Theoretical Informatics and Applications
Theoret. Informatics Appl. **35** (2001) 277–286

DEPTH LOWER BOUNDS FOR MONOTONE SEMI-UNBOUNDED FAN-IN CIRCUITS *

Jan Johannsen[1]

Abstract. The depth hierarchy results for monotone circuits of Raz and McKenzie [5] are extended to the case of monotone circuits of semi-unbounded fan-in. It follows that the inclusions $NC^i \subseteq SAC^i \subseteq AC^i$ are proper in the monotone setting, for every $i \geq 1$.

Mathematics Subject Classification. 68Q17, 68Q15.

1. Introduction

We consider boolean circuits over the basis $\{\wedge, \vee\}$, with gates of arbitrary fan-in and having negated and positive variables as inputs. A circuit is called *monotone* if it has no negated inputs; clearly, a monotone circuit can only compute a monotone boolean function.

We call the maximal fan-in of any $\vee$-gate (resp. $\wedge$-gate) in a circuit C the $\vee$-fan-in (resp. the $\wedge$-fan-in) of C. A circuit family has *semi-unbounded* fan-in if each circuit in the family has $\wedge$-fan-in 2, but arbitrary $\vee$-fan-in. This class of circuits was introduced by Venkateswaran [6] in order to give a circuit characterization of the class $LOGCFL$ of problems logspace-reducible to context-free languages.

Let SAC^i denote the class of boolean functions computable by semi-unbounded fan-in circuit families of polynomial size and depth $O(\log^i n)$, so that $NC^i \subseteq SAC^i \subseteq AC^i$. Since Borodin *et al.* [1] have shown that SAC^i is closed under complementation for every i, this is equal to the class of functions computable by polynomial size, depth $O(\log^i n)$ circuit families of $\vee$-fan-in 2 and unbounded

Keywords and phrases: Monotone circuit, semi-unbounded fan-in, communication complexity, lower bound.

* *Supported by the DFG Emmy-Noether-Programme under grant No. Jo 291/2-1.*

[1] Institut für Informatik, Ludwig-Maximilians-Universität München, Oettingenstraße 67, 80538 München, Germany; e-mail: `jjohanns@informatik.uni-muenchen.de`

$\wedge$-fan-in. The characterization given by Venkateswaran [6] is that $LOGCFL$ equals logspace-uniform SAC^1.

Monotone circuits of semi-unbounded fan-in were considered by Grigni and Sipser [2], who extended the $\Omega(\log^2 n)$ depth lower bound for bounded fan-in monotone circuits computing *st*-connectivity of Karchmer and Wigderson [3] to monotone circuits with $\wedge$-gates of fan-in $O(2^{n^{1-\delta}})$ for some $\delta > 0$.

Following Grigni and Sipser [2], for a circuit complexity class C, we write mC for the corresponding monotone circuit complexity class. In particular, we denote by $mSAC^i$ the class of functions computable by monotone semi-unbounded fan-in circuits of polynomial size and depth $O(\log^i n)$, and by $co\text{-}mSAC^i$ the dual class, with bounded $\vee$-fan-in and unbounded $\wedge$-fan-in. More generally, we call a monotone circuit with bounded $\wedge$-fan-in and unbounded $\vee$-fan-in (or $\vee$-fan-in bounded by a growing function of n) an $mSAC$-circuit, and analogously we define $co\text{-}mSAC$-circuits.

Recently, Raz and McKenzie [5] have shown a tight depth hierarchy for monotone circuits up to a depth of n^ϵ, for some $\epsilon > 0$. Although this is not stated explicitely, their proof actually shows that mNC^i is properly contained in $mSAC^i$, for every $i \geq 1$. In this note, we extend their lower bound to monotone semi-unbounded fan-in circuits. In particular, it follows from our result that the classes $mSAC^i$ and $co\text{-}mSAC^i$ are incomparable for every $i \geq 1$, and thus we get proper inclusions between the classes in the following diagram:

$$\begin{tikzcd}
& mSAC^i \arrow[dr, dash] & \\
mNC^i \arrow[ur, dash] \arrow[dr, dash] & & mAC^i \\
& co\text{-}mSAC^i \arrow[ur, dash] &
\end{tikzcd}$$

Our main result is the following theorem.

Theorem 1.1. *There are $\epsilon, \delta > 0$ such that for every function $d(n) \leq O(n^\epsilon)$, there is a monotone boolean function f computable by $mSAC$-circuits of depth $O(d(n))$ and size $n^{O(1)}$, such that $co\text{-}mSAC$-circuits of $\wedge$-fan-in $O(2^{n^\delta})$ computing f require depth $\Omega(d(n)\log n)$.*

By considering the functions $g(x_1, \dots, x_n) = \overline{f(\bar{x}_1, \dots, \bar{x}_n)}$ dual to the functions f in the theorem, we can easily get a separation of the depth complexity of $co\text{-}mSAC$ from that of $mSAC$ circuits in the opposite direction.

Corollary 1.2. *For ϵ, δ the same as in Theorem 1.1, and every function $d(n) \leq O(n^\epsilon)$, there is a monotone boolean function g computable by $co\text{-}mSAC$-circuits of depth $O(d(n))$ and size $n^{O(1)}$, such that $mSAC$-circuits of $\vee$-fan-in $O(2^{n^\delta})$ computing g require depth $\Omega(d(n)\log n)$.*

An obvious problem left open is to separate mAC^i from mNC^{i+1}. The notion of asymmetric communication complexity introduced below probably provides the right framework to attack this problem, but it would require a non-trivial extension of the lower bound method of Raz and McKenzie [5] and the present note.

2. Asymmetric communication complexity

The main tool for proving depth lower bounds for monotone circuits is the correspondence between circuit depth and communication complexity of search problems, first used by Karchmer and Wigderson [3]. An excellent detailed exposition of this correspondence can be found in the book by Kushilevitz and Nisan [4].

Let f be a monotone boolean function. If x, y are such that $f(x) = 1$ and $f(y) = 0$, then there must be an index i such that $x_i = 1$ and $y_i = 0$. This fact can be formulated as a search problem, the Karchmer–Wigderson game, named after the paper [3] where it was first used.

Definition 2.1. For a monotone n-ary boolean function f, the Karchmer–Wigderson game KW_f is the search problem defined as follows:

- $X = f^{-1}[1]$ and $Y = f^{-1}[0]$.
- $KW_f \subseteq X \times Y \times [n]$ is defined by

$$(x, y, i) \in KW_f \quad \text{iff} \quad x_i = 1 \wedge y_i = 0 \ .$$

The importance of the Karchmer–Wigderson game stems from the fact that its communication complexity is exactly the minimal depth of a monotone circuit computing f [3]. This fact can be generalized to circuits with gates of unbounded fan-in by allowing the transmission of several bits at unit cost.

An (α, β)-protocol is a generalized communication protocol, where Alice may send up to α bits, and Bob may send up to β bits in one step. Formally we define:

Definition 2.2. An (α, β)-protocol P over $X \times Y$ with range Z is a tree, where each internal node ν is either labeled by a function $a_\nu : X \to \{0,1\}^{d_\nu}$ with $1 \leq d_\nu \leq \alpha$, or by a function $b_\nu : Y \to \{0,1\}^{d_\nu}$ with $1 \leq d_\nu \leq \beta$. The node ν has 2^{d_ν} sons, and the edges going from ν to these sons are labeled by the elements of $\{0,1\}^{d_\nu}$. Each leaf is labeled by an element $z \in Z$.

The value $P(x, y)$ of P on input $(x, y) \in X \times Y$ is the label on the leaf reached by the walk that starts at the root and

- at a node ν labeled by a_ν, follows the edge labeled $a_\nu(x)$;
- at a node ν labeled by b_ν, follows the edge labeled $b_\nu(y)$.

The cost of the protocol is the height of the tree.

A protocol P solves a search problem $R \subseteq X \times Y \times Z$, if for every input $(x, y) \in X \times Y$, we have $(x, y, P(x, y)) \in R$. The *asymmetric communication complexity* $cc_{(\alpha,\beta)}(R)$ is the minimal cost of any (α, β)-protocol that solves R.

We can now state the correspondence between the depth of semi-unbounded fan-in circuits and asymmetric communication complexity.

Lemma 2.3. *Let C be a monotone circuit of depth d, with $\vee$-fan-in r and $\wedge$-fan-in s computing f. Then there is a $(\lceil \log r \rceil, \lceil \log s \rceil)$-protocol solving KW_f with cost at most d.*

Proof. Let g be a gate in C with $g(x) = 1$ and $g(y) = 0$ for some inputs x and y. If g is an $\vee$, then $g'(y) = 0$ holds for every gate g' entering g. Also, $g'(x) = 1$ holds for at least one of those gates, and Alice can tell Bob for which by communicating at most $\lceil \log r \rceil$ bits. Symmetrically, if g is an $\wedge$, Bob can communicate up to $\lceil \log s \rceil$ bits to tell Alice for which gate g' entering g it holds that $g'(x) = 1$ and $g'(y) = 0$.

This way, given inputs x, y with $C(x) = 1$ and $C(y) = 0$, they can find a path from the output to an input, such that for every gate g on the path $g(x) = 1$ and $g(y) = 0$ holds, so in particular this holds for the input x_i that was reached. The cost of this protocol is the depth d of the circuit. □

The opposite direction also holds; since we do not make use of this direction, we omit the proof, which is an easy generalization of the fan-in 2 case.

Lemma 2.4. *If there is an (α, β)-protocol with cost c solving KW_f, then f can be computed by a monotone circuit of $\vee$-fan-in 2^α and $\wedge$-fan-in 2^β of depth c.*

3. DART games and structured protocols

The main result in [5] is derived from a general theorem about the communication complexity of a certain class of search problems, the so-called DART games. We generalize this to the case of asymmetric communication complexity, where Bob is allowed to communicate several bits in one round.

The class of search problems DART(m, k), for $m, k \in \mathbb{N}$, is defined as follows. Any DNF tautology $D = C_1 \vee \ldots \vee C_t$ in variables $z_1, \ldots, z_k$ gives rise to a search problem, where the input is an assignment α to the variables $\vec{z}$, and the question is to find one of the terms C_i of D that is satisfied by α.

From this DNF search problem, we define a communication problem as follows: the set X of inputs to Alice is $[m]^k$, the set of k-tuples $x = (x_1, \ldots, x_k)$ of elements of $[m]$. The set Y of inputs to Bob is $(2^{[m]})^k$, *i.e.*, each input $y \in Y$ is a k-tuple $(y_1, \ldots, y_k)$ of colorings $y_i : [m] \to \{0, 1\}$. From two inputs $x \in X$ and $y \in Y$, an assignment α is defined by $\alpha(z_i) := y_i(x_i)$. This assignment is taken as input to the DNF search problem, *i.e.*, given inputs x and y, Alice and Bob have to find a term in D that is satisfied by the so defined assignment α.

A *structured protocol* is a communication protocol for solving a DART(m, k) search problem, where in each round, Alice reveals the value x_i for some i, and Bob replies with $y_i(x_i)$. The structured communication complexity $scc(R)$ of $R \in$ DART(m, k) is the minimal number of rounds in a structured protocol solving R.

Theorem 3.1. *For every $R \in$ DART(m, k), where $m \geq k^{14}$, and every $\beta \leq \frac{m^{\frac{1}{14}}}{\log m}$,*

$$cc_{(1,\beta)}(R) \geq scc(R) \cdot \Omega(\log m) .$$

The proof of the theorem is similar to the proof of the main theorem in [5], therefore we do not give all the details, but only those parts that require modification. We prove a more general statement about the complexity of DART games on restricted domains.

To a such a restricted DART game, one of two operations is applied to the following effect. The first operation makes the domain smaller to reduce the asymmetric communication complexity, the other modifies the DART game itself to decrease its structured complexity, while the asymmetric communication complexity remains equal. Assuming that the asymmetric communication complexity is too small, these operations can be performed alternatingly to obtain a contradiction. Which of the two operations is to be applied is determined by certain combinatorial properties of the domain, which are defined next.

Let $A \subseteq [m]^k$ and $1 \leq j \leq k$. For $x \in [m]^{k-1}$, let

$$\deg_j(x, A) := \Big|\{\, \xi \in [m]\,;\, (x_1, \ldots, x_{j-1}, \xi, x_j, \ldots, x_{k-1}) \in A \,\}\Big| \cdot$$

Then we define

$$\begin{aligned} A[j] &:= \big\{\, x \in [m]^{k-1}\,;\, \deg_j(x, A) > 0 \,\big\} \\ \operatorname{avdeg}_j(A) &:= \frac{|A|}{|A[j]|} \\ \operatorname{Thickness}(A) &:= \min_{1\leq j\leq k}\ \min_{x\in A[j]} \deg_j(x, A)\ . \end{aligned}$$

The following lemmas about these notions were proved in [5]:

Lemma 3.2. *For every $A' \subseteq A$ and $1 \leq j \leq k$,*

$$\operatorname{avdeg}_j(A') \geq \frac{|A'|}{|A|} \operatorname{avdeg}_j(A) \tag{1}$$

$$\operatorname{Thickness}(A[j]) \geq \operatorname{Thickness}(A). \tag{2}$$

Lemma 3.3. *If there is $0 < \delta < 1$ such that for every $1 \leq j \leq k$, $\operatorname{avdeg}_j(A) \geq \delta m$, then for every $\alpha > 0$ there is $A' \subseteq A$ with $|A'| \geq (1-\alpha)|A|$ and*

$$\operatorname{Thickness}(A') \geq \frac{\alpha\delta m}{k} \cdot$$

In particular, setting $\alpha = \frac{1}{2}$ and $\delta = 4m^{-\frac{1}{14}}$, we get:

Corollary 3.4. *If $m \geq k^{14}$ and for every $1 \leq j \leq k$, $\operatorname{avdeg}_j(A) \geq 4m^{\frac{13}{14}}$, then there is $A' \subseteq A$ with $|A'| \geq \frac{1}{2}|A|$ and $\operatorname{Thickness}(A) \geq m^{\frac{11}{14}}$.*

For $R \in \mathrm{DART}(m, k)$ and $A \subseteq X$, $B \subseteq Y$, let $cc_{(1,\beta)}(R, A, B)$ denote the minimal cost of a $(1, \beta)$-protocol solving R restricted to the domain $A \times B$.

Definition 3.5. Let $m \in \mathbb{N}$ be given. A triple (R, A, B) is called an (ϵ, δ, ℓ)-game, if the following hold.

- $R \in \mathrm{DART}(m, k)$ for some $k \leq m^{\frac{1}{14}}$, with $scc(R) \geq \ell$.
- $A \subseteq X = [m]^k$ with $|A| \geq 2^{-\epsilon}|X|$ and $\operatorname{Thickness}(A) \geq m^{\frac{11}{14}}$.
- $B \subseteq Y = (2^{[m]})^k$ with $|B| \geq 2^{-\delta}|Y|$.

Lemma 3.6. *Let (R, A, B) be an (ϵ, δ, ℓ)-game, and $\delta < 8m^{\frac{13}{14}}$. If for all $1 \leq j \leq k$, $\operatorname{avdeg}_j(A) \geq 8m^{\frac{13}{14}}$, then there is (R', A', B'), which is either an $(\epsilon+2, \delta, \ell)$-game or an $(\epsilon, \delta + \beta, \ell)$-game, with*

$$cc_{(1,\beta)}(R', A', B') \leq cc_{(1,\beta)}(R, A, B) - 1 .$$

Proof. As in [5], we first prove that $cc_{(1,\beta)}(R, A, B) > 0$. Assume otherwise, then there is a term in the DNF tautology defining R which is satisfied for every input $(x, y) \in A \times B$. Therefore $y_j(x_j)$ is constant for at least one $j \leq k$. If γ denotes the number of possible values of x_j in elements of A, then this implies that $|B| \leq 2^{mk-\gamma}$. On the other hand, $|B| \geq 2^{mk-\delta}$, hence it follows that $\delta \geq \gamma$, but from $\operatorname{avdeg}_j(A) \geq 8m^{\frac{13}{14}}$ we have $\gamma \geq 8m^{\frac{13}{14}}$, so this contradicts the assumption.

Now let an optimal $(1, \beta)$-protocol P solving R over $A \times B$ be given. The case where Alice sends the first bit can be treated as in [5]: we partition $A = A_0 \cup A_1$ according to the value of this bit, then R restricted to $A_i \times B$ for $i = 0, 1$ is solved by the sub-protocol of P following this transmission.

W.l.o.g. we assume $|A_0| \geq \frac{1}{2}|A|$, hence by Lemma 3.2, $\operatorname{avdeg}_j(A_0) \geq 4m^{\frac{13}{14}}$ for every j, and therefore Corollary 3.4 yields a subset $A' \subseteq A_0$ with $|A'| \geq \frac{1}{4}|A|$ with $\operatorname{Thickness}(A') \geq m^{\frac{11}{14}}$. Thus (R, A', B) is an $(\epsilon + 2, \delta, \ell)$-game.

Otherwise, Bob sends the first message of $d \leq \beta$ bits, and we can partition B according to this message as $B = B_0 \cup \ldots \cup B_{2^d-1}$. Now for some $i \leq 2^d - 1$, we have $|B_i| \geq 2^{-d}|B| \geq 2^{-\delta-d}|Y| \geq 2^{-\delta-\beta}|Y|$, and the sub-protocol of P following Bob's transmission solves R restricted to $A \times B_i$, thus (R, A, B_i) is an $(\epsilon, \delta + \beta, \ell)$-game. □

Lemma 3.7. *Let (R, A, B) be an (ϵ, δ, ℓ)-game with $\ell \geq 1$. If for some $1 \leq j \leq k$, $\operatorname{avdeg}_j(A) < 8m^{\frac{13}{14}}$, then there is an $(\epsilon + 3 - \frac{\log m}{14}, \delta + 1, \ell - 1)$-game (R', A', B') with*

$$cc_{(1,\beta)}(R', A', B') \leq cc_{(1,\beta)}(R, A, B) .$$

The proof of this lemma can be taken without changes from [5], only the numbers have to be adjusted to give a slightly better bound. We therefore omit the proof. Now we can finish the proof of Theorem 3.1.

Proof of Theorem 3.1. We show that for every (ϵ, δ, ℓ)-game (R, A, B), with $\delta \leq m^{\frac{1}{7}}$, and every $\beta \leq \frac{m^{\frac{1}{14}}}{\log m}$,

$$cc_{(1,\beta)}(R, A, B) \geq \ell \cdot \left[\frac{\log m}{28} - \frac{3}{2} - \frac{1}{\beta}\right] - \frac{\epsilon}{2} - \frac{\delta}{\beta} . \tag{3}$$

The theorem follows since R itself is an (ϵ, δ, ℓ) game (R, X, Y) with $\epsilon = \delta = 0$ and $\ell = scc(R)$.

We prove (3) by induction. Assume inductively that (3) holds for all $(\epsilon', \delta', \ell')$-games where either $\ell' < \ell$, or $\ell' = \ell$ and $\delta' > \delta$, or $\ell' = \ell$, $\delta' = \delta$ and $\epsilon' > \epsilon$.

Let (R,A,B) be an (ϵ,δ,ℓ)-game with

$$cc_{(1,\beta)}(R,A,B) < \ell \cdot \left[\frac{\log m}{28} - \frac{3}{2} - \frac{1}{\beta}\right] - \frac{\epsilon}{2} - \frac{\delta}{\beta}\,.$$

Now if $\mathrm{avdeg}_j(A) \geq 8m^{\frac{13}{14}}$ for every $1 \leq j \leq k$, then by Lemma 3.6 there is either an $(\epsilon+2,\delta,\ell)$-game (R',A',B') with

$$\begin{aligned} cc_{(1,\beta)}(R',A',B') &\leq cc_{(1,\beta)}(R,A,B) - 1 \\ &< \ell \cdot \left[\frac{\log m}{28} - \frac{3}{2} - \frac{1}{\beta}\right] - \frac{\epsilon+2}{2} - \frac{\delta}{\beta} \end{aligned}$$

or there is an $(\epsilon,\delta+\beta,\ell)$-game (R',A',B') with

$$\begin{aligned} cc_{(1,\beta)}(R',A',B') &\leq cc_{(1,\beta)}(R,A,B) - 1 \\ &< \ell \cdot \left[\frac{\log m}{28} - \frac{3}{2} - \frac{1}{\beta}\right] - \frac{\epsilon}{2} - \frac{\delta+\beta}{\beta} \end{aligned}$$

both contradicting the inductive assumption.

Otherwise there is $1 \leq j \leq k$ with $\mathrm{avdeg}_j(A) < 8m^{\frac{13}{14}}$, and by Lemma 3.7 there is an $(\epsilon + 3 - \frac{\log m}{14}, \delta+1, \ell-1)$-game (R',A',B') with

$$\begin{aligned} cc_{(1,\beta)}(R',A',B') \leq cc_{(1,\beta)}(R,A,B) &< \ell \cdot \left[\frac{\log m}{28} - \frac{3}{2} - \frac{1}{\beta}\right] - \frac{\epsilon}{2} - \frac{\delta}{\beta} \\ &= (\ell-1) \cdot \left[\frac{\log m}{28} - \frac{3}{2} - \frac{1}{\beta}\right] - \frac{\epsilon + 3 - \frac{\log m}{14}}{2} - \frac{\delta+1}{\beta} \end{aligned}$$

in contradiction to the inductive assumption.

The induction base is trivial for $\ell = 0$, and for $\delta = m^{\frac{1}{7}}$ we get

$$\begin{aligned} \ell \cdot \left[\frac{\log m}{28} - \frac{3}{2} - \frac{1}{\beta}\right] - \frac{\epsilon}{2} - \frac{\delta}{\beta} &\leq m^{\frac{1}{14}} \left[\frac{\log m - 42}{28} - \frac{\log m}{m^{\frac{1}{14}}}\right] - \frac{m^{\frac{1}{7}} \log m}{m^{\frac{1}{14}}} \\ &\leq \frac{m^{\frac{1}{14}}(\log m - 42)}{28} - \log m - m^{\frac{1}{14}} \log m \end{aligned}$$

which is ≤ 0 for large m, hence (3) holds trivially. Also, the right hand side of (3) is ≤ 0 for $\epsilon \geq \frac{1}{14} m^{\frac{1}{14}} \log m - 2\log m - 3$, hence the induction base also holds for large ϵ.[2] □

4. Application

For $d \in \mathbb{N}$, let $Pyr_d := \{\,(i,j)\,;\, 1 \leq j \leq i \leq d\,\}$ be the pyramid of depth d. In [5], the search problem $\textsc{PyrGen}(m,d) \in \mathrm{DART}(m, \binom{d+1}{2})$ is defined as follows:

[2] Note that this last case was omitted from the proof in [5].

The indices $1, \ldots, \binom{d+1}{2}$ are interpreted as elements of Pyr_d, and we picture them as laid out in a pyramidal form with $(1,1)$ at the top and (d,j), $1 \leq j \leq d$ at the bottom. The goal is to find one of the following situations:

- $y_{1,1}(x_{1,1}) = 0$.
- $y_{i,j}(x_{i,j}) = 1$ and $y_{i+1,j}(x_{i+1,j}) = y_{i+1,j+1}(x_{i+1,j+1}) = 0$ for some $(i,j) \in Pyr_{d-1}$.
- $y_{d,j}(x_{d,j}) = 1$ for some $j \leq d$.

The following lower bound on the structured communication complexity of PyrGen(m,d) was proved in [5].

Lemma 4.1. *$scc($*PyrGen*$(m,d)) \geq d$.*

By Theorem 3.1, we thus obtain a lower bound on the asymmetric communication complexity of PyrGen(m,d).

Corollary 4.2. *For $m \geq d^{28}$ and $\beta \leq m^{\frac{1}{14}} / \log m$,*

$$cc_{(1,\beta)}(\text{PyrGen}(m,d)) \geq \Omega(d \log m) \ .$$

Next we define a property of monotone boolean functions of n^3 inputs $t_{a,b,c}$ for $a,b,c \in [n]$. The input $\vec{t}$ is viewed as the definition of a formal system T, where the formulas are the elements of $[n]$, the only axiom is 1 and each input bit $t_{a,b,c} = 1$ defines an inference rule $a, b \vdash c$.

We say that an input $\vec{t}$ *allows a depth d pyramidal derivation* if there is a derivation of n in T of a special form, where the formulas can be arranged in a pyramid of depth d such that each formula is inferred from the two formulas below it. Formally, $\vec{t}$ allows a depth d pyramidal derivation if and only if there is a mapping $\mu : Pyr_d \to [n]$ such that the following conditions hold:

- $1, 1 \vdash \mu(d,j)$ for every $1 \leq j \leq d$.
- $\mu(i+1,j), \mu(i+1,j+1) \vdash \mu(i,j)$ for every $(i,j) \in Pyr_{d-1}$.
- $\mu(1,1), \mu(1,1) \vdash n$.

We say that an input $\vec{t}$ is *separable* if there is a coloring $\chi : [n] \to \{0,1\}$ such that $\chi(1) = 0$, $\chi(n) = 1$ and all inference rules in T preserve the color 0, *i.e.*, if $\chi(a) = \chi(b) = 0$ and $a, b \vdash c$, then $\chi(c) = 0$.

Finally, a function f is called d-pyramidal, if $f(\vec{t}) = 1$ for all inputs t that allow a depth d pyramidal derivation, and $f(\vec{t}) = 0$ for all $\vec{t}$ that are separable.

Proposition 4.3. *There is a d-pyramidal function that can be computed by an mSAC circuit of polynomial size, $\vee$-fan-in n^2 and depth $3d+3$.*

Proof. The function f decides whether n has a tree-like derivation of depth d in the formal system T defined by the input $\vec{t}$. For each $i \in [d]$ and $c \in [n]$, we define a circuit $D(i,c)$ that decides whether c has a derivation of depth i. These circuits are defined inductively by

- $D(1,c) = 1$ if c can be derived immediately from the axiom 1, thus $D(1,c)$ is $(1, 1 \vdash c)$, *i.e.*, the variable $t_{1,1,c}$.

- for $i \geq 2$, $D(i,c) = 1$ if c can be inferred from some a and b that have derivations of depth $i-1$, *i.e.*, $D(i,c)$ is

$$\bigvee_{a,b \in [n]} (a, b \vdash c) \wedge D(i-1, a) \wedge D(i-1, b) \; .$$

Finally, the circuit computing $f(\vec{t})$ is $\bigvee_{c \in [n]}(c, c \vdash n) \wedge D(d, c)$. Obviously, the size, depth and fan-in of this circuit are as claimed, and the function f it computes is d-pyramidal. □

Lemma 4.4. *For every m, d, β and $n := m\binom{d+1}{2} + 2$, any monotone d-pyramidal function f of n^3 inputs satisfies*

$$cc_{(1,\beta)}(\text{PyrGen}(m,d)) \leq cc_{(1,\beta)}(KW_f) \; .$$

Proof. We reduce the search problem PyrGen(m,d) to the Karchmer–Wigderson game for the function f, in fact, this is exactly the reduction to KW_{Gen} used in [5].

From their inputs x and y to PyrGen(m,d), Alice and Bob compute inputs $\vec{t}$ and $\vec{u}$, respectively, to KW_f without any communication, such that from a solution of KW_f for these inputs one can immediately read off a solution of PyrGen(m,d).

We interpret the elements between 2 and $n-1$ as triples (i,j,k), where $(i,j) \in Pyr_d$ and $k \in [m]$. Alice computes from her input $x : Pyr_d \to [m]$ an input $\vec{t}$ that allows a depth d pyramidal derivation by setting the following, where $a_{i,j} := (i, j, x_{i,j})$.

$$\begin{aligned} &1, 1 \vdash a_{d,j} && \text{for } 1 \leq j \leq d \\ &a_{1,1}, a_{1,1} \vdash n && \\ &a_{i+1,j}, a_{i+1,j+1} \vdash a_{i,j} && \text{for } (i,j) \in Pyr_{d-1}. \end{aligned}$$

Since f is d-pyramidal, $f(\vec{t}) = 1$.

Similarly, Bob computes from his input $y : Pyr_d \to 2^{[m]}$ a coloring χ of $[n]$ by setting $\chi(1) = 0$, $\chi(n) = 1$ and $\chi((i,j,k)) = y_{i,j}(k)$. From this coloring, he computes a separable input $\vec{u}$ with $f(\vec{u}) = 0$ by setting $a, b \vdash c$ for all triples $a, b, c \in [n]$ except for those with $\chi(c) = 1$ and $\chi(a) = \chi(b) = 0$.

A solution of the Karchmer–Wigderson game for f is a triple (a,b,c) such that $a, b \vdash c$ in $\vec{t}$ and $a, b \not\vdash c$ in $\vec{u}$. This means that $\chi(a) = \chi(b) = 0$ and $\chi(c) = 1$, and by therefore one of the following cases holds:

- $a = b = 1$ and $c = a_{d,j}$ for some $j \leq d$, and hence $y_{d,j}(x_{d,j}) = 1$.
- $c = n$ and $a = b = a_{1,1}$, and therefore $y_{1,1}(x_{1,1}) = 0$.
- $a = a_{i+1,j}$, $b = a_{i+1,j+1}$ and $c = a_{i,j}$, in which case we have $y_{i,j}(x_{i,j}) = 1$, and $y_{i+1,j}(x_{i+1,j}) = y_{i+1,j+1}(x_{i+1,j+1}) = 0$.

In either case, the players have found a solution to PyrGen(m,d) without any additional communication. □

With this information, we get a lower bound for *co-mSAC* circuits computing a d-pyramidal function.

Proposition 4.5. *Let $m \geq d^{28}$ and $n := \binom{d+1}{2}m + 2$. Any co-mSAC circuit of $\wedge$-fan-in $2^{m^{\frac{1}{14}}/\log m}$ computing a d-pyramidal function f of n^3 inputs requires depth $\Omega(d \log m)$.*

Proof. Let $\beta := \frac{m^{\frac{1}{14}}}{\log m}$. By Lemma 4.4 and Corollary 4.2, we get

$$cc_{(1,\beta)}(KW_f) \geq \Omega(d \log m)\,,$$

and hence by Lemma 2.3, a *co-mSAC* circuit of $\wedge$-fan-in 2^{β} computing f requires depth $\Omega(d \log m)$. □

Finally, this lower bound together with the upper bound of Proposition 4.3 proves Theorem 1.1.

References

[1] A. Borodin, S.A. Cook, P.W. Dymond, W.L. Ruzzo and M. Tompa, Two applications of inductive counting for complementation problems. *SIAM J. Comput.* **18** (1989) 559-578.

[2] M. Grigni and M. Sipser, Monotone complexity, in *Boolean Function Complexity*, edited by M.S. Paterson. Cambridge University Press (1992) 57-75.

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

[4] E. Kushilevitz and N. Nisan, *Communication Complexity.* Cambridge University Press (1997).

[5] R. Raz and P. McKenzie, Separation of the monotone *NC* hierarchy. *Combinatorica* **19** (1999) 403-435.

[6] H. Venkateswaran, Properties that characterize LOGCFL. *J. Comput. System Sci.* **43** (1991) 380-404.

Communicated by I. Wegener.
Received January, 2001. Accepted August 8, 2001.