SIAM J. DISC. MATH.
Vol. 3, No. 2, pp. 255–265, May 1990

008

MONOTONE CIRCUITS FOR CONNECTIVITY REQUIRE SUPER-LOGARITHMIC DEPTH*

MAURICIO KARCHMER†‡ AND AVI WIGDERSON†

Abstract. It is proved here that every monotone circuit which tests *st*-connectivity of an undirected graph on n nodes has depth $\Omega(\log^2 n)$. This implies a superpolynomial ($n^{\Omega(\log n)}$) lower bound on the size of any monotone formula for *st*-connectivity.

The proof draws intuition from a new characterization of circuit depth in terms of communication complexity. Within the same framework, a very simple and intuitive proof is given of a depth analogue of a theorem of Khrapchenko concerning formula size lower bounds.

Key words. circuit complexity, communication complexity, monotone circuits, graph connectivity

AMS(MOS) subject classifications. 06E30, 94A05, 94C10

1. Introduction.

The circuit complexity of Boolean functions has been studied for the past forty years, but its main problem remains unsolved: we have no example of a simple function (say in NP) that requires super linear circuit size or super logarithmic (bounded fan-in) circuit depth. The reason is, perhaps, that although the circuit model is elegantly simple, our understanding of the way it computes is, at the most, vague.

In the last years, however, advance has been surprisingly fast. On the one hand, results of Andreev [An] and Razborov [Ra], improved by Alon and Boppana [AB], give exponential size lower bounds for monotone circuits. On the other hand, results of a long list of authors (e.g., [Aj], [FSS], [Y1], [H]) give exponential size lower bounds for constant depth circuits. More than the results themselves, perhaps the main contribution of the mentioned papers has been the development of some general techniques for proving lower bounds, such as random restrictions and circuit approximation. These techniques, however, turn out to be difficult to apply to other problems so that new ideas have been sought.

In this paper we show the equivalence between circuit depth and the communication complexity of a certain related problem.[1] We believe that the later model is much more appealing for both showing and understanding upper bounds, as well as for proving lower bounds. This characterization is reminiscent of, but somehow more explicit and intuitive than, the well known relationship between circuits and alternating machines [Ru]. This characterization allows us to view computation top-down (from output to input) and apply such techniques as random restrictions in that direction (rather than the common bottom-up approach). We argue the relevance of this model by presenting a very simple proof of a theorem of Khrapchenko, and by proving the first super-logarithmic (in the size of the circuit) depth lower bound for monotone circuits.

Though the mentioned results of Andreev and Razborov give exponential (in $\log n$) depth lower bounds for monotone circuits computing certain functions, the depth lower bound is always logarithmic in the size bound. That is, the techniques apply to size rather

* Received by the editors March 1, 1989; accepted for publication in revised form June 9, 1989.

† Institute of Mathematics and Computer Science, Hebrew University, Jerusalem, Israel 91904. Part of this work was done while the authors were visiting the University of California at Berkeley and was supported by National Science Foundation grant DCR-8612563. The second author also wishes to acknowledge support from the Alon Fellowship and an American-Israeli Binational Science Foundation grant.

‡ Present address, Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139.

[1] Yannakakis independently discovered this equivalence [KPPY].

than to depth. We present a technique which captures, in a strong way, the essence of circuit depth. We give here a tight $\Omega(\log^2 n)$ depth bound for *st*-connectivity,[2] a function which has $O(n^2 \log n)$ size, $O(\log^2 n)$ depth monotone circuits. As a consequence, we get nonpolynomial ($n^{\Omega(\log n)}$) size lower bounds for monotone formulas computing *st*-connectivity and hence separate the monotone analogues of NC^1 and AC^1.

While our proof bears no obvious similarity to the methods of Razborov and Andreev, we point out the important role that (different) nontrivial results from extremal set theory play in both cases.

It is interesting to note here the different character of the connectivity and majority functions in the Boolean and arithmetic monotone circuits models. Shamir and Snir [ShS] showed an $\Omega(\log^2 n)$ depth bound for both functions in the arithmetic model. The difficulty in applying these techniques to Boolean circuits are the axioms $x \vee xy = x$ and its dual, which do not hold in rings. Indeed, Valiant [V] (by probabilistic methods) and Ajtai, Komlos, and Szemerédi [AKS] (by explicit constructions) showed that these axioms make a difference for the majority function which admits $O(\log n)$ depth monotone Boolean circuits. Our result says that, unlike for majority, for connectivity the situation in the Boolean case is very similar to the arithmetic one.

It is worthwhile to mention that our results apply to undirected graph *st*-connectivity, a function that, in some models, is easier than its directed version. For example, see [AKLLR] for some relevant evidence. More recently, Ajtai and Fagin [AF] show that, while undirected *st*-connectivity is definable in monadic second order logic, the directed case is not.

The paper is organized as follows: In § 2 we define the communication game and show its equivalence to circuit depth; in § 3 we give a simple proof of a theorem of Khrapchenko. In § 4 we give the lower bound for connectivity.

2. Communication complexity and circuit depth. In this section we show the equivalence between circuit depth and a problem in communication complexity. We will be considering circuits over the basis $\{\vee, \wedge, \neg\}$ where $\{\vee, \wedge\}$-gates have fan-in 2 and $\neg$-gates are only applied to input variables. For a function f, $d(f)$ is the minimum depth of a circuit computing f.

Let $B_0, B_1 \subseteq \{0,1\}^n$ such that $B_0 \cap B_1 = \varnothing$. Consider the following game between players I and II: Player I gets $x \in B_1$ while player II gets $y \in B_0$; their goal is to find a coordinate i such that $x_i \neq y_i$. Let $C(B_1, B_0)$ be the minimum number of bits they have to communicate in order for both to agree on such a coordinate. Note that unlike standard problems in communication complexity [Y1], the task of the players here is to solve a search, rather than a decision, problem.

THEOREM 2.1. *For every function* $f:\{0,1\}^n \to \{0,1\}$ *we have*

$$d(f)=C(f^{-1}(1), f^{-1}(0)).$$

Proof. The proof follows from the following two lemmas. □

LEMMA 2.1. *For all functions f and all $B_0, B_1 \subseteq \{0,1\}^n$ such that $B_0 \subseteq f^{-1}(0)$ and $B_1 \subseteq f^{-1}(1)$ we have*

$$C(B_1, B_0) \leqq d(f).$$

Proof. The proof is shown by induction on $d(f)$.

If $d(f)=0$ then f is either x_i or $\bar{x}_i$. In either case, we have that for all $x \in B_1$ and $y \in B_0$, $x_i \neq y_i$ so that i is always an answer and $C(B_1, B_0)=0$.

[2] We present here an improved and simplified version of an early result of ours giving a $\Omega(\log^2 n/\log\log n)$ bound. This was possible after Hastad formulated and proved Lemma 4.1. A similar improvement was independently discovered by Boppana.

For the induction step we suppose that $f = f_1 \wedge f_2$ (the case $f = f_1 \vee f_2$ is treated similarly) so that $d(f) = \max(d(f_1), d(f_2)) + 1$. Let $B_0^j = B_0 \cap f_j^{-1}(0)$ for $j = 1, 2$. By induction we have that $C(B_1, B_0^j) \leqq d(f_j)$ for $j = 1, 2$. Consider the following protocol for B_1 and B_0: player II sends a 0 if $y \in B_0^1$, otherwise he sends a 1; the players then follow the best protocol for each of the subcases. We have

$$C(B_1, B_0) \leqq 1 + \max_{j=1,2} (C(B_1, B_0^j)) \leqq 1 + \max_{j=1,2} (d(f_j)) = d(f). \qquad \square$$

The converse is as follows.

LEMMA 2.2. *Let $B_0, B_1 \subseteq \{0, 1\}^n$ such that $B_0 \cap B_1 = \varnothing$. Then, there exists a function f with $B_0 \subseteq f^{-1}(0)$ and $B_1 \subseteq f^{-1}(1)$ such that*

$$d(f) \leqq C(B_1, B_0).$$

Proof. The proof is shown by induction on $C(B_1, B_0)$.

If $C(B_1, B_0) = 0$ then there exists an i such that for all $x \in B_1$ and for all $y \in B_0$, $x_i \neq y_i$. It is clear that for all $x', x'' \in B_1$ we have $x_i' = x_i''$ and the same holds for all y', $y'' \in B_0$. Without loss of generality $x_i = 1$ so that letting $f = x_i$ we have $B_0 \subseteq f^{-1}(0)$ and $B_1 \subseteq f^{-1}(1)$.

To prove the induction step, we assume that player II sends the first bit (the other case is treated similarly). For some partition $B_0 = B_0^1 \cup B_0^2$, player II sends a 0 if $y \in B_0^1$, a 1 otherwise; the players then continue with the best protocol for each of the subcases and

$$C(B_1, B_0) = 1 + \max_{j=1,2} (C(B_1, B_0^j)).$$

By induction, there exist f_1, f_2 so that $B_0^j \subseteq f_j^{-1}(0)$, $B_1 \subseteq f_j^{-1}(1)$ and $d(f_j) \leqq C(B_1, B_0^j)$ for $j = 1, 2$. Taking now $f = f_1 \wedge f_2$ we have

$$B_1 \subseteq f_1^{-1}(1) \cap f_2^{-1}(1) = f^{-1}(1)$$

$$B_0 = B_0^1 \cup B_0^2 \subseteq f_1^{-1}(0) \cup f_2^{-1}(0) = f^{-1}(0)$$

and

$$d(f) \leqq 1 + \max_{j=1,2} (d(f_j)) \leqq 1 + \max_{j=1,2} (C(B_1, B_0^j)) = C(B_1, B_0). \qquad \square$$

For monotone circuits we can give a modified version of Theorem 2.1 that captures, in a nice way, the restrictions of monotone computation. A *minterm* (*maxterm*) of a monotone function f is a minimal set of variables where, if we set to 1 (0), f will be equal to 1 (0) regardless of the other variables. Define $\min(f)$, $\mathrm{Max}(f)$ as the set of minterms, respectively, maxterms, of f. It is easy to see that every minterm intersects every maxterm. We will look at minterms and maxterms as subsets of $[n]$.[3] For a monotone function f, let $d_m(f)$ be the minimum depth of a monotone circuit computing f.

Consider the following communication game (the *monotone* game) between players I and II. Let $P, Q \subseteq 2^{[n]}$ be such that for all $p \in P$ and for all $q \in Q$ we have $p \cap q \neq \varnothing$. Player I gets a $p \in P$ while player II gets a $q \in Q$; their goal is to find an element in $p \cap q$. Let $C_m(P, Q)$ be the minimum number of bits they have to communicate in order to find such an element.

THEOREM 2.2. *For every monotone function f we have*

$$d_m(f) = C_m(\min(f), \mathrm{Max}(f)).$$

[3] $[n] = \{1, \cdots, n\}$.

Proof. Note that in the base case of Lemma 2.1, if the circuit is monotone, we always find a coordinate i such that $x_i = 1$ while $y_i = 0$. On the other hand, if the protocol always gives a coordinate i with the above property, Lemma 2.2 gives a monotone circuit.

Let $x \in f^{-1}(1)$ be the characteristic vector of a subset $p \subseteq [n]$. Similarly, let $y \in f^{-1}(0)$ be the characteristic vector of the complement of a subset $q \subseteq [n]$ (i.e., $i \in q \Leftrightarrow y_i = 0$). By the above argument, it is clear that the answer of the protocol will be an element of $p \cap q$. The theorem follows by noticing that it is enough to give a protocol for $(\min(f), \operatorname{Max}(f))$ because the players, in case they get inputs p' and q', can always behave as if they got $p \subseteq p'$ and $q \subseteq q'$ where $p \in \min(f)$ and $q \in \operatorname{Max}(f)$. □

For proving lower bounds for the communication game, it may be convenient to have more structure in the way the players behave. We would like to synchronize the protocol so that the players communicate in rounds where players I and II send messages of fixed lengths.

THEOREM 2.3. *For any function f, there exists a protocol D where at each round player* II *sends 2^a bits while player* I *responds with a bits and such that the number k of rounds satisfies*

$$k \leqq \frac{d(f)}{a}$$

for the general game and

$$k \leqq \frac{d_m(f)}{a}$$

for the monotone one.

Proof. Let C be the best circuit for f. The idea is to simulate a layers of C with a round of D. Divide C into stages of depth a each and look at the subcircuits of each stage. Each one computes a function which depends on at most 2^a wires and, thus, can be represented in Conjunctive Normal Form (CNF) with at most 2^{2a} clauses, each of length at most 2^a. Following the proof of Lemma 2.1, it is easy to see that such a CNF representation can be simulated by a round where player II sends 2^a bits and player I sends a bits. The same holds for the monotone case. □

Of course, in Theorem 2.3, the roles of players I and II can be switched so that both players send 2^a and a bits per round, respectively.

3. Khrapchenko's bound. As a nice application of Theorem 2.1, we give a simple proof of a depth analogue of a theorem of Khrapchenko [K]. Let C_n be the graph of the n-cube with vertex set $\{0, 1\}^n$ and two nodes adjacent if and only if they differ in one coordinate. Any subset A of edges induces a graph G_A of C_n in the natural way. For a graph G_A and a node x, we denote $d_A(x)$, $N_A(x)$ as the degree of x in A and the set of neighbors of x in A, respectively. We drop the subindex A if no confusion arises. Let E denote expectation with uniform distribution.

THEOREM 3.1 (Khrapchenko). *Let $B_0, B_1 \subseteq \{0, 1\}^n$ such that $B_0 \cap B_1 = \varnothing$. Let $A = C_n \cap (B_0 \times B_1)$. Then, for every function f with $B_0 \subseteq f^{-1}(0)$ and $B_1 \subseteq f^{-1}(1)$ we have*

$$d(f) \geqq \log \frac{|A|^2}{|B_0|\,|B_1|}.$$

Proof. Fix a protocol D for the communication game and let $C(x, y)$ be the number of bits D uses on inputs x, y. We will prove that for (x, y) taken uniformly from A

we have

(*)

so that by Lemma 2.1,

We view (*) as fo

and note that $|A|/|B$

respectively. In what f

least the logarithm of

tuitively, this is so bec

II which x he has.

We now proceed

bits player I and II sen

We claim:

○ For any $x \in B$

player II know

○ Similarly, for a

We now conclud

where the last inequal

4. A lower boun

bound for monotone

is organized as follow

in § 4.2 we give some

of the theorem.

4.1. Intuition. T

of an undirected grap

is a path from s to t c

sponding to minimal

st-paths as ordered se

set of vertices into two

cut contains all edges

$q: V \rightarrow \{0, 1\}$ where

we have

$$(*)\qquad E(C(x,y)) \geqq \log \frac{|A|^2}{|B_0|\,|B_1|}$$

so that by Lemma 2.1, we get $d(f) \geqq E(C(x, y))$.

We view $(*)$ as follows: Write

$$\log \frac{|A|^2}{|B_0|\,|B_1|} = \log \frac{|A|}{|B_0|} + \log \frac{|A|}{|B_1|}$$

and note that $|A|/|B_0|$ and $|A|/|B_1|$ are the average degrees of nodes in B_0 and B_1, respectively. In what follows, we will claim that the number of bits player I sends is at least the logarithm of the average degree of nodes in B_1 (similarly with player II). Intuitively, this is so because even if player I knows y, he needs $\log d(y)$ bits to tell player II which x he has.

We now proceed formally. For $(x, y) \in A$, let $b_{\mathrm{I}}(x, y)$, $b_{\mathrm{II}}(x, y)$ be the number of bits player I and II send when the input to the protocol is (x, y). We have

$$E(C(x,y)) = \frac{1}{|A|}\left[\sum_{(x,y)\in A} (b_{\mathrm{I}}(x,y) + b_{\mathrm{II}}(x,y))\right]$$

$$= \frac{1}{|A|}\left[\sum_{x\in B_1}\sum_{y\in N(x)} b_{\mathrm{II}}(x,y) + \sum_{y\in B_0}\sum_{x\in N(y)} b_{\mathrm{I}}(x,y)\right].$$

We claim:

- For any $x \in B_1$, $\sum_{y\in N(x)} b_{\mathrm{II}}(x, y) \geqq d(x) \log d(x)$. This is so because, even if player II knows x, he has to tell player I which y he has.
- Similarly, for all $y \in B_0$ we have $\sum_{x\in N(y)} b_{\mathrm{I}}(x, y) \geqq d(y) \log d(y)$.

We now conclude that

$$E(C(x,y)) \geqq \frac{1}{|A|}\left[\sum_{x\in B_1} d(x)\log d(x) + \sum_{y\in B_0} d(y)\log d(y)\right]$$

$$\geqq \frac{1}{|A|}\left[\sum_{x\in B_1} \frac{|A|}{|B_1|}\log\frac{|A|}{|B_1|} + \sum_{y\in B_0}\frac{|A|}{|B_0|}\log\frac{|A|}{|B_0|}\right] = \log\frac{|A|^2}{|B_1|\,|B_0|}$$

where the last inequality follows from the convexity of $x \log x$. $\square$

4. A lower bound for connectivity. In this section we give a $\Omega(\log^2 n)$ depth lower bound for monotone circuits computing undirected graph *st*-connectivity. This section is organized as follows: In § 4.1 we give some intuition and we state the main theorem; in § 4.2 we give some definitions and useful lemmas; finally, in § 4.3 we give the proof of the theorem.

4.1. Intuition. The function *st*-connectivity receives as input the adjacency matrix of an undirected graph with two distinguished vertices s and t, and tests whether there is a path from s to t or not. The function is obviously monotone with minterms corresponding to minimal *st*-paths and maxterms corresponding to minimal *st*-cuts. We view *st*-paths as ordered sets of vertices excluding s and t. We view *st*-cuts as partitions of the set of vertices into two subsets, one containing s and the other containing t. The minimal cut contains all edges between the two subsets. A partition may be regarded as a coloring $q: V \to \{0, 1\}$ where $q(s) = 0$ and $q(t) = 1$. The game is as follows: Player I gets an *st*-

path while player II gets a coloring of the nodes. Their goal is to find a bichromatic edge in the path.

Let us look at the protocol based on the idea of raising the adjacency matrix of the graph to the nth power: Player I sends the name of the middle vertex on his path; player II responds with the color of that vertex. The players then continue recursively on the half path where a bichromatic edge is ensured to exist. Note that the protocol requires $O(\log n)$ rounds in each of which player I sends $\log n$ bits and player II sends just one.

The crucial observation is that, even if player II were allowed to send $O(n^\epsilon)$ bits each round (instead of one bit as in the protocol), the players will still need many rounds. Basically, this is because player II doesn't know much about the nodes in player I's path. If he sends $O(n^\epsilon)$ bits and the path is of length $O(n^\epsilon)$, then the probability that player I gets valuable information from player II is negligible. If we could prove a $\Omega(\log n)$ lower bound for the number of rounds needed, we will be able to use Theorem 2.3 to get the promised $\Omega(\log^2 n)$ depth lower bound for circuits.

Note the asymmetry between players I and II. Indeed, if the roles of both players were switched so that player I would be the one who sends $O(n^\epsilon)$ bits per round, they would be able to solve the problem in a constant number of rounds. This is consistent with the intuition in Shamir and Snir in [ShS].

Define *stconn*(l) as the restriction of *st*-connectivity to the case where player I gets a path of length l. We state the main theorem of this section.

THEOREM 4.1. *Suppose* $l \leqq n^{1/10}$. *There exists an* $0 < \epsilon < \frac{1}{2}$ *such that if* D *is a* k-*round protocol for stconn*(l) *where at each round player* I *sends* $\epsilon \log n$ *bits and player* II *sends* n^ϵ *bits, then* $k \geqq \log l$.

COROLLARY 4.1. *The monotone depth complexity of st-connectivity is* $\Omega(\log^2 n)$.

Proof. The proof follows from Theorems 2.3 and 4.1 by taking $l = n^{1/10}$. □

COROLLARY 4.2. *The monotone formula size complexity of st-connectivity is* $n^{\Omega(\log n)}$.

Proof. The proof follows by noting that the relation $d(f) = O(\log L(f))$ holds also in the monotone case [S]. □

Theorem 4.1 is a consequence of the following theorem. Let *vector*(l) be the game where player I gets an $(l+2)$-vector p with $p[0] = s$ and $p[l+1] = t$ and other entries from $[n]$ and player II gets a coloring $q \in \{0, 1\}^n$ of $[n]$ extended so that $q(s) = 0$ and $q(t) = 1$. The goal of the players is to find an element $v \in [n]$ such that for some index i, $p[i] = v$ and either $q(p[i]) \neq q(p[i+1])$ or $q(p[i-1]) \neq q(p[i])$.

THEOREM 4.2. *Suppose* $l \leqq n^{1/10}$. *There exist an* $0 < \epsilon < \frac{1}{2}$ *such that if* D *is a* k-*round protocol where at each round player* I *sends* $\epsilon \log n$ *bits and player* II *sends* n^ϵ *bits, and* D *solves the game vector*(l) *for a fraction* $\frac{1}{8}n^{-\epsilon}$ *of the possible vectors, then* $k \geqq \log l$.

Note that in *stconn*(l) the players are asked to find a bichromatic edge, while in *vector*(l) they are asked to find an endpoint of a bichromatic edge. Also, in *stconn*(l), player I receives a simple path which can be viewed as a vector without repetitions. Given this, Theorem 4.1 follows by noting that, by our choice of l, a protocol for *stconn*(l) solves the game *vector*(l) for a fraction $1 - o(1)$ of the vectors.

To prove Theorem 4.2, we will assume, for contradiction, the existence of a k-round protocol ($k < \log l$) good for a large family of all possible vectors and a large family of all possible colorings. We will pick a large subset of the vectors and colorings for which players I and II sent the same message in the first round. We will give some extra information (by applying a random restriction to the coloring of the nodes) to both players so as to get smaller, yet nicer, subsets which are in 1-1 correspondence with a family of vectors shorter in length (but of higher quality) and a family of colorings of fewer nodes. The fact that the original protocol had $(k-1)$ rounds to go will allow us to find a $(k-1)$-round protocol for the smaller families. Repeating this k times will give us a

protocol without commu
any messages.
Note the top-down
the output of a shallow
then there is a wire which
used in [KPPY].

4.2. Notation and d
from $[n]$. An *interval* I
and an interval $I \subseteq [l]$,
$\{p_I : p \in P\}$ is the projecti
$P \subseteq [n]^l$ and an interval
in P within I. We will d
the *support* of p, supp (p)
arises, we will denote sup
we will denote a vector p
the respective interval.
Similarly, for a colo
into T and for $Q \subseteq \{0,$
$\{0, 1\}^{|T|}$, $Q \subseteq \{0, 1\}^n$
set of extensions of q in
possible). For a restrictio
in Q consistent with ρ, (
For a subset A of a
what follows, we will wo
the context, we will drop
we may mix densities wi
We will need the f
$\cdots \times A_k$ and for $v \in A_i$,
H, $Ext_{A_i}(v)$ will be cons
A_k and, in what follows,
LEMMA 4.1. *Let* H
Then

Proof. Say that a n
the set of bad elements i

$\mu(\bar{H}$

the lemma follows imm

COROLLARY 4.3.
COROLLARY 4.4.
$\{1, \cdots, k\}$.

protocol without communication that solves a problem which cannot be solved without any messages.

Note the top-down structure of the proof; essentially, the argument shows that, if the output of a shallow circuit depending on a set of wires is in some sense complex, then there is a wire which computes a complex subfunction. This is similar to the argument used in [KPPY].

4.2. Notation and definitions. Let $[n]^l$ denote the set of all l-vectors with entries from $[n]$. An *interval* $I \subseteq [l]$ is a subset of consecutive integers. For a vector $p \in [n]^l$ and an interval $I \subseteq [l]$, p_I is the *projection* of p into the interval I. For $P \subseteq [n]^l$, $P_I = \{p_I : p \in P\}$ is the projection of P into I. Note that $P_I \subseteq [n]^{|I|}$. Conversely, for $p \in [n]^{|I|}$, $P \subseteq [n]^l$ and an interval I, let $Ext_{P,I}(p) = \{\tilde{p} \in P : \tilde{p}_I = p\}$ be the set of extensions of p in P within I. We will drop the subindices P and I if no confusion arises. For $p \in [n]^l$, the *support* of p, supp (p), is defined as the set of nodes contained in p. When no confusion arises, we will denote supp (p) by p. Given a partition of $[l]$ into two intervals L and R, we will denote a vector $p \in [n]^l$ by (p_L, p_R) where each entry is the projection of p into the respective interval.

Similarly, for a coloring $q \in \{0, 1\}^n$ and a subset $T \subseteq [n]$, q_T is the projection of q into T and for $Q \subseteq \{0, 1\}^n$, $Q_T = \{q_T : q \in Q\}$ is the projection of Q into T. For $q \in \{0, 1\}^{|T|}$, $Q \subseteq \{0, 1\}^n$ and a subset $T \subseteq [n]$, let $Ext_{Q,T}(q) = \{\tilde{q} \in Q : \tilde{q}_T = q\}$ be the set of extensions of q in Q within T (again, we drop the subindices Q and T whenever possible). For a restriction $\rho : [n] \mapsto \{0, 1, *\}$, we will denote by Q^ρ the set of colorings in Q consistent with ρ, (i.e., $\{q \in Q : \rho(i) \neq * \Rightarrow \rho(i) = q_i\}$).

For a subset A of a universe Ω, the density of A, $\mu_\Omega(A)$, is defined as $|A|/|\Omega|$. In what follows, we will work with densities rather than with cardinalities. If Ω is clear from the context, we will drop the subindex and write $\mu(A)$. The reader should be aware that we may mix densities with respect to different universes in the same equation.

We will need the following combinatorial lemma due to Hastad: Let $H \subseteq A_1 \times \cdots \times A_k$ and for $v \in A_i$, let $Ext_{A_i}(v) = \{u \in H : u_i = v\}$. Note that, though $Ext_{A_i}(v) \subseteq H$, $Ext_{A_i}(v)$ will be considered as a subset of $H/A_i = A_1 \times \cdots \times A_{i-1} \times A_{i+1} \times \cdots \times A_k$ and, in what follows, its density will be defined with respect to H/A_i.

LEMMA 4.1. *Let $H \subseteq A_1 \times \cdots \times A_k$. Let $B_i = \{u \in A_i : \mu(Ext_{A_i}(u)) \geqq \mu(H)/2k\}$. Then*

$$\prod_{i=1}^{k} \mu(B_i) \geqq \frac{\mu(H)}{2}.$$

Proof. Say that a member $(u_1, \cdots, u_k)$ of H is bad if for some i, $u_i \notin B_i$. Let $\bar{H}$ be the set of bad elements in H. We have

$$\mu(\bar{H}) \leqq \sum_{i=1}^{k} \mu\left(\bigcup_{u \notin B_i} Ext_{A_i}(u)\right) < \sum_{i=1}^{k} \frac{\mu(H)}{2k} = \frac{\mu(H)}{2};$$

the lemma follows immediately, by noting that

$$\prod_{i=1}^{k} \mu(B_i) \geqq \mu(H) - \mu(\bar{H}). \qquad \square$$

COROLLARY 4.3. *If $k = 2$, then there exists an i such that $\mu(B_i) \geqq (\mu(H)/2)^{1/2}$.*

COROLLARY 4.4. $\Pr(\mu(B_i) < (\mu(H)/2)^{2/k}) < \frac{1}{2}$ *for i chosen randomly from* $\{1, \cdots, k\}$.

4.3. The proof.

Proof of Theorem 4.2. In what follows, all our protocols will be synchronized so that at each round player I sends $\varepsilon \log n$ bits and player II responds with n^ε bits. The existence of ε will be clear from the proof, though we can check that $\varepsilon = \frac{1}{10}$ suffices. We will define a sequence of problems of different sizes as follows: We first define the parameters of the problems, let $t_{\max} = \log l - 1$.

Let $n_0 = n$ and $n_{t+1} = n_t - 4n_t^{1/2}$. Note that

$$(1) \qquad n/2 \leqq n_t \leqq n \quad \text{for } t \leqq t_{\max}.$$

Let $l_0 = l$ and $l_{t+1} = l_t/2$ and note that

$$(2) \qquad 2 \leqq l_t \leqq l \quad \text{for } t \leqq t_{\max}.$$

Consider the following property:

H(t, k). *There exist a collection of vectors* $P^t \subseteq [n_t]^{l_t}$ *of length* l_t, *and a collection of colorings* $Q^t \subseteq \{0, 1\}^{n_t}$ *of* $[n_t]$, *with* $\mu(P^t) \geqq \frac{1}{8}n^{-\varepsilon}$ *and* $\mu(Q^t) \geqq 2^{-2tn^\varepsilon}$ *such that there exists a k-round protocol* D^t *good for* (P^t, Q^t).

We will prove the following two claims:

CLAIM 4.1. *For* $t \leqq t_{\max}$ $\neg H(t, 0)$.

CLAIM 4.2. *For* $t \leqq t_{\max}$ $H(t, k) \rightarrow H(t+1, k-1)$.

It is clear that the two claims imply $\neg H(0, t_{\max})$ which in turn implies our theorem.

The first claim follows easily by noticing that there is not a single node (other than s and t) which appears in every vector of P^t so that player II cannot know the answer. To see this, note that the fraction of vectors of length l_t which contain a given node is $1 - (1 - 1/n_t)^{l_t} \ll \frac{1}{8}n^{-\varepsilon}$. This is enough for proving the claim as both players must know the answer. However, it can also be shown that, for most input pairs, player I will not know the color of a single node in its vector.

The second claim will be proved by assuming $H(t, k)$ and constructing P^{t+1}, Q^{t+1}, and D^{t+1} so as to satisfy $H(t+1, k-1)$. Take P^t, Q^t, and D^t which satisfy $H(t, k)$. Let us look at the protocol after the first round. By the pigeonhole principle, there exist $P \subseteq P^t$ with $\mu(P) \geqq \frac{1}{8}n^{-2\varepsilon}$ such that for every vector in P, player I sent the same message. Similarly, there exists $Q \subseteq Q^t$ with $\mu(Q) \geqq 2^{-(2t+1)n^\varepsilon}$ so that for every coloring of Q, player II sent the same message.

Let $L = \{1, \cdots, l_t/2\}$ and $R = \{l_t/2 + 1, \cdots, l_t\}$ be a partition of the vector's coordinates into left and right intervals of the same length. We say that P is L-good if *many* left projections of P have, each, *many* extensions to the right; that is, if

$$\mu(\{p_L : \mu(Ext_{P,L}(p_L)) \geqq n^{-2\varepsilon}/32\}) \geqq \tfrac{1}{4}n^{-\varepsilon}.$$

R-goodness is defined similarly. The following lemma states that if we shrink the length of the vectors to half and we restrict our family P to one of the intervals, then we can improve the quality of our collection. This is one of our main ideas: Although we cannot raise the absolute size of P, by reducing the size of the universe we can increase its density.

LEMMA 4.2. *P is either L-good or R-good.*

Proof. The lemma follows using Corollary 4.3 and viewing P as a subset of $[n_t]^{l_{t+1}} \times [n_t]^{l_{t+1}}$. $\square$

Without loss of generality, assume that P is L-good and let A be the set of vectors in P_L with many extensions. The next lemma is the heart of our argument.

LEMMA 4.3. *There exists a restriction* $\rho : [n_t] \mapsto \{0, 1, *\}$ *with* $|\rho^{-1}(*)| = n_{t+1}$ *such that the following properties hold:*

G1: $\mu(Q^{\rho}_{\rho^{-1}(*)}) \geqq 2^{-2(t+1)n^{\epsilon}}$.

G2: $\exists \bar{P} \subseteq P$ *such that*

- $\forall p \in \bar{P}, \quad p_L \subseteq \rho^{-1}(*)$ *and* $p_R \subseteq \rho^{-1}(1)$
- $\forall p, p' \in \bar{P}, \quad p_L \neq p'_L$
- $\mu(\bar{P}_L) \geqq \frac{1}{8} n^{-\epsilon}$.

Assuming the lemma is true, we will finish the proof of the second claim.

Let $Q^{t+1} = Q^{\rho}_{\rho^{-1}(*)}$ and $P^{t+1} = \bar{P}_L$ and rename the coordinates so that $[n_{t+1}] = \rho^{-1}(*)$. Note that there is a natural 1-1 correspondence between Q^{t+1} and Q^{ρ} and between P^{t+1} and $\bar{P}$. Also note that for all $q \in Q^{\rho}$ and for all $p \in \bar{P}$ any bichromatic edge lies in the interval L. The protocol D^{t+1} on (P^{t+1}, Q^{t+1}) simulates the remaining rounds of the protocol D^t on $(\bar{P}, Q^{\rho})$ by following the behavior of the associated vector and coloring. □

Proof of Lemma 4.3. In what follows, we denote $V = [n_t]$, $v = n_t$, $l = l_t$, $l' = l_{t+1}$ for simplicity. The existence of a good restriction will be shown by probabilistic methods. We will pick ρ uniformly from the set of all restrictions with $|\rho^{-1}(*)| = v - 4\sqrt{v}$ and $\Pr(\rho(x) = 0 \mid \rho(x) \neq *) = \frac{1}{2}$, and show that, with positive probability, the conditions of the lemma are fulfilled. Specifically, we will show that $\Pr(\neg\mathbf{G1}) + \Pr(\neg\mathbf{G2}) \leqq \frac{1}{2} + o(1)$.

Let us start with **G1:** Intuitively, the following lemma says that, with high probability, ρ does not give player I too much information about the colors of nodes in $\rho^{-1}(*)$.

LEMMA 4.4. $\Pr(\mu(Q^{\rho}_{\rho^{-1}(*)}) < 2^{-2(t+1)n^{\epsilon}}) \leqq \frac{1}{2} + o(1)$.

Proof. Let $\alpha = 2^{-(2t+1)n^{\epsilon}}$. Picking ρ uniformly from all restrictions with $|\rho^{-1}(*)| = v - 4\sqrt{v}$, is equivalent to picking randomly $T = \rho^{-1}(1) \cup \rho^{-1}(0)$ among all $4\sqrt{v}$-subsets of V, and then picking the restriction of ρ to T randomly among all vectors x in $\{0, 1\}^{4\sqrt{v}}$. Let $k = \sqrt{v}/4$. Say T is *bad* if

$$\mu\left(\left\{x : \mu(Ext_{Q,T}(x)) \geqq \frac{\alpha}{2k}\right\}\right) < \left(\frac{\alpha}{2}\right)^{2/k},$$

T is *good* otherwise. We have

$$\Pr\left(\mu(Q^{\rho}_{\rho^{-1}(*)}) < \frac{\alpha}{2k}\right) \leqq \Pr(T \text{ is bad}) + \Pr\left(\mu(Q^{\rho}_{\rho^{-1}(*)}) < \frac{\alpha}{2k} \,\middle|\, T \text{ is good}\right).$$

Note that $Q^{\rho}_{\rho^{-1}(*)} = Ext_{Q,T}(x)$. By the definition of goodness, and the choice of k, the second term is bounded by $1 - (\alpha/2)^{2/k} = o(1)$. Also note that $\alpha/2k \geqq 2^{-2(t+1)n^{\epsilon}}$. It remains to bound the first term: We pick a random T by first picking a random partition of V into $4\sqrt{v}$-subsets and then picking a random subset from the partition. We must show that for any partition, $\Pr(T \text{ is bad}) < \frac{1}{2}$ for a random T in the partition. But this is precisely the content of Corollary 4.4. □

Now we take care of **G2.**

Let $A^* = \{p \in A : p \subseteq \rho^{-1}(*)\}$. We say that ρ *kills* a vector $p_L \in A$ if there is no $p_R \in Ext(p_L)$ with $p_R \subseteq \rho^{-1}(1)$. We will show that for every choice of ρ, $\mu(A^*)$ is large and hence $\Pr(\neg\mathbf{G2}) \leqq \Pr(\exists p_L \in A \text{ killed by } \rho)$.

CLAIM 4.3. *For every* ρ, $\mu(A^*) \geqq \frac{1}{8} n^{-\epsilon}$.

Proof. Recall that $|\rho^{-1}(*)| = v - 4\sqrt{v}$ so that $|V \setminus \rho^{-1}(*)| = 4\sqrt{v}$. It is easy to see that at most a fraction $1 - [(v - 4\sqrt{v})/v]^{l'} \leqq \frac{1}{8} n^{-\epsilon}$ of the vectors in $[v]^{l'}$ intersect $V \setminus \rho^{-1}(*)$ so that at least a fraction $\frac{1}{4} n^{-\epsilon} - \frac{1}{8} n^{-\epsilon} \geqq \frac{1}{8} n^{-\epsilon}$ of them are in A^*. □

We now use some combinatorics to bound the probability that there exists a vector in A killed by ρ.

CLAIM 4.4. $\Pr(\exists p_L \in A$ *killed by* $\rho) = o(1)$.

Proof. We have

$$\Pr(\exists p_L \in A \text{ killed by } \rho) \leqq |A| \cdot \max_{p_L \in A} \{\Pr(p_L \text{ is killed by } \rho)\}$$

so let us look at the worst possible $p_L \in A$. Let $F \equiv (p_L$ is killed by $\rho)$. Note that $\Pr(F)$ depends only on $\rho^{-1}(1)$. We pick $\rho^{-1}(1)$ as follows: Pick a number t between 0 and $4\sqrt{v}$ according to the binomial distribution (i.e., $\Pr(t = i) = \binom{4\sqrt{v}}{i} 2^{-4\sqrt{v}}$). If $t < \sqrt{v}$, we assume that F fails. Otherwise, we pick a subset $T = \rho^{-1}(1)$ where $|T| = t$ by choosing $\sqrt{v}/l'$ independent random vectors $y_1 \cdots y_{\sqrt{v}/l'}$ from $[v]^{l'}$, putting all nodes in these vectors in T, and adding enough random nodes so that $|T| = t$. It is clear that we are simulating our original distribution on $\rho^{-1}(1)$. We can now estimate $\Pr(F)$ by

$$\begin{aligned} \Pr(F) &\leqq \Pr(t < \sqrt{v}) + \Pr(F \mid t \geqq \sqrt{v}) \\ &\leqq (2/e)^{\sqrt{v}} + \Pr(\forall i\, y_i \notin Ext(p_L)) \\ &\leqq (2/e)^{\sqrt{v}} + (1 - \mu(Ext(p_L)))^{\sqrt{v}/l'} \\ &\geqq \exp(-n^{1/5}) \end{aligned}$$

where we are using Chernoff's bound to estimate $\Pr(t < \sqrt{v})$ [Ch].

Recalling that $|A|$ is less than $n^{n^{1/10}}$, we easily conclude our calculations and get

$$\Pr(\exists p \in A \text{ killed by } \rho) \leqq n^{n^{1/10}} \cdot \exp(-n^{1/5}) = o(1).$$

We have $\Pr(\neg \mathbf{G1}) + \Pr(\neg \mathbf{G2}) \leqq \frac{1}{2} + o(1)$ implying the existence of a good restriction. Take any consistent extension of each $p_L \in A^*$ not killed by ρ to form $\bar{P}$. We have $\mu(\bar{P}_L) \geqq \frac{1}{8} n^{-\epsilon}$ and Lemma 4.3 is proved. □

Acknowledgments. We are very grateful to Miklós Ajtai for a conversation which led to the proof of Theorem 4.1. We are indebted to Johan Hastad for allowing us to present his improvements of our early results, and to Ravi Boppana for simplifying Claim 4.4. We are also thankful to Uri Zwick for helping us improve a previous draft.

REFERENCES

[AB] N. ALON AND R. BOPPANA, *The monotone circuit complexity of Boolean functions*, Combinatorica, 7 (1987), pp. 1–22.

[An] A. E. ANDREEV, *On a method for obtaining lower bounds for the complexity of individual monotone functions*, Sov. Math. Dokl., 31 (1985), pp. 530–534.

[Aj] M. AJTAI, Σ_1^1*-formulae on finite structures*, Ann. Pure Appl. Logic, 24 (1983), pp. 1–48.

[AF] M. AJTAI AND R. FAGIN, *Reachability is harder for directed than for undirected finite graphs*, Proceedings of 29th FOCS, White Plains, NY, 1988, pp. 358–367.

[AKLLR] R. ALELIUNAS, R. M. KARP, R. J. LIPTON, L. LOVASZ, AND C. RACKOFF, *Random walks, universal traversal sequences, and the complexity of maze problems*, Proceedings of 20th FOCS, San Juan, Puerto Rico, 1979, pp. 218–223.

[AKS] M. AJTAI, J. KOMLÓS, AND E. SZEMERÉDI, *An $O(n \log n)$ sorting network*, Proceedings 15th STOC, Boston, MA, 1983, pp. 1–9.

[Ch] H. CHERNOFF, *A measure of the asymptotic efficiency for tests of a hypothesis based on the sum of observations*, Ann. Math. Statist., 23 (1952), pp. 493–509.

[FSS] M. FURST, J. B. SAXE, AND M. SIPSER, *Parity circuits and the polynomial time hierarchy*, Proceedings of 22nd FOCS, Nashville, TN, 1981, pp. 260–270.

[H] J. HASTAD, *Improv*
CA, 1986, pp.

[KPPY] M. KLAWE, W. J. PA
depth, Proceed

[K] V. KHRAPCHENKO,
Notes Acad. S

[Ra] A. A. RAZBOROV,
Math. Dokl., 3

[Ru] W. L. RUZZO, *Tree*

[ShS] E. SHAMIR AND M.
pp. 301–322.

[S] P. M. SPIRA, *On t*
Hawaii Symp.

[V] L. G. VALIANT, *Sh*
363–366.

[Y1] A. C.-C. YAO, *Som*
STOC, Atlant

[Y2] ———, *Separatin*
pp. 1–10.

[H] J. HASTAD, *Improved lower bounds for small depth circuits*, Proceedings of 18th STOC, Berkeley, CA, 1986, pp. 6–20.

[KPPY] M. KLAWE, W. J. PAUL, N. PIPPENGER, AND M. YANNAKAKIS, *On Monotone formulae with restricted depth*, Proceedings of 16th STOC, Washington, DC, 1984, pp. 480–487.

[K] V. KHRAPCHENKO, *A method of determining lower bounds for the complexity of Π schemes*, Math. Notes Acad. Sci. USSR, (2) 1971, pp. 474–479.

[Ra] A. A. RAZBOROV, *Lower bounds for the monotone complexity of some Boolean functions*, Sov. Math. Dokl., 31 (1985), pp. 354–357.

[Ru] W. L. RUZZO, *Tree-size bounded alternation*, J. Comput. System Sci., 21 (1980), pp. 218–235.

[ShS] E. SHAMIR AND M. SNIR, *On the depth complexity of formulas*, Math. Systems Theory, 13 (1980), pp. 301–322.

[S] P. M. SPIRA, *On time-hardware complexity tradeoffs for Boolean functions*, Proceedings of 4th Hawaii Symp. on System Sciences, 1971, pp. 525–527.

[V] L. G. VALIANT, *Short monotone formulae for the majority function*, J. Algorithms, 5 (1984), pp. 363–366.

[Y1] A. C.-C. YAO, *Some complexity questions related to distributive computing*, Proceedings of 11th STOC, Atlanta, GA, 1979, pp. 209–213.

[Y2] ———, *Separating the polynomial-time hierarchy by oracles*, Proceedings of 26th FOCS, 1985, pp. 1–10.