# TOP-DOWN LOWER BOUNDS FOR DEPTH-THREE CIRCUITS

J. Håstad, S. Jukna and P. Pudlák

**Abstract.** We present a top-down lower bound method for depth-three $\wedge, \vee, \neg$-circuits which is simpler than the previous methods and in some cases gives better lower bounds. In particular, we prove that depth-three $\wedge, \vee, \neg$-circuits that compute parity (or majority) require size at least $2^{0.618...\sqrt{n}}$ (or $2^{0.849...\sqrt{n}}$, respectively). This is the first simple proof of a strong lower bound by a top-down argument for non-monotone circuits.

**Key words.** Computational complexity; small-depth circuits.

**Subject classifications.** 68Q25.



## 1. Introduction

To prove lower bounds in various computational models is still one of the major challenges in complexity theory. In spite of some recent progress, there are still no strong lower bounds for general Boolean circuits. Even worse, there is not even any well defined line of attack of this problem where the hope of progress is substantial and well founded. In view of this situation, it is crucial to get a better understanding of existing techniques for proving lower bounds and in particular, to understand exactly in what situation a particular technique might be used and how the bounds obtained by one method relate to bounds obtained by another method.

In this paper, we will be concerned with a special case of the general problem about the tradeoff between the size and depth of circuits with $\wedge, \vee, \neg$

gates, namely we shall study the size of depth-three circuits. The technique we shall use has two sources. The first one is a "finite" version of the topological approach proposed by Sipser (1985). Given a shallow circuit for a boolean function $f$, the idea is to combine rejecting computations on inputs in $f^{-1}(0)$ into an incorrect rejecting computation on an input in $f^{-1}(1)$. This incorrect rejecting computation is obtained as a "limit" of correct ones.

The second one, introduced by Karchmer and Wigderson (1990), is based on the fact that the circuit depth is equivalent to the number of bits needed to be exchanged to solve a particular combinatorial game. Both proof techniques correspond in a natural way to a top-down argument for circuits. Such top-down arguments have been successfully applied to usual (fan-in 2) monotone circuits (Karchmer & Wigderson 1990, Raz & Wigderson 1990) and to bounded depth (unbounded fan-in) monotone circuits (Klawe *et al.* 1984). Here, we shall apply such an argument to nonmonotone bounded depth circuits.

There have been a number of results for small-depth circuits (Ajtai 1983, Furst *et al.* 1984, Yao 1985, Håstad 1989, Razborov 1987, Smolensky 1987), where superpolynomial and exponential lower bounds on circuit size have been proved for simple Boolean functions like parity and majority. Nontrivial results have been obtained for circuits of depth up to $\Omega(\log n/\log\log n)$ (Håstad 1989, Razborov 1987, Smolensky 1987). All those papers have used essentially bottom-up arguments, i.e., starting at the inputs and analyzing the circuit level by level. When switching to a top-down argument, we improve the results for circuits of depth three. The bounds we get are stronger (only the constant changes in most cases, but some of the old results were tight up to the value of the constant), and the argument is simple in that it only uses more or less standard combinatorics. Our results are only the first step in this direction. It would be of great value if the top-down approach could be extended to greater depth, or if one could prove a lower bound larger than $2^{const\cdot\sqrt{n}}$ for depth three.

The paper is organized as follows: In Section 2, we establish the basic connections between circuits and the combinatorial problem we analyze. Our presentation will be based on limits, but the reader should bear in mind that there is an equivalent game-theoretical interpretation. In Section 3, we prove lower bounds for depth-three circuits computing parity and majority. These bounds give better values for the constant in the exponent than bounds obtained by previous methods. In Section 4, we improve the bounds on the cost of switching from a $\Sigma_3$-circuit to a $\Pi_3$-circuit. These bounds constitute an improvement also in the asymptotic dependence. We end in Section 5 with a number of open problems.

## 2. Circuits and limits

A $\Pi_d^{\ell,k}$-*circuit* (resp. a $\Sigma_d^{\ell,k}$-*circuit*) is a depth-$d$ unbounded fan-in circuit $C$ over $\{\wedge,\vee\}$ of size $\ell$ with the top gate $\wedge$ (resp. $\vee$) and with bottom fan-in bounded by $k$, i.e., each gate next to the bottom has at most $k$ inputs. As usual, we assume that literals (inputs or negated inputs) are at the bottom and that each level consists of the same type of gate. We also say that $C$ is a $\Pi_d^{\ell,k+}$-*circuit* if each gate next to the bottom has at most $k$ negated inputs (the total number of inputs to the gate may be $n$).

We will be particularly interested in $\Pi_3$-circuits. (Note that both parity and majority are selfdual if the number of inputs $n$ is odd, thus our lower bounds hold also for $\Sigma_3$-circuits.) The behavior of such circuits can be described in purely combinatorial terms using the following notion of "limit vectors" introduced by Sipser (1985, 1991). Our modification "lower limit" is a technical concept which enables us to get better constants in lower bounds. We shall use the following notation: $[n]=\{1,\dots,n\}$ and $[n]^k=\{S\subseteq[n]\,:\,|S|=k\}$. Also, we let $x|_S$ denote the restriction of $x$ to the set $S$ for vectors $x\in\{0,1\}^n$ and $S\subseteq[n]$.

DEFINITION 2.1. *Let $B\subseteq\{0,1\}^n$ be a set of vectors. A vector $y\in\{0,1\}^n$ is a* $k$-limit *for a set $B$ if, for any subset of indices $S\in[n]^k$, there exists a vector $x\in B$ such that $x\neq y$ and $y|_S=x|_S$. If $x>y$ instead of $x\neq y$, we call $y$ a* lower $k$-limit *for $B$.*

We say that the pair $(A,B)$ of subsets of $\{0,1\}^n$ has the property $P(k,\ell)$ if, for any coloring of $B$ by $\ell$ colors, there is a color class $B'\subseteq B$ such that the set $A$ contains at least one $k$-limit for $B'$. If the same holds with "$k$-limit" replaced by "lower $k$-limit", then we say that $(A,B)$ has the property $P^+(k,\ell)$. We also say that a circuit $C$ *separates* the pair $(A,B)$ if $C$ computes 1 (resp. 0) on inputs from $A$ (resp. $B$). The following lemma is essentially due to Sipser.

LEMMA 2.2. *Let $A,B\subseteq\{0,1\}^n$, $A\cap B=\emptyset$. If the pair $(A,B)$ has the property $P(k,\ell)$, then it cannot be separated by a $\Pi_3^{\ell,k}$-circuit. If, moreover, the pair has the property $P^+(k,\ell)$, then it also cannot be separated by a $\Pi_3^{\ell,k+}$-circuit.*

PROOF. Let $C$ be a $\Pi_3^{\ell,k}$-circuit separating $(A,B)$. Then, the $\vee$-gates $g_i$ $(i\leq\ell)$ feeding into the top gate of $C$ separate pairs $(A,B_i)$ so that $\cup_{i=1}^{\ell}B_i=B$.

Suppose the pair $(A, B)$ has the property $P(k, \ell)$. Then, for some $i_0 \leq \ell$, the set $A$ contains a vector $y$ which is a $k$-limit for the set $B_{i_0}$. The gate $g_{i_0}$ must reject all $x \in B_{i_0}$. We show that in this case $g_{i_0}$, and hence the whole circuit $C$, is forced to incorrectly reject the limit $y$. Let $\mathcal{F}$ be the family consisting of the sets of indices of inputs to the $\wedge$-gates feeding into $g_{i_0}$. Since $g_{i_0}$ is an $\vee$-gate, we know that all these $\wedge$-gates compute 0 on all $x \in B_{i_0}$. Since sets in $\mathcal{F}$ are of cardinality at most $k$ and $y$ is a $k$-limit for $B_{i_0}$, we also have that on each $S \in \mathcal{F}$, the vector $y$ coincides with at least one vector $x_S \in B_{i_0}$. Therefore, every $\wedge$-gate feeding into $g_{i_0}$ must compute 0 on $y$ also, and thus, $g_{i_0}(y) = 0$, a contradiction.

To prove the second claim, it is enough to take $\mathcal{F}$ to be the family consisting of the sets of indices of negated inputs, and use the additional property $x_S \geq y$. Take an $\wedge$-gate $h$ feeding into $g_{i_0}$, and let $S$ be the corresponding set of negated inputs to $h$. We know that $y$ coincides on these inputs with some vector $x_S$ for which $h(x_S) = 0$. If some negated variable feeding in $h$ computes 0 on $x_S$, then it does the same on $y$, and hence, $h(y) = 0$. Otherwise, the 0 is produced on $x_S$ by some not negated variable. Since $y \leq x_S$, this variable must produce 0 on $y$ also, and hence, $h(y) = 0$. $\square$

Now we can explain our method. Suppose a function $f$ can be computed by a $\Pi_3$-circuit $C$.

1. First, we apply a restriction to reduce the bottom fan-in of the circuit $C$.
2. Then, we prove the existence of a limit in $A = \{x : f(x) = 1\}$ for every sufficiently large subset of $B = \{x : f(x) = 0\}$ and apply Lemma 2.2.

The reduction of the bottom fan-in is quite standard. For now, let us point out that it is not necessary to use *random* restrictions (see Lemma 3.2), and that both the restriction and the limit can be found by deterministic methods. Thus, the whole method avoids randomness.

It turns out that there is a classical result in combinatorics which can be used to prove the existence of a (lower) limit. It is convenient now to switch to set-theoretical language, namely, from now on we look at a vector $x \in \{0,1\}^n$ as the corresponding subset $X = \{i : x_i = 1\}$ of $[n]$. A *cover* of a family of sets $\mathcal{F}$ is a set which intersects every member of $\mathcal{F}$. The minimum cardinality of a cover is denoted by $\tau(\mathcal{F})$. For a set $Y$ and a family of sets $\mathcal{F}$, let

$$\mathcal{F}_Y = \{X \setminus Y : X \in \mathcal{F},\, X \supseteq Y\},$$

and let $\mathcal{F} \triangle Y$ denote the family of all symmetric differences $(X \setminus Y) \cup (Y \setminus X)$ for $X \in \mathcal{F}$. In these terms, a set $Y$ is a $k$-limit for $\mathcal{F}$ iff $\tau(\mathcal{F} \triangle Y) \geq k+1$, and a lower $k$-limit iff $\tau(\mathcal{F}_Y) \geq k+1$.

Recall that a family of sets $X_1, \ldots, X_{k+1}$ is *a sunflower with* $(k+1)$ *petals and core* $Y$ if, for every $i \neq j$, $X_i \cap X_j = Y$. Clearly, if $\mathcal{F}$ has such a sunflower, then $\tau(\mathcal{F}_Y) \geq k$, i.e., the core $Y$ is a lower $(k-1)$-limit for $\mathcal{F}$.

THEOREM 2.3. (ERDÖS & RADO 1960) *Let $\mathcal{F}$ be a family with more than $s!(k-1)^s$ sets of cardinality $s$. Then $\mathcal{F}$ contains a sunflower with $k$ petals.*

This theorem can be directly applied to get a bound of $2^{\Omega(n^{1/3})}$ for the majority function. Its proof can be easily modified to get the following theorem which gives the same bound for the parity function.

THEOREM 2.4. *Let $s \geq 2$ be an even (resp. odd) integer and let $\mathcal{F}$ be a family with more than $n^{s/2}k^{s/2} \cdot \frac{1\cdot 3\cdots(s-1)}{2\cdot 4\cdots s}$ (resp. more than $n^{(s-1)/2}k^{(s+1)/2} \cdot \frac{1\cdot 3\cdots s}{2\cdot 4\cdots(s-1)}$) sets of cardinality $s$. Then $\mathcal{F}$ contains a sunflower with $k+1$ petals and with an odd (resp. even) core.*

In order to get bounds closer to the optimal ones, one needs to consider limits. The proof of the existence of limits given below is very similar to the proofs of the above Theorems 2.3 and 2.4. Therefore, we leave out the proof of Theorem 2.4.

## 3. The lower bound for parity and majority

Let $F(n,k,s)$ denote the function defined by

$$F(n,k,s) = \begin{cases} \frac{n^{s/2}k^{s/2}}{2\cdot 4\cdots s} & \text{if } s \text{ is even} \\ \frac{n^{(s-1)/2}k^{(s+1)/2}}{2\cdot 4\cdots(s-1)} & \text{if } s \text{ is odd.} \end{cases}$$

LEMMA 3.1. *Let $\mathcal{F}$ be a family of $s$-element subsets of $[n]$, $s \geq 2$ , and suppose that $|\mathcal{F}| > F(n,k,s)$. Then, there exists a lower $k$-limit $Y \subseteq [n]$ for $\mathcal{F}$ such that $|Y| \equiv s+1 \bmod 2$.*

PROOF. Using the discussion in the previous section, we just need to find a set $Y$ of the desired parity such that $\tau(\mathcal{F}_Y) \geq k+1$. The basis $s = 2$ is trivial. In this case, $\mathcal{F}$ is the ordinary graph with more than $F(n,k,2) = kn/2$ edges, and hence, it contains a vertex of degree at least $k+1$.

Suppose now that the lemma is true for $s$ and prove it for $s+1$. Take a family $\mathcal{F}$ of $(s+1)$-element subsets of $[n]$ with $|\mathcal{F}| > F(n,k,s+1)$. For $x \in [n]$, let $\mathcal{F}_x = \{X : x \in X \in \mathcal{F}\}$.

**Case 1**: $s+1$ is odd ($s$ is even). If $\tau(\mathcal{F}) \geq k+1$, we are done since we can take $Y = \emptyset$ (which is even). Otherwise, there exists an $x \in [n]$ for which the following relations hold:

$$|\mathcal{F}_x| \geq \frac{|\mathcal{F}|}{k} > \frac{F(n,k,s+1)}{k} = \frac{1}{k} \cdot \frac{n^{s/2} k^{(s+2)/2}}{2 \cdot 4 \cdots s} = F(n,k,s).$$

The family $\mathcal{F}_x$ consists of even sets and by induction, $\tau\left((\mathcal{F}_x)_{Y'}\right) \geq k+1$ for some odd $Y'$. Thus, $\tau(\mathcal{F}_Y) \geq k+1$ where $Y = Y' \cup \{x\}$ is even.

**Case 2**: $s+1$ is even ($s$ is odd). There exists an $x \in [n]$ which is contained in at least $(s+1)|\mathcal{F}|/n$ sets of $\mathcal{F}$. For this $x$, we have the following relations:

$$|\mathcal{F}_x| > \frac{(s+1)F(n,k,s+1)}{n} = \frac{(s+1)}{n} \cdot \frac{n^{(s+1)/2} k^{(s+1)/2}}{2 \cdot 4 \cdots (s-1)(s+1)} = F(n,k,s).$$

The family $\mathcal{F}_x$ consists of odd sets and by induction, $\tau\left((\mathcal{F}_x)_{Y'}\right) \geq k+1$ for some even $Y'$. Thus, $\tau(\mathcal{F}_Y) \geq k+1$ where $Y = Y' \cup \{x\}$ is odd. □

The following lemma will be used to reduce the bottom fan-in.

LEMMA 3.2. *Let $k, \ell$ be positive integers. Let $\mathcal{F}$ be a family of $\ell$ subsets of $[n]$ each of cardinality more than $k$. Suppose that the following inequality holds:*

$$\ell < \left(\frac{n+1}{m+1}\right)^k. \tag{3.1}$$

*Then, there exists a subset $T \subseteq [n]$ such that $|T| \leq n-m$ and $T$ intersects every set in $\mathcal{F}$.*

PROOF. We construct the set $T$ via the following "greedy" procedure. Let $\mathcal{F}^1 = \mathcal{F}$. For each $i$, $1 \leq i \leq n-m$, include in $T$ the element $x_i \in [n]$ which occurs in the largest number of sets of $\mathcal{F}^i$, then remove all the sets containing $x_i$ from $\mathcal{F}^i$ to obtain $\mathcal{F}^{i+1}$. Sets deleted after $i$ steps intersect the set $\{x_1, \ldots, x_i\}$. The size of $\mathcal{F}^i$ is bounded from above by

$$|\mathcal{F}^1| \left(1 - \frac{k}{n}\right)\left(1 - \frac{k}{n-1}\right) \cdots \left(1 - \frac{k}{n-i+2}\right).$$

We need to show that the bound is less than 1 for $i = n - m + 1$. This follows from the following estimate

$$\begin{aligned}
& \left(1-\frac{k}{n}\right)\left(1-\frac{k}{n-1}\right)\cdots\left(1-\frac{k}{n-(n-m+1)+2}\right) \\
= \;& \left(1-\frac{k}{n}\right)\left(1-\frac{k}{n-1}\right)\cdots\left(1-\frac{k}{m+1}\right) \\
\leq \;& e^{-\frac{k}{n}-\frac{k}{n-1}-\ldots-\frac{k}{m+1}} \leq e^{-k(\ln(n+1)-\ln(m+1))} \\
= \;& \left(\frac{n+1}{m+1}\right)^{-k}. \quad \square
\end{aligned}$$

THEOREM 3.3. *Any depth-three circuit computing the parity of $n$ variables has size at least $2^{c\cdot\sqrt{n}-o(\sqrt{n})}$ where $c = 1/(\sqrt{2e}\ln 2) = 0.618\ldots$ .*

PROOF. Let $\ell$ be the minimal size of a depth-three circuit computing the parity of $n$ variables. W.l.o.g., we can assume that it is a $\Pi_3$-circuit. We first use Lemma 3.2 to reduce the bottom fan-in. Say that an $\wedge$-gate on the bottom is *bad* if it has more than $k$ negated inputs. Let $\mathcal{F}$ be the family of sets of indices of negated inputs to bad $\wedge$-gates. This family has no more than $\ell$ sets. By Lemma 3.2, for every $m$ satisfying the inequality (3.1), there exists a subset $T$ of $n-m$ indices which intersects every set in $\mathcal{F}$. Thus, the assignment of the constant 1 to all the variables with indices in $T$ evaluates all bad gates to 0. The remaining gates are good, i.e., each has no more than $k$ negated inputs. Therefore, for any $k$ satisfying the following inequality:

$$k \geq \frac{\ln \ell}{\ln\left((n+1)/(m+1)\right)}, \tag{3.2}$$

there is a $\Pi_3^{\ell,k+}$-circuit $C$ which computes the parity of $m$ variables. Let $2 \leq s \leq m/2$ be an even integer (to be specified later). The circuit $C$ must, in particular, separate the pair $(A,B)$, where $A \subseteq \{0,1\}^m$ is the set of all odd vectors and $B$ is the set of all vectors with exactly $s$ ones. By Lemma 2.2, the pair $(A,B)$ does not have the property $P^+(k,\ell)$. This, in particular, means that $A$ contains no lower $k$-limit for an $\ell^{-1}$ fraction of $B$. By Lemma 3.1, this fraction cannot be larger than $F(m,k,s)$. Therefore, for any $k$ satisfying (3.2), the size $\ell$ must satisfy the inequality

$$\ell \geq \frac{|B|}{F(m,k,s)} = \frac{\binom{m}{s}\cdot\left(\frac{s}{2}\right)!}{\left(\frac{mk}{2}\right)^{s/2}}. \tag{3.3}$$

So, the desired lower bound for $\ell$ can be obtained by an appropriate choice of the parameters $m$ and $s$. The optimal bound $\ln \ell = \theta(\sqrt{n})$ is obtained for $k, s = \theta(\sqrt{n})$ and $m = \theta(n)$ and the computation is quite simple. However, we want to compute the constant explicitly; therefore, we need to compute more precisely. In particular, we must choose the constants for the parameters $k, s, m$. We shall use the following estimate (for $s \leq m/2$):

$$\binom{m}{s} \geq \gamma \left(\frac{me}{s}\right)^s \quad \left(\text{where} \quad \gamma = \frac{1}{\sqrt{4\pi s}} e^{-s^2/m}\right),$$

which can be easily derived using Stirling's formula

$$n! = n^n e^{-n} \sqrt{2\pi n}\, e^{\alpha_n},$$

where $1/(12n+1) < \alpha_n < 1/12n$.

Using the estimate for $\binom{m}{s}$, the inequality (3.3) gives the following bound

$$\ell \geq \frac{\sqrt{\pi s}}{\sqrt{4\pi s}\, e^{s^2/m}} \cdot \left(\frac{em}{s}\right)^s \cdot \left(\frac{s}{2e}\right)^{s/2} \cdot \left(\frac{mk}{2}\right)^{-s/2} \geq \frac{1}{e^{s^2/m+1}} \cdot \left(\frac{em}{sk}\right)^{s/2}.$$

Taking logarithms, we obtain

$$\ln \ell \geq \frac{s}{2} \cdot \ln \frac{em}{sk} - \frac{s^2}{m} - 1 = \frac{s}{2} \cdot \ln \frac{em}{sk} - O(1),$$

since $s = \theta(\sqrt{n})$ and $m = \theta(n)$. The function $s \cdot \ln(a/s)$ attains its maximum for $s = a/e$, hence we take $s = m/k$ which gives $\ln \ell \geq m/(2k) - O(1)$ and, by (3.2), we have the following inequalities:

$$\begin{aligned}
\ln \ell &\geq \frac{m \ln((n+1)/(m+1))}{2 \ln \ell} - O(1) \geq \frac{m \ln(n/m)}{2 \ln \ell} - O(1), \\
(\ln \ell)^2 &\geq \frac{m \ln(n/m)}{2} - O(\ln \ell) = \frac{m \ln(n/m)}{2} - o(n), \\
\ln \ell &\geq \sqrt{\frac{m/n \cdot \ln(n/m)}{2}} \cdot \sqrt{n} - o(\sqrt{n}).
\end{aligned}$$

The right hand side has a maximum for $m/n = e^{-1}$. Hence, $\ell \geq 2^{c\sqrt{n} - o(\sqrt{n})}$ where $c = 1/(\sqrt{2e} \ln 2)$. □

In case of the majority function, we use the following bound for the existence of limits.

LEMMA 3.4. *Let $\mathcal{F}$ be a family of $s$-element subsets of $[n]$, $s \geq 1$. If $|\mathcal{F}| > k^s$, then there exists a lower $k$-limit $Y$ for $\mathcal{F}$ such that $|Y| \leq s-1$.*

PROOF. The same as that of Lemma 3.1 in Case 1 using $k^s$ instead of $F(m,k,s)$. The basis $s=1$ is trivial. Suppose now that the lemma is true for $s$ and prove it for $s+1$. Take a family $\mathcal{F}$ of $(s+1)$-element subsets of $[n]$ with $|\mathcal{F}| > k^{s+1}$. If $\tau(\mathcal{F}) \geq k+1$, we are done since we can take $Y = \emptyset$. Otherwise, there exists an $x \in [n]$ for which $|\mathcal{F}_x| \geq |\mathcal{F}|/k > k^s$ and we can apply the induction hypothesis. □

THEOREM 3.5. *Any depth-three circuit computing the majority function has size at least $2^{d\cdot\sqrt{n}-o(\sqrt{n})}$ where $d = 1/\sqrt{\ln 4} = 0.849\ldots$ .*

PROOF. Let $\ell$ be the minimal size of a depth-three circuit computing $\neg\mathrm{MAJ}_n$, the negation of majority (and hence, the minimal size of a depth-three circuit computing $\mathrm{MAJ}_n$ itself). Since $\neg\mathrm{MAJ}_n$ is selfdual (i.e., complementing the output and all inputs does not change the function), we can w.l.o.g. assume that we have a $\Pi_3$-circuit. The argument is similar to that of Theorem 3.3; hence, let us only describe how to modify that proof. Set $m = n/2 + s$ with $s \leq n/2$ and reduce the bottom fan-in using Lemma 3.2, i.e., we now have $m$ remaining variables and the bottom fan-in is bounded by $k$, where $k$ is the smallest integer that satisfies inequality (3.1). Now our circuit $C$ must separate the pair $(A,B)$, where $A \subseteq \{0,1\}^m$ is the set of all vectors with at most $s-1$ ones and $B$ is the set of all vectors with exactly $s$ ones. By Lemmas 2.2 and 3.4,

$$\ell \geq \binom{m}{s} \cdot k^{-s} = \Omega\left(\frac{1}{\sqrt{s}}\left(\frac{em}{sk}\right)^s\right). \tag{3.4}$$

Now, if we choose $s = m/k$, then (3.4) gives $\ell = \Omega\left(e^s/\sqrt{s}\right)$. However, we need to fulfill (3.1) and hence we want to make sure that $e^s \leq \left(\frac{n+1}{m+1}\right)^k$. If we take $s = k\ln(2-\delta)$ with $\delta = O(n^{-1/2})$, then since $s = m/k$, we obtain $k = \sqrt{m/\ln(2-\delta)}$ which gives the bound $\ell \geq 2^{d\cdot\sqrt{n}-o(\sqrt{n})}$, where $d = \sqrt{1/\ln 4}$ is approximately $0.849\ldots$ . □

For the threshold function $\neg T^n_{(1-e^{-1})n}$, one can get the lower bound $2^{d\cdot\sqrt{n}-o(\sqrt{n})}$ with a slightly better constant $d = 1/(\sqrt{e}\ln 2) = 0.875\ldots$ .

## 4. A lower bound for a function computable by a small $\Sigma_3$-circuit

In this section, we prove an optimal lower bound for a function computable by a small $\Sigma_3$-circuit. Let $S_{s,m}$ be the boolean function with $n = 2sm$ variables defined as follows:

$$S_{s,m}(\mathbf{x},\mathbf{y}) = \bigvee_{i=1}^{s} \bigwedge_{j=1}^{m} (\bar{x}_{i,j} \vee \bar{y}_{i,j}).$$

We shall show that this function requires $\Pi_3$-circuits of size $2^{\Omega(\sqrt{n})}$, while it has a $\Sigma_3$-circuit of size $O(n)$. By a result of Klawe *et al.* (1984), this function has $\Pi_3$-circuits of size $2^{O(\sqrt{n})}$, thus the bound is optimal (up to the constant in the exponent).

LEMMA 4.1. *If $f = \bigvee_{i=1}^{s} \bigwedge_{j=1}^{m} \bar{x}_{i,j}$ is computed by a $\Pi_3^{\ell,k+}$-circuit, then the following inequality holds:*

$$\ell \geq \left(\frac{m}{k}\right)^s.$$

PROOF. Assume to the contrary that $\ell < (m/k)^s$. Any $\Pi_3^{\ell,k+}$-circuit for $f$ must separate the pair $(A,B)$, where $A \subseteq \{0,1\}^m$ is the set of all vectors with at most $s-1$ ones and $B$ is the set of $m^s$ vectors with exactly $s$ ones killing all $\wedge$'s in $f$. By Lemma 2.2, this pair $(A,B)$ does *not* have the property $P^+(k,\ell)$. This, in particular, means that there exists a subset $B' \subseteq B$ such that $|B'| \geq |B|/\ell = m^s/\ell > k^s$ and no vector in $A$ is a lower $k$-limts for $B'$, a contradiction with Lemma 3.4. □

THEOREM 4.2. *Any $\Pi_3$-circuit computing $S_{\sqrt{n/2},\sqrt{n/2}}$ has size at least $2^{c\cdot\sqrt{n}}$ with $c = 0.453\ldots$ .*

PROOF. In order to apply Lemma 4.1, we need only decrease the fan-in on the first level. In particular, we need to make sure that no gate on the first level has more than $k$ negated inputs. The most natural way to do this is to randomly fix one variable from each pair $x_{i,j}, y_{i,j}$ to 1. If an $\wedge$-gate contains both $x_{i,j}$ and $y_{i,j}$ negatively for some $i,j$, then it is always reduced to 0. Otherwise, an $\wedge$-gate with more than $k$ negated inputs is reduced to 0 with probability at least $1 - 2^{-k-1}$. This means that if $k \geq c\sqrt{n}$, then with probability at least a

half, all gates that originally had at least $k+1$ negated inputs will be reduced to 0, and in particular, such a restriction exists.

Let us note that we can avoid randomness also here, using a standard trick. Namely, to each gate $g$ with $a > k$ negated inputs which do not contain both $x_{i,j}$ and $y_{i,j}$ negatively for some $i, j$, assign a weight $w(g) = 2^{-a}$. Note that we can disregard the gates which originally have no more than $k$ negated inputs and those gates which contain both $x_{i,j}$ and $y_{i,j}$ negatively for some $i, j$. The former are allowed to remain and the latter are always reduced to 0. We determine the restriction piece by piece and at each point we let the weight of a gate be 0 if it has already been reduced to 0 and $2^{-b}$ otherwise, where $b$ is the number of negated variables that come from pairs where we so far have not determined which variable to fix. In other words, the weight is the probability that the gate will not be reduced to 0 if we make random choices in the future. We now determine the value of the restriction on the pair $x_{i,j}, y_{i,j}$ by calculating the total weight in the cases when we set $x_{i,j}$ to 1 and $y_{i,j}$ to 1, respectively. By definition, the average of these two numbers is the current total weight, and hence, one of the alternatives will give at most the same weight. We fix this choice and then continue with the next pair. The assignment constructed in this way gives a final weight which is at most one half and since the restriction is completely determined, it must be 0; hence, we have reduced all the gates in question to 0.

Using Lemma 4.1, we thus get a lower bound for the size of a $\Pi_3$-circuit computing $S_{s,m}$:

$$\ell \geq \min\left\{2^k, \left(\frac{m}{k}\right)^s\right\}. \tag{4.1}$$

Choosing $s = m = \sqrt{m/2}$ and $k = c \cdot \sqrt{n}$ with $c = 0.453\ldots$ gives the bound of the theorem. □

Note that the previous result (Håstad 1989) gave only a lower bound $2^{\Omega(n^{1/6}/\sqrt{\log n})}$ for the size of $\Sigma_3$-circuits computing a function which has a $\Sigma_4$-circuit of size $O(n)$.

## 5. Conclusions and open problems

The combinatorial techniques that we have used are very simple. Therefore, we hope that by applying more complicated arguments, it will be possible to get

substantially more. We shall list some problems which we consider important and give motivations for them.

PROBLEM 1. *Prove a superpolynomial lower bound for depth larger than three using a top-down argument.*

A top-down approach has been successfully applied in the case of monotone circuits (Klawe *et al.* 1984). What we do for depth three is quite similar. Therefore, it is possible that our argument can be extended to larger depths.

PROBLEM 2. *Prove a lower bound $2^{\Omega(n^\epsilon)}$ with $\epsilon > 1/2$ for depth-three circuits. More generally, prove such a bound with $\epsilon > 1/(d-1)$ for depth-$d$ circuits.*

Such bounds would give nonlinear lower bound for formula size using the reduction of Klawe *et al.* (1984). In fact, if a function has a lower bound $2^{\Omega(n^\epsilon)}$ with a fixed $\epsilon > 0$ for all depths $d$, then it is not in $\mathcal{NC}_1$.

PROBLEM 3. *Prove a bound for $\Pi_3^{\ell,k}$-circuits with $k \log \ell = \omega(n)$.*

Using the above technique, we can prove a bound larger than $2^{\Omega(\sqrt{n})}$, but the product $k \log \ell$ is always $O(n)$. Improving it is interesting, because if one could eventually prove a lower bound $\ell = 2^{\omega(n/\log\log n)}$ for $k \approx n^\epsilon$, where $\epsilon$ is an arbitrary small positive constant, then we would have a nonlinear lower bound for depth $O(\log n)$ circuits (with fan-in 2) by a result of Valiant (1977). Another reason why such an improvement would be interesting is the possibility to prove non-trivial space-time trade-offs. Take a non-deterministic Turing machine computing $f$ in time $T$ and space $S$. Using the ideas of Theorem 1 in (Borodin *et al.* 1993), one can prove the following: if $f$ has the property $P(k, \ell)$, then $S \cdot T = \Omega(k \log \ell)$. Details can be found in (Jukna 1994).

PROBLEM 4. *Determine the asymptotical complexity of depth-three circuits for majority.*

The best upper bound for the majority function is $2^{O\left(\sqrt{n \log n}\right)}$, using monotone circuits (see Klawe *et al.* 1984). For $ks \leq n$, the bound in Lemma 3.4 is optimal: take $s$ mutually disjoint subsets of $[n]$ $A_1, \ldots, A_s$, each of cardinality $k$, and define $\mathcal{F} = \{X \subseteq [n] : |X \cap A_i| = 1, \forall i\}$. Then $|\mathcal{F}| = k^s$ but $\tau(\mathcal{F}_Y) \leq k$

for any set $Y \subseteq [n]$, $|Y| \leq s-1$. We do not know the optimal value for $ks > n$. It is possible that for such parameters, one can obtain a bound larger than $2^{\Omega(\sqrt{n})}$.

It seems that what is needed is the following. Recall the property $P$ introduced in Section 2. In the above lower bounds we always took the color class $B'$ with the largest cardinality and looked for a limit there. In many cases, this may be not the best choice. We need an argument which uses the whole partition, not just one class.

## Acknowledgements

We would like to thank Ingo Wegener for being an initial link of communication between us which resulted in the present work. We would also like to thank an anonymous referee for many helpful comments. The second and third authors acknowledge support from the Alexander von Humboldt Foundation. The second author also acknowledges support from DFG grant Me 1077/5-2.

## References

M. Ajtai, $\Sigma^1_1$-formulae on finite structures. *Ann. Pure and Appl. Logic* **24** (1983), 1–48.

A. Borodin, A. Razborov and R. Smolensky, On lower bounds for read-$k$-times branching programs. *Computational Complexity* **3** (1993), 1–18.

P. Erdös and R. Rado, Intersection theorems for systems of sets. *J. London Math. Soc.* **35** (1960), 85–90.

M. Furst, J. Saxe and M. Sipser, Parity, circuits and the polynomial time hierarchy. *Math. Systems Theory* **17** (1984), 13–27.

J. Håstad, *Almost Optimal Lower Bounds for Small Depth Circuits.* Advances in Computing Research, ed. S. Micali, Vol 5 (1989), 143–170.

S. Jukna, *Finite limits and lower bounds for circuit size.* Tech. Rep. 94–06, Informatik, University of Trier, 1994.

M. Karchmer and A. Wigderson, Monotone circuits for connectivity require super-logarithmic depth. *SIAM J. Disc. Math.* **3** (1990), 255–265.

M. Klawe, W.J. Paul, N. Pippenger, M. Yannakakis, On monotone formulae with restricted depth. In *Proc. Sixteenth Ann. ACM Symp. Theor. Comput.*, 1984, 480–487.

R. Raz and A. Wigderson, Monotone circuits for matching require linear depth. In *Proc. Twenty-second Ann. ACM Symp. Theor. Comput.*, 1990, 287–292.

A. A. Razborov, Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$. *Math. Notes of the Academy of Sciences of the USSR* **41**:4 (1987), 333–338.

M. Sipser, Private communication, 1991.

M. Sipser, A topological view of some problems in complexity theory. In *Colloq. Math. Soc. János Bolyai* **44** (1985), 387–391.

R. Smolensky, Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proc. Nineteenth Ann. ACM Symp. Theor. Comput.*, 1987, 77–82.

L.G. Valiant, Graph-theoretic arguments in low level complexity. In *Proc. Sixth Conf. Math. Foundations of Computer Science*, Lecture Notes in Computer Science, 1977, Springer-Verlag, 162–176.

A.C. Yao, Separating the polynomial time hierarchy by oracles. In *Proc. Twenty-sixth Ann. IEEE Symp. Found. Comput. Sci.*, 1985, 1–10.

Manuscript received October 24, 1993

J. Håstad
Royal Institute of Technology
Stockholm, SWEDEN
johanh@nada.kth.se

S. Jukna
Institute of Mathematics
Vilnius, LITHUANIA

P. Pudlák
Mathematical Institute
Prague, CZECH REPUBLIC
pudlak@csearn.bitnet
pudlak@earn.cvut.cz

Current address of S. Jukna:
University of Trier
Trier, GERMANY
jukna@ti.uni-trier.de