comput complexity 5 (1995), 191–204 1016-3328/95/040191-14 $1.50+0.20

SUPER-LOGARITHMIC DEPTH LOWER BOUNDS VIA THE DIRECT SUM IN COMMUNICATION COMPLEXITY

MAURICIO KARCHMER, RAN RAZ, AND AVI WIGDERSON

Abstract. Is it easier to solve two communication problems together than separately? This question is related to the complexity of the composition of boolean functions. Based on this relationship, an approach to separating NC^1 from P is outlined. Furthermore, it is shown that the approach provides a new proof of the separation of monotone NC^1 from monotone P.
Key words. Lower-bound; complexity; direct-sum; circuit.
Subject classifications. 68Q15, 68Q25.

1. Introduction

The communication complexity model was first studied by Yao [22]. It was originally motivated by applications to distributed computing and VLSI, where it captures essential features in an natural way (see [2] and the references within). Recently, unexpected connections were found between this model and seemingly unrelated areas of combinatorial optimization [21] and circuit complexity [15].

A very natural question to ask is the "direct sum" question: Is it easier to solve two problems together than separately? This question is related, in its essence, to similar questions in algebraic complexity [3] and other models [7]. For the original model of Yao [22], in which the problems are Boolean functions, we give lower bounds for the amount of savings possible. Our main interest, though, is in the case of search problems, or relations. This is because of the equivalence between communication complexity of relations and circuit depth [15]. In particular, we will informally relate the direct sum question to the complexity of the composition of boolean functions.

The key observation which motivates this paper is that if the depth complexity of the composition of two functions is close to the sum of the individual complexities, then NC^1 is different from P. This direction provides an explicit family of functions, quite different from P-complete functions, for which this approach can lead to super-logarithmic lower bounds.

We test the feasibility of our approach in two settings. One is the setting of universal relations, which abstract the role of the functions involved. The second is the setting of monotone computation. Both settings provide encouraging answers. For universal relations, the lower bounds for composition were proven by Edmonds *et al.* in [4]. For monotone computation, we give here a simple new proof of the separation between the monotone analogues of NC^1 and P. This was first proved by Karchmer & Wigderson in [15].

2. Preliminaries

Consider three finite sets X, Y, and Z, and a ternary relation $R \subseteq X \times Y \times Z$. Given such a relation, consider the following *game* between players I and II: For $(x, y) \in X \times Y$, give x to player I and y to player II. Their goal is to agree on any $z \in Z$ with the proviso that $(x, y, z) \in R$. Let $C(R)$ be the communication complexity of the above problem.

This model, for the case where R defines a function $F : X \times Y \mapsto Z$ has been extensively studied in the literature [22],[16],[2]. In particular, Mehlhorn & Schmidt [16] gave a useful way of obtaining a lower bound on $C(F)$ from the rank of an associated matrix. Let K be any field, and assume without loss of generality that $Z \subseteq K$. Let $M(F)$ be a matrix whose rows (columns) are labeled by elements of X (respectively Y), and whose (x, y) entry is $F(x, y)$. Then, if rk is the rank function of matrices over K, we have the following result. (The logarithm in this paper is always taken base 2.)

PROPOSITION 2.1 ([16]). $C(F) \geq \log \mathrm{rk}(M(F))$.

For general relations (search problems), the model was studied in [15],[12] with the following motivation. Let $f : \{0,1\}^n \mapsto \{0,1\}$ be a Boolean function, and let $d(f)$ be the minimal depth of a boolean circuit computing f. Let $[n] = \{1, \ldots, n\}$. Define the relation $R_f \subseteq f^{-1}(1) \times f^{-1}(0) \times [n]$ by $(x, y, i) \in R_f$ if and only if $x_i \neq y_i$. The following theorem is our starting point.

THEOREM 2.2 ([15]). *For every f, $d(f) = C(R_f)$.*

For monotone computation, we have a similar theorem. Let $f : \{0,1\}^n \mapsto \{0,1\}$ be a monotone function, and let $d_m(f)$ be the minimal depth of a monotone boolean circuit computing f. Let $\min(f)$ and $\max(f)$ be the set of *minterms* and *maxterms* of f. Recall that $p \subseteq [n]$ is in $\min(f)$ (respectively $\max(f)$) if it is a minimal subset with the property that assigning the value 1 (respectively 0) to the variables in p forces f to output 1 (respectively 0). We define the monotone relation associated with f, $R_f^m \subseteq \min(f) \times \max(f) \times [n]$, by $(p, q, i) \in R_f^m$ if and only if $i \in p \cap q$. Now we have the following result.

THEOREM 2.3 ([15]). *For every monotone f, $d_m(f) = C(R_f^m)$.*

In what follows, we will use the notion of reducibilities between relations.

DEFINITION 2.4. *Let $R \subseteq X \times Y \times Z$ and $R' \subseteq X' \times Y' \times Z'$. We say that R is* reducible *to R', $R \leq R'$, if there exist functions $\phi_I : X \mapsto X'$, $\phi_{II} : Y \mapsto Y'$ and $\psi : Z' \mapsto Z$ such that for every $(x, y) \in X \times Y$,*

$$(\phi_I(x), \phi_{II}(y), z') \in R' \Rightarrow (x, y, \psi(z')) \in R.$$

The motivation for the above definition is contained in the following lemma.

LEMMA 2.5. *Let $R \subseteq X \times Y \times Z$ and $R' \subseteq X' \times Y' \times Z'$. If $R \leq R'$, then $C(R) \leq C(R')$.*

We will also use a more general definition of reducibilities which can be defined as follows, in informal terms: We say that $R \leq_\alpha R'$ if there is a protocol for R that first obtains a result z' for an instance of R' as above, and then uses α extra bits of communication to find a solution z of R. In this way, if $R \leq_\alpha R'$, then $C(R) \leq C(R') + \alpha$. See [12] for further details concerning reductions.

We will use the following "disjointness" functions: Let $\mathcal{P}([n])$ denote the power set of $[n]$ and let $\mathcal{P}_l([n])$ denote the collection of all subsets of $[n]$ of size l. Let $I_n : \mathcal{P}([n]) \times \mathcal{P}([n]) \mapsto \{0, 1\}$ where $I_n(S, T) = 0$ iff $S \cap T = \emptyset$. Also, for $l \leq n/2$, let $I_{l,n} : \mathcal{P}_l([n]) \times \mathcal{P}_l([n]) \mapsto \{0, 1\}$ where $I_{l,n}(S, T) = 0$ iff $S \cap T = \emptyset$. It is well known that the associated matrices have full rank over the reals.

THEOREM 2.6 ([11]). *Over the reals, $\mathrm{rk}(M(I_n)) = 2^n$ and $\mathrm{rk}(M(I_{l,n})) = \binom{n}{l}$.*

COROLLARY 2.7. *$C(I_n) \geq n$ and $C(I_{l,n}) \geq \log \binom{n}{l}$.*

3. Direct sum of relations

Definition 3.1. *Given two relations* $R \subseteq X \times Y \times Z$ *and* $R' \subseteq X' \times Y' \times Z'$ *we define the* direct sum *(or* tensor product*), as follows:*

$$R \otimes R' \subseteq (X \times X') \times (Y \times Y') \times (Z \times Z'),$$

where $((x_1, x_2), (y_1, y_2), (z_1, z_2)) \in R \otimes R'$ *if and only if* $(x_1, y_1, z_1) \in R$ *and* $(x_2, y_2, z_2) \in R'$.

Intuitively, $R \otimes R'$ corresponds to solving instances of R and R' simultaneously. Given any relation R and $k \geq 1$ we define the relation $R^{(k)}$ by $R^{(1)} = R$ and $R^{(k)} = R \otimes R^{(k-1)}$. The following definition arises naturally.

Definition 3.2. *For a relation* R*, define the* amortized *complexity of* R*,* $\Phi(R)$*, as follows:*

$$\Phi(R) = \inf_k \left\{ \frac{1}{k} \cdot C(R^{(k)}) \right\}.$$

Open Question 3.3. *What is the relation between* $C(R \otimes R')$ *and* $C(R) + C(R')$*?*

Clearly, $C(R \otimes R') \leq C(R) + C(R')$. Feder *et al.* [6] give an example where $C(R \otimes R) = C(R) + O(1)$. In the example, $C(R) = O(\log n)$ (where n is the input size) so it may be that one can never save more than an additive amount of $O(\log n)$. In fact, it was proven in [6] that for the case of non-deterministic complexity, one can never save more than an additive factor of $O(\log n)$.

For functions, the situation is simpler. We give below two lower bounds on the possible savings in computing direct sum of functions.

The first one is based on the fact that the rank of matrices is multiplicative with respect to tensor product, and implies that the rank lower bound of Proposition 2.1 is additive with respect to the direct sum of functions.

Proposition 3.4. *For* R, R' *functions, we have*

$$C(R \otimes R') \geq \log \mathrm{rk}(M(R)) + \log \mathrm{rk}(M(R')).$$

Proof. For two matrices M and M' over the same field K, denote by $M \otimes M'$ their (standard) tensor product. It is well known that $\mathrm{rk}(M \otimes M') = \mathrm{rk}(M)\mathrm{rk}(M')$.

Assume that the answer sets Z, Z' of R, R' are subsets of the field K, and let $R \cdot R' : (X \times X') \times (Y \times Y') \to K$ be the function defined by $R \cdot R'((x, x'), (y, y')) = R(x, y)R'(x', y')$ (multiplication in K). Note that $M(R \cdot R') = M(R) \otimes M(R')$. It is easy to see that a trivial reduction gives $R \otimes R' \geq R \cdot R'$. Therefore, using Proposition 2.1, we have

$$\begin{aligned} C(R \otimes R') &\geq C(R \cdot R') \\ &\geq \log \mathrm{rk}(M(R) \otimes M(R')) \\ &\geq \log \mathrm{rk}(M(R)) + \log \mathrm{rk}(M(R')). \square \end{aligned}$$

COROLLARY 3.5. *If R is a function, then $\Phi(R) \geq \log \mathrm{rk}(M(R))$ over any field.*

The relationship between the logarithm of the rank and communication complexity is not known, and there may be an exponential gap between them. Thus, we give here another lower bound on the amortized communication complexity of functions in terms of its communication complexity. The same result was independently obtained in [6]. The reader is referred to the very nice proof given in [6].

THEOREM 3.6. *For a function R with $C(R) \geq 2(\log n)^2$ (again, n is the input size), we have*

$$\Phi(R) = \Omega(\sqrt{C(R)}).$$

4. Composition of boolean functions

Let B_n denote the set of all boolean functions on n variables. Given $f \in B_n$ and $g \in B_m$, we define the composition $f \diamond g : \{0,1\}^{nm} \mapsto \{0,1\}$ as follows:

$$f \diamond g(\vec{X}_1, \ldots, \vec{X}_n) = f(g(\vec{X}_1), \ldots, g(\vec{X}_n)),$$

where $\vec{X}_i \in \{0,1\}^m$ for $1 \leq i \leq n$. (i.e., the input variables for $f \diamond g$ are given in a matrix. We first apply g on each row of the matrix, and then apply f on the vector of the results). For $k \geq 1$, we define a function $f^{(k)}$ by $f^{(1)} = f$ and $f^{(k)} = f \diamond f^{(k-1)}$.

We believe that $C(R_{f \diamond g})$ may be related to $C(R_f) + C(R_g)$. To understand why, one has to look closely at the game defined by $R_{f \diamond g}$. Player I gets a vector $(\vec{X}_1, \ldots, \vec{X}_n)$ which induces a vector $\vec{x} \in f^{-1}(1)$ by $x_i = g(\vec{X}_i)$. Similarly, player II gets a vector $(\vec{Y}_1, \ldots, \vec{Y}_n)$ which induces a vector $\vec{y} \in f^{-1}(0)$. Suppose that the vectors are such that if $x_i = y_i$ then $\vec{X}_i = \vec{Y}_i$. Then an answer (i, j) for the game $R_{f \diamond g}$ will provide us with an answer i for R_f and an answer j for an instance of R_g.

Therefore, when one looks at the relation $R_{f \diamond g}$, one gets the impression that to solve it, one will have to solve an instance of R_f and an instance of R_g (obviously, solving an instance of R_f and an instance of R_g will be enough). A natural question to ask here is the following.

OPEN QUESTION 4.1. *What is the relation between $C(R_{f \diamond g})$ and $C(R_f) + C(R_g)$?*

Clearly, $C(R_{f \diamond g}) \leq C(R_f) + C(R_g)$. As pointed out by Sipser [20], we can have strict inequality if we let $f = g = x_1 \oplus x_2 \oplus x_3$. Pudlák [17] gave an example with an additive gap that tends to infinity. He shows that taking $f = g = T_2^n$ (where T_2^n is the threshold 2 function) gives $C(R_{f \diamond g}) \leq C(R_f) + C(R_g) - \log \log n$. We know of no example that achieves a bigger gap. In the next section, we will argue that if $C(R_{f \diamond g})$ is not too far from $C(R_f) + C(R_g)$, then $NC^1 \neq P$.

The only nontrivial case when such a lower bound can be proven was proposed by Andreev [1], and was a main source of inspiration for this paper. Let $\oplus_n$ be the parity function on n bits. Implicit in [1] is the following theorem.

THEOREM 4.2 ([1]).

$$C(R_{f \diamond \oplus_n}) \geq C(R_f) + \frac{3}{4} C(R_{\oplus_n}) - O(\log \log n).$$

After a sequence of improvements, an essentially optimal bound for this case was obtained by Hastad [8].

THEOREM 4.3 ([8]).

$$C(R_{f \diamond \oplus_n}) \geq C(R_f) + C(R_{\oplus_n}) - O(\log \log n).$$

Both results in fact give the corresponding stronger result for formula size. They use random restriction arguments, which go particularly well with functions like parity but seem to be inadequate for our purposes, as may become clearer in the next section.

5. Compositions of functions and NC^1 vs. P

In this section, we will relate the notion of composition to the NC^1 versus P question. The main idea is that if we start with a hard function on a few bits and compose it with itself many times, then we will hopefully get a function on n variables with super-logarithmic depth complexity but which can be defined in P (and even in NC^2). The following theorem shows that some possible answers to Question 4.1 imply $NC^1 \neq P$. Note that the condition we need is much weaker than the separation provided by the examples in the previous section.

THEOREM 5.1. *If for some $1 \geq \epsilon > 0$, every f satisfies $C(R_{f\diamond f}) \geq (1+\epsilon)C(R_f)$, then $NC^1 \neq NC^2$.*

PROOF. Take $k = \log n/\log\log n$ and let $f \in B_{\log n}$ be the hardest function on $\log n$ variables so that $d(f) = C(R_f) = \Omega(\log n)$. Then, $f^{(k)}$ has n variables and it is readily seen to be in NC^2. But

$$\begin{aligned} C(R_{f^{(k)}}) &\geq (1+\epsilon)\cdot C(R_{f^{(k/2)}}) \\ &\geq (1+\epsilon)^{\log k}\cdot C(R_f) \\ &= k^{\log(1+\epsilon)}\cdot \Omega(\log n) \\ &= \Omega(\log^{1+\epsilon'} n/\log\log n) \end{aligned}$$

so that $f^{(k)} \notin NC^1$. □

Note that we do not need an explicit description of f. We could take f to be a random function. Also, we do not need the full strength of the assumption of the theorem. We can weaken the assumptions in many ways without weakening the conclusion. For example, we have the following theorem.

THEOREM 5.2. *If for a random function f and for every g, $C(R_{f\diamond g}) \geq C(R_g) + \epsilon\cdot C(R_f)$, then $NC^1 \neq NC^2$.*

PROOF. Let $f_1, \ldots, f_k$ be k random functions on $\log n$ variables each. Obviously, $\forall i\ C(R_{f_i}) = \Omega(\log n)$. Using the assumption, an inductive argument shows that $C(R_{f_1\diamond\cdots\diamond f_k}) \geq \sum_{i=1}^k \epsilon\cdot C(R_{f_i})$. This is true by taking $f = f_1$, $g = f_2 \diamond \cdots \diamond f_k$ in the assumption, and using the inductive hypothesis that $C(R_g) \geq \sum_{i=2}^k \epsilon\cdot C(R_{f_i}))$. Choosing $k = \log n/\log\log n$ as before yields a function $f_1 \diamond \cdots \diamond f_k$ in NC^2 which requires $\Omega(\log^2 n/\log\log n)$ depth. □

And so on and so forth. Also, by noting that any function on $\log n$ variables can be described with only n bits, the above theorems yield a separation between non-uniform NC^1 and uniform NC^2.

6. The universal relation for composition

One way to test our approach is by introducing a "universal" relation that abstracts away the role of a particular function in the composition. We define a communication problem $U_{k,n}$ as follows: Let T be a balanced, degree n, depth k tree. Players I and II have labelings φ_I and φ_{II}, respectively, each mapping every node of T to $\{0,1\}$. The pair $(\varphi_I, \varphi_{II})$ is legal if the following conditions hold:

(1) $\varphi_I(r) \neq \varphi_{II}(r)$, where r is the root of T,

(2) if $\varphi_I(v) \neq \varphi_{II}(v)$, then there is a son u of v such that $\varphi_I(u) \neq \varphi_{II}(u)$.

The goal of the players is to agree on a leaf l of T such that $\varphi_I(l) \neq \varphi_{II}(l)$ if $(\varphi_I, \varphi_{II})$ is legal. In case the input pair is illegal, the players can output any answer.

The following lemma shows why we call $U_{k,n}$ the *Universal Relation for Composition.*

LEMMA 6.1. *For any* $f_1, \ldots, f_k \in B_n$, $R_{f_1 \diamond \cdots \diamond f_k} \leq U_{k,n}$.

PROOF. Let $f = f_1 \diamond \cdots \diamond f_k$. A circuit for f can be described by putting in every node of T of depth i, $0 \leq i \leq k-1$, a gate of the function f_{i+1}, and letting the leaves be the input wires in the natural order. Every input to f gives a truth value to every node in T in the natural way, by evaluating the subcircuit rooted at this node. Finally, observe that the labelings φ_I, φ_{II} obtained in this way from two inputs x_I, x_{II} (for the two players in the game R_f) form a legal pair. Thus, we have just described the required reduction from R_f to $U_{k,n}$. □

Note that $f_1 \diamond \cdots \diamond f_k$ has n^k variables, and that $C(U_{k,n}) \leq kn(1 + o(1))$. In [14], we conjectured that this bound is tight, with the obvious motivation of testing our approach. This conjecture was proved by Edmonds *et al.* [4]. They used beautiful information theoretic arguments to measure the progress made (in a top-down direction) by an arbitrary protocol on successive levels of the composition, and proved the following strong bound.

THEOREM 6.2 ([4]). $C(U_{k,n}) \geq kn - O(k^2\sqrt{n \log n})$.

A completely different method was used by Hastad & Wigderson [9] to give a slightly stronger lower bound. They use a bottom-up approach that utilizes a Nečiporuk-like subadditive measure on protocols.

THEOREM 6.3 ([9]). $C(U_{k,n}) \geq kn - O(k^3 \log k)$.

Note that both lower bounds leave open whether $C(U_{k,n}) = \Omega(kn)$ when $k \geq \sqrt{n}$. While this range is not too interesting when replacing the universal problem by real functions, determining $U_{k,n}$ in this range remains an interesting problem in communication complexity.

7. The monotone universal relation for composition

In this section, we define the monotone analogue $U^m_{k,n}$ of the universal relation, and prove a tight lower bound for its communication complexity, for all values of k and n.

Let T be as before. Let players I and II have labelings φ_I and φ_{II}, respectively, mapping every node of T to $\{0,1\}$. This time, the pair $(\varphi_I, \varphi_{II})$ is legal if the following conditions hold:

(1) $\varphi_I(r) = \varphi_{II}(r) = 1$,

(2) if $\varphi_I(v) = \varphi_{II}(v) = 1$, then there is a son u of v such that $\varphi_I(u) = \varphi_{II}(u) = 1$.

The goal of the players is to agree on a leaf l of T such that $\varphi_I(l) = \varphi_{II}(l) = 1$ if $(\varphi_I, \varphi_{II})$ is legal. In case the input pair is illegal, the players can output any answer.

The following lemma is the analogue to Lemma 6.1. We omit its proof which is essentially the same.

LEMMA 7.1. *For any monotone* $f_1, \ldots, f_k \in B_n$, $R^m_{f_1 \diamond \cdots \diamond f_k} \leq U^m_{k,n}$.

For this problem, it is much easier to prove a tight lower bound which relies on a connection between the monotone universal relation and the set disjointness problem. This connection was also used in [18].

THEOREM 7.2. $C(U^m_{k,n}) \geq nk - 2$.

PROOF. Observe that $U^m_{1,n}$ is the problem in which every player gets a subset of $[n]$ as input, and their task is to find a member of the intersection if it is nonempty. This gives the simple reduction $I_n \leq_2 U^m_{1,n}$, in which both players, after receiving the result of $U^m_{1,n}$ on their input subsets, check that indeed it is a member of their input.

It is natural to seek a similar reduction from $I_n^{(k)}$ to $U_{k,n}^m$, but we are not convinced that one exists. Rather, we define a weaker function $I_n^{(\wedge k)}$, and reduce it to $U_{k,n}^m$. As for $I_n^{(k)}$, the players get k pairs of subsets of $[n]$ (each player gets one set from each pair), but rather than deciding for each pair if it is intersecting, they are required only to output 1 if all k pairs are intersecting, and 0 otherwise (i.e., if some pair has empty intersection). It is easy to see that $M(I_n^{(\wedge k)})$ is the kth tensor power of $M(I_n)$. By Propositions 2.1 and 2.2, we have $C(I_n^{(\wedge k)}) \geq kn$.

Note that k sets $S_1, S_2, \ldots, S_k$ can be used to define a labeling of T in the following way: the root is labeled 1, and the node at depth j defined by the path $i_1, i_2, \ldots, i_j$ is labeled 1 iff for all $1 \leq l \leq j$, we have $i_l \in S_l$ (it is labeled 0 otherwise).

Given inputs for $I_n^{(\wedge k)}$, the players can use this procedure to define labelings φ_I,φ_{II}. It is easy to check that in this case, the pair $(\varphi_I, \varphi_{II})$ is legal for $U_{k,n}^m$ iff there exists a leaf l of T such that $\varphi_I(l) = \varphi_{II}(l) = 1$. This occurs iff all the k input pairs for $I_n^{(\wedge k)}$ consist of intersecting subsets. The reduction $I_n^{(\wedge k)} \leq_2 U_{k,n}^m$ is given now by applying a protocol for $U_{k,n}^m$ on the pair $(\varphi_I, \varphi_{II})$, and checking that indeed both labelings have 1 on the answer.

Therefore, we have $C(U_{k,n}^m) \geq C(I_n^{(\wedge k)}) - 2 \geq nk - 2$. □

8. The approach and mNC^1 vs. mP

In this section, we show that the proposed approach provides us with a simple new way of separating the monotone classes mNC^1 from mP. This separation was first proved in [15] by providing an $\Omega((\log n)^2)$ monotone depth lower bound for the st-connectivity function. That proof relied on complicated combinatorial and probabilistic arguments. In contrast, the new proof uses a sequence of simple reductions, following the monotone version of the ideas in Section 5. Still, we remark that the lower bound obtained here is only $\log n \log\log n$. This bound can be slightly improved, using the fact that the complexity of the function f below is $O(n^{\log n})$.

Recall that the intuition behind our belief that $C(R_{f\diamond g})$ is close to $C(R_f) + C(R_g)$ was that, to solve $R_{f\diamond g}$, we have to solve an instance of R_f and an instance of R_g. In the monotone case, we can prove the following result.

LEMMA 8.1. *For every monotone f, g, $R_f^m \otimes R_g^m \leq R_{f\diamond g}^m$.*

PROOF. A minterm (or maxterm) of $f \diamond g$ consists of a minterm m_f (or a maxterm M_f) of f and for each $i \in m_f$ (or $i \in M_f$) a minterm m_g^i (or a maxterm M_g^i, respectively) of g. This understood, we can define the reduction by letting the pair (m_f, m_g) be mapped to the minterm of $f \diamond g$ defined by $m_g^i = m_g$ for every i, and similarly with the maxterms. $\square$

COROLLARY 8.2. $C(R_f^m \otimes R_g^m) \leq C(R_{f\diamond g}^m)$.

COROLLARY 8.3. $(R_f^m)^{(k)} \leq R_{f^{(k)}}^m$.

If we could find a monotone function f such that $C((R_f^m)^{(k)}) = \omega(k \log n)$, then we would have $mNC^1 \neq mP$ by the above considerations. Fortunately, the following theorem is implicit in Razborov [19], and was made explicit in [12].

THEOREM 8.4 ([19],[12]). *Let $l = c \log n$ for some suitable $c > 0$. There exists a monotone function f on n variables such that $I_{l,n} \leq_1 R_f^m$.*

In fact, the function f can be explicitly described—it is the SET-COVERING problem. However, this is not important for us. We also remark that while this theorem is the only step in the whole proof that is technically nontrivial, this reduction is reasonably simple.

COROLLARY 8.5. *For f and l as above, $I_{l,n}^{(k)} \leq_k (R_f^m)^{(k)} \leq R_{f^{(k)}}^m$.*

We can now give a simple proof that $mNC^1 \neq mP$.

THEOREM 8.6. $mNC^1 \neq mP$.

PROOF. To apply the ideas of Section 5, we scale the number of variables logarithmically. Let $l = c \log\log n$ and f be the function on $\log n$ variables given by Theorem 8.4. $C(R_{f^{(k)}}^m) \geq C(I_{l,\log n}^{(k)}) = \Omega(k(\log\log n)^2)$ follows from Corollary 8.5, the additivity of the rank lower bound (Proposition 3.4) and Theorem 2.6. If $k = \log n / \log\log n$, then $f^{(k)}$ has n variables and $C(R_{f^{(k)}}^m) = \Omega(\log n \cdot \log\log n)$.

Note that it does not matter if f is an explicit function or not; as it has only $\log n$ variables, its truth table could be given as an extra n input bits. $\square$

9. Conclusions and future work

In this paper, we have presented a concrete new approach for proving non-monotone super-logarithmic lower bounds for circuit depth. This approach has generated new types of questions in communication complexity, which were studied here and in subsequent papers [6],[13],[4],[9], some of which show that this approach is useful in restricted settings. We feel that the results obtained so far are encouraging enough to seriously attempt to use this approach for the general model, and we make it somewhat more concrete below.

Our approach suggests to consider the following: first, the intuition that to solve $R_{f\circ g}$ one has to solve an instance of R_f and an instance of R_g; second, the intuition that one cannot save much by solving two problems together. The following plan to show $NC^1 \neq NC^2$ comes to mind.

(1) Show that $C(R_{f^{(k)}})$ is close to $C(R_f^{(k)})$.

(2) Show that there is a hard function $f \in B_n$ such that $C(R_f^{(k)}) = \omega(k \log n)$.

Note that Item 2 asks for the existence, rather than for an explicit construction, of a hard function.

OPEN QUESTION 9.1. *Is there a function $f \in B_n$ such that $\Phi(R_f) = \omega(\log n)$?*

An affirmative answer will put us half way through our plan. A negative answer, on the other hand, will break most of our intuition. It is worthwhile to note that Khrapchenko's lower bound [11] is additive with respect to $\otimes$ so that $\Phi(R_{\oplus_n}) \geq 2 \log n$ where $\oplus_n$ is the parity of n variables. Also, it is not hard to show that $\Phi(U_{1,n}) \geq n - 1$. We believe that Φ is not far from C.

Acknowledgements

A preliminary version of the paper appeared in the 6th Symposium on Structure in Complexity Theory. Research of Mauricio Karchmer supported by NSF grant NSF-CCR-90-10533. Research of Avi Wigderson Supported by the American-Israeli Binational Science Foundation grant 89-00126.

References

[1] A. E. ANDREEV, On a Method for Obtaining more than Quadratic Effective Lower Bounds for the Complexity of π-Schemes. *Moscow University Math. Bull.* **42**:1 (1987).

[2] A. V. AHO, J. D. ULLMAN, AND M. YANNAKAKIS, On Notions of Information Transfer in VLSI Circuits. In *Proc. Fifteenth Ann. ACM Symp. Theor. Comput.*, 1983, 133–139.

[3] N. H. BSHOUTY, On the Extended Direct Sum Conjecture. In *Proc. Twenty-first Ann. ACM Symp. Theor. Comput.*, 1989, 177–185.

[4] J. EDMONDS, R. IMPAGLIAZZO, S. RUDICH, AND J. SGALL, Communication Complexity towards Lower Bounds on Circuit Depth. In *Proc. 32nd Ann. IEEE Symp. Found. Comput. Sci.*, 1991, 249–257.

[5] T. FEDER, *Personal communication*, 1990.

[6] T. FEDER, E. KUSHILEVITZ, AND M. NAOR, Amortized Communication Complexity. In *Proc. 32nd Ann. IEEE Symp. Found. Comput. Sci.*, 1991, 239–248.

[7] G. GALIBATI AND M. J. FISCHER, On the Complexity of 2-Output Boolean Networks. *Theoret. Comput. Sci.* **16** (1981), 177–185.

[8] J. HASTAD, The Shrinkage Constant is 2. In *Proc. 34th Ann. IEEE Symp. Found. Comput. Sci.*, 1993, 114–123.

[9] J. HASTAD AND A. WIGDERSON, Composition of the Universal Relation. In *Amer. Math. Soc.—DIMACS series*, ed. J. Y. CAI, to appear.

[10] V. KHRAPCHENKO, A Method of Determining Lower Bounds for the Complexity of π-Schemes. *Math. Notes Acad. Sci. USSR* (1971), 474–479.

[11] W. M. KANTOR, On Incidence Matrices of Finite Projective and Affine Spaces. *Math. Z.* **124** (1972), 315–318.

[12] M. KARCHMER, *Communication Complexity: A new Approach to Circuit Depth.* MIT Press, 1989.

[13] M. KARCHMER, E. KUSHILEVITZ, AND N. NISAN, Fractional Covers and Communication Complexity. In *Proc. 7th Ann. IEEE Conf. Structure in Complexity Theory*, 1992, 262–274.

[14] M. KARCHMER, R. RAZ, AND A. WIGDERSON, On Proving Super-Logarithmic Depth Lower Bounds via the Direct Sum in Communication Complexity. In *Proc. 6th Ann. IEEE Conf. Structure in Complexity Theory*, 1991.

[15] M. KARCHMER AND A. WIGDERSON, Monotone Circuits for Connectivity Require Super-Logarithmic Depth. *SIAM J. Disc. Math.* **3**:2 (1990), 255–265.

[16] K. MEHLHORN AND E. M. SCHMIDT, Las Vegas is Better than Determinism in VLSI and Distributive Computing. In *Proc. Fourteenth Ann. ACM Symp. Theor. Comput.*, 1982, 330–337.

[17] P. PUDLÁK, *Personal communication*, 1992.

[18] R. RAZ AND A. WIGDERSON, Probabilistic Communication Complexity of Boolean Relations. In *Proc. 30th Ann. IEEE Symp. Found. Comput. Sci.*, 1989, 562–567.

[19] A. A. RAZBOROV, Applications of Matrix Methods for the Theory of Lower Bounds in Computational Complexity. *Combinatorica* **10**:1 (1990), 81–93.

[20] M. SIPSER, *Personal communication*, 1988.

[21] M. YANNAKAKIS, Expressing Combinatorial Optimization Problems by Linear Programs. In *Proc. Twentieth ACM Symp. Theor. Comput.*, 1988, 223–228.

[22] A. C. C. YAO, Some Complexity Questions Related to Distributive Computing. In *Proc. Eleventh Ann. ACM Symp. Theor. Comput.*, 1979, 209–213.

Manuscript received 15 December 1994

M. KARCHMER
Dept. of Mathematics
M.I.T
Cambridge, MA 02139

R. RAZ
Dept. of App. Mathematics
Weizmann Institute
Rehovot 76100, Israel
ranraz@wisdom.weizmann.ac.il

A. WIGDERSON
Dept. of Computer Science
Hebrew University
Jerusalem, Israel
avi@cs.huji.ac.il

Current address of M. KARCHMER:
ITG Inc.
44 Farnsworth St., 9th floor
Boston, MA 02210
karchmer@itginc.com