (w(1), \ldots, w(m), \rho(x_{m+1}), \ldots, \rho(x_n)) \) is in \( S \). By the symmetry of \( S \), \( w \) is in \( S \) iff every permutation \( \pi \) of \( \{1, \ldots, m\} \), \( w_{\pi} = (w(\pi(1)), \ldots, w(\pi(m)), \rho(x_{m+1}), \ldots, \rho(x_n)) \) is in \( S \). This implies that \( S' \) is symmetric. The proof is completed by noting that, by the symmetry of \( S' \) and \( S' \), \( w_{m,j} \) is in \( S' \) iff \( w_{n,j+1} \) is in \( S \), for \( j = 0, \ldots, m \).

Corollary: Assume that in the above lemma \( |\rho^{-1}(1)| = |\rho^{-1}(0)| \) (that is, \( l = (n - m)/2 \)). Then \( n/2 \) is a boundary of \( S \) iff \( m/2 \) is a boundary for \( S' \).

Lemma 2. If \( j \) is a boundary of \( S \), then every depth-2 circuit recognizing \( S \) has gates of bottom fan-in at least \( \min(j, n-j) \).

Proof: Consider first an OR of ANDs circuit, \( C \), that accepts \( S \). Let \( j \) be a left boundary of \( S \). Then \( w_{n,j} = 1^{\left\lfloor n/2 \right\rfloor} \) is in \( S \), and hence \( C \) has an AND gate \( G(w_{n,j}) \) that accepts (outputs 1) on \( w_{n,j} \). We claim that for \( i = 1, \ldots, j \), \( G(w_{n,j}) \) must have the literal \( x_i \) as an input: Otherwise, \( G(w_{n,j}) \) will accept also the word \( w' = 1^{j-i}0^{j-i}1^{n-j} \). But \( w' \) is a permutation of \( w_{n,j-1} = 1^{j-i}0^{n-j+1} \), contradicting the assumption that \( j \) is a left boundary of \( S \). Thus, we conclude that if \( j \) is a left boundary of \( S \) then the fan-in of \( G(w_{n,j}) \) is at least \( j \). Similarly, if \( j \) is a right boundary of \( S \) then \( G(w_{n,j}) \) must have an input literal \( x_i \) for \( i = j+1, \ldots, n \), and hence it has a fan-in at least \( n-j \).

Let now \( C \) be an AND of ORs circuit accepting \( S \). Then the OR of ANDs circuit \( C' \) obtained from \( C \) by interchanging AND and OR gates and replacing literals by their negations accepts the complement of \( S \), \( COM(S) \). Clearly, it is sufficient to prove the lemma for \( C' \). Let \( j \) be a left boundary of \( S \). Then \( j-1 \) is a right boundary of \( COM(S) \), and hence it corresponds to a gate with a bottom fan-in \( \geq n-j+1 \) in \( C' \). Similarly, if \( j \) is a right boundary of \( S \) then \( j+1 \) is a left boundary of \( COM(S) \), and hence it corresponds to a gate of fan-in \( \geq j+1 \) in \( C' \). We conclude that if \( j \) is a left boundary of \( S \) it requires a fan-in of \( \min(j, n-j+1) \) in either kind of circuit, and if \( j \) is a right boundary of \( S \) it requires a fan-in of \( \min(n-j, j+1) \) in either kind of circuit. The lemma follows.

3. LOWER BOUNDS FOR SYMMETRIC FUNCTIONS

Theorem 1: Let \( S \) be a symmetric subset of \( \{0, 1\}^n \), and assume that \( n/2 \) is a boundary of \( S \). Then every depth-\( k \) circuit recognizing \( S \) is of size \( \Omega(2^{0.1(0.3n)^{\omega-3}}) \), for \( k \leq \log n (\log \log n + D) \) for some constant \( D \).

Proof: The proof is similar to the proof of the lower bound for the majority function given in [H]: The base \( k = 2 \) is by Lemma 2, and the induction step is carried out by considering random restrictions \( \rho \) that satisfy \( |\rho^{-1}(1)| = |\rho^{-1}(0)| \) and using the corollary to Lemma 1. The full proof is given in the appendix.

Let \( B(S) \) be the set of boundaries of a symmetric set \( S \subseteq \{0, 1\}^n \). \( b(S) \) is the integer defined by:

\[
b(S) = \max_{j \in B(S)} \min(j, n-j).
\]
The next theorem implied that $b(S)$ is closely related to the size of depth $k$ circuits recognizing $S$.

**Theorem 2:** Let $S$ be a symmetric subset of $\{0,1\}^n$, and let $b(S)/n=b$ for some $0<b\leq 0.5$. Then every depth $k$ circuit recognizing $S$ is of size $\Omega(2^{0.1(0.6b)n^{k-1}})$.

**Note:** By substituting $b=0.5$ in the above Theorem we get the lower bounds for the parity and majority functions in [H].

**Proof:** By the definition of $b(S)$, either $bn$ or $n-bn$ is a boundary of $S$. We prove the theorem for the case that $bn$ is a boundary of $S$. The proof of the other case is similar.

Let $p_0$ be the restriction satisfying $p_0(x_i)=1$ for $1\leq i\leq 2bn$ and $p_0(x_i)=0$ otherwise. Then by Lemma 1 $S'=S|_{p_0}$ is a symmetric subset of $\{0,1\}^m$ for $m=2bn$, and $m\leq bn$ is a boundary of $S'$. This implies that every depth $k$ circuit $C$ recognizing $S$ contains a subcircuit $C'=C|_{p_0}$ of depth $k$ recognizing a set $S'$ over $2bn$ variables satisfying the condition of Theorem 1. The Theorem follows by substitution.

The next lemma shows that, in a certain sense, the converse of Theorem 2 is also true.

**Lemma 3** If the size of every depth $\geq 2$ circuit recognizing $S$ is at least $2^{cn}$ for some constant $0<c\leq 0.5$, then $b(S)/n>\geq c(2\log c)$.

**Proof:** Let $b(S)/n=b$. If $b\geq 1/3$ then, since $c<0.5$, we are done. So we may assume that $b\leq 1/3$.

By the definition of $b(S)$, $S$ has no boundaries greater than $bn$ or smaller than $n-bn$. This means that either $S$ or $\text{COM}(S)$ does not contain permutations of $w_{a,j}$ for $bn<j<n-bn$. The total number of permutations of $w_{a,j}$ for $0\leq j\leq bn$ is $\sum_{i=0}^{bn} \binom{n}{i}$. Since $b\leq 1/3$, we have that for $i\leq bn$ it holds that $\binom{n}{i}\geq 2\binom{n}{i-1}$. Hence the sum above is dominated by the sum of the geometric series with ratio 0.5 and largest element $\binom{n}{bn}$, and hence by $2\binom{n}{bn}$. By symmetry, the number of permutations of $w_{a,j}$ for $n-bn\leq j\leq n$ is bounded by the same bound. Thus we have that either $S$ or $\text{COM}(S)$ is of cardinality $M=4\binom{n}{bn}$, and hence $S$ can be accepted by a depth 2 circuit of size $M$ (one bottom gate per each word in $S$ or per each word in $\text{COM}(S)$). Thus we have that for almost all $n$,

$$2^{cn}\leq M=4\binom{n}{bn}=\frac{4}{(b^n(1-b)^n)^n\sqrt{2\pi b(1-b)n}}<((b^{-b}(1-b)^{1-b})^n<2^{2b\log(1/b)n}$$

(the = sign is by Stirling formula, and the last inequality follows by the fact that $b\leq 1/3$, and hence $(1-b)^{-b}b^b$).

Thus, we get that $c<2b\log(1/b)$, which implies the lemma.

In [H] it is shown that there are sets that can be recognized by a polynomial size depth-$k$ circuits but require exponential size for depth $k-1$ circuits. Our last result implies that such a set cannot be symmetric.

**Theorem 3:** Let $S$ be a symmetric subset of $\{0,1\}^n$. Then if the size of every depth 2 circuit recognizing $S$ is at least
We need few more definitions before presenting the proof of the above theorem. A logical formula in CNF is

\[ b(S) \geq \frac{-c}{2 \log c} n. \]

The theorem follows by substituting this \( b(S) \) in Theorem 2. ☐

References

APPENDIX: PROOF OF THEOREM 1
Theorem 1: Let \( S \) be a symmetric subset of \((0,1)^n\), and assume that \( n/2 \) is a boundary of \( S \). Then every depth \( k \) circuit recognizing \( S \) is of size \( \Omega(2^{0.1(n^0.32\log n)}) \), for \( k \leq \log n / \log \log n + D \) for some constant \( D \).

We need few more definitions before presenting the proof of the above theorem. A logical formula in CNF is a depth 2 AND of OR’s Boolean circuit. A minterm of a logical formula \( G \) is a minimal set of literals such that assigning the value 1 to each of them fixes the value of \( G \) to 1. The size of a minterm is the number of literals in it. Since a Boolean function can be written as the Boolean sum of its minterms, the maximum size of a minterm of a formula is the maximum bottom fan-in in a depth 2 OR of AND’s circuit computing \( G \).

Let \( G \) be a logical formula in CNF and let \( p \) be a random restriction. \( G \mid p \) denotes the formula resulted from \( G \) by applying \( p \), and \( \min(G \mid p) \geq s \) denotes the event that this formula contains a minterm of size at least \( s \).

Next we state the Main Lemma of [H], which is the main tool used in the proof of Theorem 1.

Main Lemma [H]: For an integer \( t \geq 1 \) and a probability \( p \), let \( \alpha_{t,p} \) be the positive root of the equation:

\[ \left( \frac{4p}{(1+p)\alpha_{t,p}} \right)^t = \left( \frac{2p}{(1+p)\alpha_{t,p}} \right)^{t+1} + 1. \]

Then for each formula \( G \) in CNF with bottom fan-in \( \leq t \) and for each integer \( s \) it holds that:

\[ p_r [\min(G \mid p) \geq s] < \alpha_{t,p}. \]

For each \( t \), let \( p_t \) be defined by \( \alpha_{t,p_t} = 0.5 \). For large \( t \), \( p_t = \frac{\ln \Phi}{4t} \), where \( \Phi \) is the golden ratio. In particular, \( p_t > 0.1/t \).

As in [H], we prove first a theorem that is slightly weaker than Theorem 1.

Theorem 1A: Let \( S \) be a symmetric subset of \((0,1)^n\), and assume that \( n/2 \) is a boundary of \( S \). Then there are no circuits of depth \( k \) and at most \( 2^{0.1n^{0.32}(k-1)} \) gates of depth at least \( 2 \) and bottom fan-in at most \( 0.1n^{0.32}(k-1) \) that accept
$S$, for $k \leq \log_{n}(\log_{n} \log_{n} + D)$ for some constant $D$.

**Proof.** Induction on $k$. For $k = 2$ use Lemma 2 with $j = n/2$.

Induction step: For contradiction, let $k$ be the minimal integer such that there are circuits of depth $k$ and $n$ input variables contradicting the theorem (for some $D$, to become clear later), and let $C$ be such a circuit. WLG assume that the bottom gates of $C$ are OR gates. Consider a random restriction $\rho$ of probability $p = n^{-1/(k-1)}$ on the variables of $C$. First we show that with probability $\geq 1/n$ we have that $|\rho^{-1}(\ast)|$ is large and $|\rho^{-1}(1)| = |\rho^{-1}(0)|$:

The expected size of $\rho^{-1}(\ast)$ is $n^{(k-2)/(k-1)}$, and with probability greater than $1/3$ it is at least this number. Also, by Stirling formula,

\[
\Pr[|\rho^{-1}(1)| = |\rho^{-1}(0)|] = \Pr[\text{a binary string of length } n \text{ has an equal number of 0's and 1's}] = \frac{1}{\sqrt{2\pi n}}. 
\]

This implies that

\[
\Pr[|\rho^{-1}(1)| = |\rho^{-1}(0)| \geq 2\sqrt{n^{(k-2)/(k-1)}}] \geq 3/n 
\]

for almost all $n$.

Hence, the probability that $|\rho^{-1}(\ast)| \geq 2\sqrt{n^{(k-2)/(k-1)}}$ and $|\rho^{-1}(1)| = |\rho^{-1}(0)|$ is greater than $1/n$ for almost all $n$ (or, for all $n$ satisfying $\log_{n}(\log_{n} \log_{n} + D) \geq k \geq 3$ for some $D$).

Next we show that the probability that $C \mid \rho$ contain a depth 2 gate which has a minterm larger than $0.1 n^{1/(k-1)}$ is smaller than $1/n$, by using the main lemma of [H]. For this, Let $\epsilon = 0.1 n^{1/(k-1)}$. Then $p = 0.1/n < \epsilon$, and hence the probability that a given depth 2 gate in $C \mid \rho$ has a minterm larger than $\epsilon$ is smaller than $\alpha$, for some $\alpha < 0.5$. In particular, the probability that $C \mid \rho$ contains any depth 2 gate that has such a minterm is smaller than $2\alpha$ such gates. Since $2\alpha < 1$, we have that this probability is smaller than $1/n$, provided that $k \leq \log_{n}(\log_{n} + D)$ for some $D$.

Thus, there is a $\rho$ for which $|\rho^{-1}(\ast)| \geq n^{(k-2)/(k-1)}$, $|\rho^{-1}(1)| = |\rho^{-1}(0)|$ and the depth 2 gates of $C \mid \rho$ have no minterms larger than $\epsilon$. This means that each of these gates can be written as OR of ANDs of bottom fan-in $\leq \epsilon$. By doing this, we obtain a circuit $C'$ of depth $k-1$ over $m \geq n^{(k-2)/(k-1)}$ inputs with at most $2^{\epsilon}$ gates of depth at least 2 and bottom fan-in at most $\epsilon$, where $\epsilon = 0.1 n^{1/(k-1)} < 0.1 n^{1/(k-2)}$. By the corollary to Lemma 1, the set $S \mid \rho$ accepted by $C'$ is a symmetric subset of $\{0,1\}^m$ with a boundary $m/2$. Also, since $k \leq \log_{n}(\log_{n} + D)$, we have that $k-1 \leq \log_{n}(\log_{n} + D)$. Thus $C'$ contradicts the minimality of $k$.

*Proof of Theorem 1.* Assume that there is a depth-$k$ circuit contradicting the theorem, and consider it as a circuit of depth $k+1$ and bottom fan-in 1. Apply to it a random restriction with $p = 0.3$, and observe that $\alpha_{1,p} = 2p/(1+p)$, hence $\alpha_{1,0.3} < 0.5$. By arguments similar to those in the proof of Theorem 1A we see that there is a random restriction on this circuit which implies the existence of a circuit that contradicts Theorem 1A.