Electronic Colloquium on Computational Complexity - Reports Series 1996 - available via:
ECCC
TR96-026
FTP: ftp.eccc.uni-trier.de:/pub/eccc/
WWW: http://www.eccc.uni-trier.de/eccc/
Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

Finite Limits and Monotone Computations

(Preliminary Version)

Stasys Jukna[†‡]

20 March 1996

We prove a general combinatorial lower bound on the size of monotone circuits. The argument is different from Razborov's method of approximation, and is based on Sipser's notion of 'finite limit' and Haken's 'counting bottlenecks' idea. We then apply this criterion to the CLIQUE function on n variables and obtain an $\exp(\Omega(n^{1/4}))$ lower bound for it, improving the best previous lower bound $\exp(\Omega((n^{1/6}/(\log n)^{1/3}))$ for this function obtained by Alon and Boppana using the method of approximations. The bound holds for circuits with *unbounded* fan-in AND, OR gates and *any* monotone Boolean functions of fan-in at most $n^{1/4}$ at the bottom. This supplements previous result due to Yao that the clique function has no polynomial size monotone circuit with fan-in n^{ϵ} monotone gates.

1. Introduction

A natural idea to prove a lower bound on the size of a circuit is to introduce a notion of 'progress' which any one gate in a circuit can do towards the final goal – computing correctly a given Boolean function f. The Method of Approximations due to Razborov ([9, 10]) provides a general scheme on how such a progress could look of: replace each gate by a special gate and take the error of this approximation as a progress (made by an original gate against the new one). This idea was used to prove non-trivial lower bounds for monotone circuits [9, 1], bounded depth circuits over $\{\wedge, \oplus\}$ [11], switching–and–rectifier networks [12], span and $\oplus$-branching programs [7], and monotone circuits over the reals [8]. Another approach to proving lower bounds for monotone circuits was recently described by Haken in [3]. The method employs the 'counting bottlenecks' idea from [2] and was used in [3] to prove a $2^{\Omega(n^{1/8})}$ lower bound on the size of a monotone circuit computing some special Boolean function ('broken mosquito screens' function), a version of the CLIQUE function.

In this paper we develop the approach of [3] in two ways: we prove a general (and easy to apply) combinatorial lower bound for *unbounded* fan-in monotone circuits, and use it

[†] Universität Trier, Fachbereich Informatik, D-54286 Trier, Germany. On leave from Institute of Mathematics, Vilnius, Lithuania. E-mail: jukna@ti.uni-trier.de. URL: http://www.informatik.uni-trier.de/~jukna/

[‡] Supported by a DFG grant Me 1077/10-1.

to prove a $2^{\Omega(n^{1/4})}$ lower bound for the CLIQUE function, improving the best previously known lower bound [1], which was exponential in $\exp(\Omega(n^{1/6}/(\log n)^{1/3})$.

Our main tool is the concept of 'finite limit' due to Sipser [13, 14]. A vector is a *k-limit* for a set of vectors if on every subset of k coordinates, this vector coincides with at least one vector from the set. If $f(x) = 0$ and x is a k-limit for the set $f^{-1}(1)$ then x is a 'hard' instance for a circuit computing f since the value $f(x)$ cannot be determined when looking at only k bits of x. It is therefore natural to define the progress made at a particular gate as the set of all vectors which are hard for this gate and which were not hard for previous gates. The key of the whole argument is one simple 'limit lemma' (Lemma 2.2) stating that no gate can make too large progress. If the function f is such that $f^{-1}(0)$ has many k-limits for $f^{-1}(1)$, then the progress made by the whole circuit must be large, and hence, there must be many gates.

In Section 2 we use this approximation scheme to derive a general combinatorial lower bound for circuits with unbounded fan-in AND, OR gates and arbitrary monotone Boolean functions of bounded fan-in as input–gates (Theorem 2.1). The combinatorial part of this argument is simple, essentially trivial.

In Section 3 we apply this criterion to $\mathrm{CLIQUE}_{m,k}$ function. This is a monotone Boolean function on $n = \binom{m}{k}$ variables, which, given a graph G on m vertices, computes 1 iff G contains a k-clique, i.e. a complete subgraph on k vertices. The best previously known lower bound for this function, proved by Alon & Boppana [1] using Method of Approximations, was $2^{\Omega(k^{1/2})}$ for any $k \le (m/8\log m)^{2/3}$. For maximal possible k this bound is exponential in $\exp(\Omega(n^{1/6}/(\log n)^{1/3})$. We prove a lower bound $2^{\Omega(k)}$ for any $k \le m^{1/2}$ (Theorem 3.1). This almost matches the trivial upper bound $2^{O(k\log(n/k))}$, and for $k \asymp m^{1/2}$, is exponential in $\Omega(n^{1/4})$. Moreover, this bound holds for quite general model of monotone circuits: we allow unbounded fan-in AND, OR gates and arbitrary monotone functions of fan-in $n^{1/4}$ at the bottom. This supplements previous result due to Yao [15] that the clique function has no polynomial size monotone circuit with fan-in n^{ϵ} monotone gates.

Finite limits have already been shown to work for other models of computation: AC^0-circuits [4], syntactic read-k-times branching programs [5] and depth-three threshold circuits [6]. The main advantage of using limits in all these applications is the simplicity and transparency of the whole lower bounds argument. The main aim of this paper is to show that limits can do the same job for monotone circuits.

2. The General Lower Bound

Let N be a finite set, $|N| = n$. Elements of N are called *bits*. An *input* is a mapping $x : N \to \{0,1\}$. A *Boolean function* is a mapping $f : \{0,1\}^N \to \{0,1\}$. An *$\ell$-circuit* is a usual Boolean circuit of unbounded fan-in AND and OR gates; the input-gates can be

arbitrary Boolean functions depending on at most ℓ variables. A circuit is *monotone* if all these input–gates are monotone functions.

A *witness* of input x against a set of inputs Y is a set of bits S such that x differs from every input $y \in Y$ on at least one bit from S. In the criterion we are going to state, only two parameters of witnesses will be important: their 'length' and their 'legality'. To define the length, take a mapping π (called a *projection*) which assigns to each set of bits $S \subseteq N$ a set $\pi(S)$ (of arbitrary nature)[1] and define the *length* of S as the number $|\pi(S)|$ of elements in $\pi(S)$. Throughout this section we fix a pair of projections (π_0, π_1) with the following *cross–intersection* property: if $S \cap T \neq \emptyset$ then $\pi_0(S) \cap \pi_1(T) \neq \emptyset$.

Definition. If S is a witness of an input x (against some set) then we say that this witness is *legal* if $x(i) = f(x)$ for all $i \in S$. It's *length* is $\left|\pi_{f(x)}(S)\right|$. We say that x is a *k-limit* for Y if x has *no* legal witness against Y shorter than k. Let $\lim_k(Y)$ denote the set of all k-limits for a set Y. For a set $X \subseteq f^{-1}(\epsilon)$, its *$k$-th degree* $\#_k(X)$ is the maximum of[2]

$$\left| \bigcup_{S:\pi_\epsilon(S) \supseteq H} X[S] \right|$$

over all k-element sets H, where $X[S]$ is the set of all inputs $x \in X$ with $x(i) = f(x)$ for all $i \in S$.

Our main result is the following general combinatorial lower bound for monotone ℓ-circuits.

Theorem 2.1. *Let $1 \leq \ell \leq s, r \leq n$ be integers, f be a monotone function on n variables, and let $X^0 \subseteq f^{-1}(0)$ and $X^1 \subseteq f^{-1}(1)$. Then every monotone ℓ-circuit computing f, has size at least*

$$\min\left\{ \frac{|X^0 \cap \lim_r(X^1)|}{(r-1)^s \cdot \#_s(X^0)},\ \frac{|X^1 \cap \lim_s(X^0)|}{(s-1)^r \cdot \#_r(X^1)} \right\} \tag{1}$$

The proof is based on the following simple lemmas concerning transversals and limits.

A *cover* of (or a *transversal* for) a family of sets $\mathcal{F}$ is a set T which intersects every member of $\mathcal{F}$. The *cover number* $\tau(\mathcal{F})$ of a family $\mathcal{F}$ is the minimum number of elements in a transversal for it.

Lemma 2.1. *Let $\mathcal{F}$ be a family of sets, each of cardinality at most s. Then for every*

[1] For example, in case of graphs, bits in N correspond to edges, and one can take $\pi(S)$ be the set of vertices covered by the edges in S.

[2] Notice that $X[T] \subseteq X[S]$ if $T \supseteq S$, so that it is enough to consider only minimal sets S.

$r \leq \tau(\mathcal{F})$ there is a family $\mathcal{H}_r$ of at most s^r r-element sets such that every transversal of $\mathcal{F}$ contains at least one member of $\mathcal{H}_r$.

Proof. Let $\mathcal{F} = \{S_1, \ldots, S_t\}$ and fix this order of sets. We will construct the desired family $\mathcal{H}_r$ by induction on r. For $r = 1$ we can take as $\mathcal{H}_1$ the family of all one element sets $\{x\}$ with $x \in S_1$. Assume now that $\mathcal{H}_{r-1}$ is already constructed. For each set H in this family choose the first index i for which $H \cap S_i = \emptyset$ (such an i exists since $r - 1 < \tau(\mathcal{F})$), and put in $\mathcal{H}_r$ all the r-element sets $H \cup \{x\}$ with $x \in S_i$. Then $|\mathcal{H}_r| \leq s \cdot |\mathcal{H}_{r-1}| \leq s^r$, and we are done. ■

Lemma 2.2. (Limit Lemma) *Let $1 \leq s, r \leq n$ be integers, $\epsilon \in \{0,1\}$, and let $A \subseteq X^\epsilon$ and $\emptyset \neq B \subseteq X^{\epsilon \oplus 1}$ be such that: (i) every input from A is an r-limit for B, and (ii) no input from B is an s-limit for A. Then $|A| \leq (s-1)^r \cdot \#_r(A)$.*

Proof. Let $B = \{y_1, \ldots, y_t\}$ and let x be an arbitrary input from A. By (ii) there exist subsets $S_i \subseteq N$, $i = 1, \ldots, t$ such that $|\pi_{\epsilon \oplus 1}(S_i)| \leq s - 1$ and all the inputs from A, including x, differ from y_i on at least one bit $j_i \in S_i$ for which $y_i(j_i) = \epsilon \oplus 1$. Thus, for every $i = 1, \ldots, t$ we can choose one bit $j_i \in S_i$ such that $x(j_i) = \epsilon \neq y_i(j)$. Let $T_x = \{j_i : i = 1, \ldots, t\}$ be the set of all such bits, corresponding to x, and let $\mathcal{T} = \{T_x : x \in A\}$. Since T_x is a legal witness of x against B, we have by (i) that $|\pi_\epsilon(T_x)| \geq r$. On the other hand, every $T \in \mathcal{T}$ is a transversal for the family $\{S_1, \ldots, S_t\}$, and, since the projections π_0 and π_1 have the cross–intersection property, the sets $\pi_\epsilon(T)$ are also transversals for the family $\{\pi_{\epsilon \oplus 1}(S_1), \ldots, \pi_{\epsilon \oplus 1}(S_t)\}$. By Lemma 2.1 there is a family $\mathcal{H}$ of $(s-1)^r$ r-element sets such that every set $\pi_\epsilon(T)$ with $T \in \mathcal{T}$, contains at least one set $H \in \mathcal{H}$. Thus, $A = \bigcup_{T \in \mathcal{T}} A[T] \subseteq \bigcup_{H \in \mathcal{H}} \bigcup_{\pi_\epsilon(T) \supseteq H} A[T]$, and hence, $|A| \leq \sum_{H \in \mathcal{H}} \#_{|H|}(A) \leq (s-1)^r \cdot \#_r(A)$, as desired. ■

Proof of Theorem 2.1 Set $k_0 := s$ and $k_1 := r$. Let C be an ℓ–circuit computing f. That is, C is a straight–line program $C = (g_1, \ldots, g_t)$; every gate g_i has the form $g_i = \phi(h_1, \ldots, h_{m_i})$ where ϕ is either AND or OR, and each h_j is either one of the previous gates $g_1, \ldots, g_{i-1}$ or an arbitrary monotone Boolean function on at most ℓ variables. To unify our notation, we say that g_i is a 1-*gate* if $\phi = \wedge$, and a 0-*gate* if $\phi = \vee$. For a gate g and $\epsilon \in \{0,1\}$, let $X_g^\epsilon = \{x \in X^\epsilon : g(x) = \epsilon\}$ denote the part of inputs separated correctly at g.

Say that an input x is *hard* for a gate g if g is the first gate (in C) such that $x \in X_g^\epsilon$ for some $\epsilon \in \{0,1\}$ (i.e. g classifies x correctly) and x is a k_ϵ-limit for $X_g^{\epsilon \oplus 1}$. Let Y_g denote the set of all inputs which are hard for g, and let Y^ϵ be the union of sets Y_g over all ϵ-gates g of C.

If g is an input–gate then $Y_g = \emptyset$. Indeed, in this case g is monotone and depends on at most ℓ variables. Hence, for every pair of inputs $x \in X_g^0$ and $y \in X_g^1$ there must be at least one of these (fixed) ℓ coordinates i such that $x(i) = 0$ and $y(i) = 1$. Thus, no input from X_g^ϵ can be a ℓ-limit for the other part $X^{\epsilon\oplus 1}$, and hence, no input can be hard for g.

Let now $g = \phi(h_1, \ldots, h_m)$ be an ϵ-gate. Observe that then $Y_g \subseteq X_g^\epsilon$, i.e. that no input from $X_g^{\epsilon\oplus 1}$ can be hard for g. Indeed, in this case $X_g^\epsilon = \bigcap_{i=1}^m X_{h_i}^\epsilon$ and $X_g^{\epsilon\oplus 1} = \bigcup_{i=1}^m X_{h_i}^{\epsilon\oplus 1}$. Hence, if for some j, $X_{h_{i_j}}^{\epsilon\oplus 1}$ would have an input, which is a limit for X_g^ϵ, then this input would be also a limit for $X_{h_{i_j}}^\epsilon$, meaning that this input already *was* hard for h_{i_j} or some previous gate. Thus, $Y_g \subseteq X_g^\epsilon$, and hence, no of the inputs from $X_g^{\epsilon\oplus 1}$ can be a $k_{\epsilon\oplus 1}$-limit for the set $Y_g \subseteq X_g^\epsilon$. (Note that $X_g^{\epsilon\oplus 1} \neq \emptyset$ since otherwise we could replace the gate g by the constant ϵ). On the other hand, every input from Y_g is a k_ϵ-limit for $X_g^{\epsilon\oplus 1}$, by the definition. Applying Lemma 2.2 with $A = Y_g$ and $B = X_g^{\epsilon\oplus 1}$ we obtain the following upper bound on the progress made by one gate:

$$|Y_g| \leq (k_{\epsilon\oplus 1} - 1)^{k_\epsilon} \cdot \#_{k_\epsilon}(X^\epsilon). \tag{2}$$

It remains to observe that the progress made by the whole circuit cannot be too small, namely, that for at least one $\epsilon \in \{0, 1\}$,

$$|Y^\epsilon| \geq \left| X^\epsilon \cap \lim_{k_\epsilon}(X^{\epsilon\oplus 1}) \right| \tag{3}$$

Indeed, the last gate g of C being an ϵ-gate means that every input from $X_g^\epsilon = X^\epsilon$, which does not belong to Y^ϵ, can be hard neither for g nor for any previous gate, and in particular, is not a k_ϵ-limit for the set $X_g^{\epsilon\oplus 1} = X^{\epsilon\oplus 1}$. Thus, $X^\epsilon \setminus Y^\epsilon \subseteq X^\epsilon \setminus \lim_{k_\epsilon}(X^{\epsilon\oplus 1})$, which gives the desired lower bound (3).

Since $size(C) \geq \delta_0 \cdot |Y^0| + \delta_1 \cdot |Y^1|$ where $\delta_\epsilon = 1/\max_g |Y_g|$ over all ϵ-gates g, estimates (2) and (3) imply the desired lower bound (1), completing the proof of Theorem 2.1. ■

3. Lower Bound for Clique Function

Let N be the family of all $n = \binom{m}{2}$ 2-element subsets (called *edges*) of some set V of m vertices. This way every input $x : N \to \{0, 1\}$ can be identified with the graph $G_x = (V, E)$ where $(u, v) \in E$ iff $x(u, v) = 1$. The *clique function* $\mathrm{CLIQUE}_{n,k}$ is a monotone Boolean function on n variables, which given an input x computes 1 iff the graph G_x contains a k-clique, i.e. a complete subgraph on k vertices.

Using the method of approximations, Razborov in [9] proved the super-polynomial lower bound $n^{\Omega(\log n)}$ for this function. Subsequently, Alon and Boppana [1], by strengthening the combinatorial part of Razborov's proof, were able to extend this bound until $\exp\left(\Omega(n^{1/6}/(\log n)^{1/3}\right)$. More exactly, they proved a lower bound $2^{\Omega(k^{1/2})}$ for any $k \leq (m/8\log m)^{2/3}$. These bounds were proved for usual model of fan-in 2 AND, OR

gates. Yao [15] considered monotone circuits with arbitrary monotone Boolean functions of fan-in $\leq n^{\epsilon}$ as gates, and proved that any such circuits computing $\mathrm{CLIQUE}_{n,k}$ with $k = \log\log m$, requires super-polynomial size.

Theorem 2.1 leads to a $2^{\Omega(k)}$ lower bound for any $k \leq m^{1/2}$, improving the bound of [1] until $\exp\left(\Omega(n^{1/4})\right)$. Moreover, our bound holds for circuits with *unbounded* fan-in AND, OR gates and arbitrary $\frac{k}{2}$-ary monotone Boolean functions at the bottom.

Theorem 3.1. *Let $\ell \leq \min\left\{\frac{m}{2k}, \frac{k}{2}\right\}$, and let C be a circuit with unbounded fan-in AND, OR gates and arbitrary monotone Boolean functions of fan-in ℓ at the bottom. If C computes $\mathrm{CLIQUE}_{n,k}$ then C has size $2^{\Omega(\min\{k, m/k\})}$. In particular, if $k \asymp m^{1/2}$ then the size of C is $2^{\Omega(n^{1/4})}$.*

Proof. Let X^1 be the set of all (inputs corresponding to) q-cliques, so that $|X^1| = \binom{m}{k}$. Let X^0 be the set of all (inputs corresponding to) graphs formed by assigning each vertex one of $k-1$ colors and then putting edges between those pairs of vertices with different colors. Additionally, we require that all the colors be used, so that the number of such colorings is $(k-1)^m - (k-2)^m \geq (k-2)^m$. (Two colorings can lead to the same graph but we consider them as different for counting purposes). Define the projections by: $\pi_0(S) = \pi_1(S) =$ the set of all vertices incident with at least one edge from S. The cross–intersection condition is then trivially satisfied. We are going to apply Theorem 2.1 with $s := \lceil m/2k \rceil$ and $r := \lceil k/2 \rceil$.

Observe that every k-clique is a $(k-1)$–limit for the set of all $(k-1)$–partite graphs because every $(k-1)$–clique lies entirely in at least one of such graphs. Thus, $X^1 \cap \lim_s(X^0) = X^1$. On the other hand, adding one new edge $e \notin E$ to any complete $(k-1)$–partite graph $G = (V, E)$ we obtain a graph with a k-clique. Put otherwise, no proper subset of $N \setminus E$ can witness the difference of G from graphs with k-cliques, and hence, G has no legal witness against k-cliques of length shorter r. Thus, again $|X^0 \cap \lim_r(X^1)| = |X^0| \geq (k-2)^m$. Next, observe that $\#_r(X^1)$ is the number of k-cliques containing some fixed set of r vertices, and hence, is at most $\binom{m-r}{k-r}$. On the other hand, $\#_s(X^0)$ is the number of colorings with a pre-determined value on some fixed set of s vertices, and hence, is at most $(k-2)^{m-s}$.

Putting these estimates into (1), a simple calculation shows that the first term is at least $\left(\frac{k-2}{r-1}\right)^s = 2^{\Omega(m/k)}$ and the second is at least $\left(\frac{m}{(s-1)k}\right)^r = 2^{\Omega(k)}$, as desired. ■

References

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

[2] A. HAKEN, The intractability of resolution, *Theor. Comp. Sci.,* **39** (1985), 297–308.

[3] A. HAKEN, Counting Bottlenecks to Show Monotone P≠NP, In *Proc. of the 36th Ann. IEEE Symp. Found. Comput. Sci.*, 1995.

[4] J. HÅSTAD, S. JUKNA AND P. PUDLÁK, Top-down lower bounds for depth-three circuits, *Computational Complexity*, **5** (1995), 99–112.

[5] S. JUKNA, Finite limits and lower bounds for circuit size, Tech. Rep. Nr. 94-06, Informatik, University of Trier, 1994. ftp://ftp.informatik.uni-trier.de/pub/reports/94_06.ps

[6] S. JUKNA, Computing threshold functions by depth-3 threshold circuits with smaller thresholds of their gates, *Information Processing Letters*, **56** (1995), 147–150.

[7] M. KARCHMER AND A. WIGDERSON, On span programs, In *Proc. 8th Ann. Conf. Structure in Complexity Theory,* (1993), 102–111.

[8] P. PUDLÁK Lower bounds for resolution and cutting planes proofs and monotone computations (preliminary draft), Manuscript, 1995.

[9] A. A. RAZBOROV, Lower bounds on the monotone complexity of some Boolean functions, *Doklady Akademii Nauk SSSR,* 281:4 (1985), pp. 798-801. English translation in: *Soviet Mathematics Doklady,* 31, pp. 354-357

[10] A. A. RAZBOROV, On the method of approximations, In *Proc. of the 21th Ann. ACM Symp. Theor. Comput.,* (1989), 167–185.

[11] A. A. RAZBOROV, Lower bounds on the size of bounded depth networks over a complete basis with logical addition, *Matematicheskie Zmetki* 41:4 (1987), 598–607 (in Russian). English translation in *Mathematical Notes of the Academy of Sciences of the USSR* 41:4 (1987), 333–338.

[12] A. A. RAZBOROV, Lower bounds on the size of switching–and–rectifier networks for symmetric Boolean functions, *Matematicheskie Zmetki* 48:6 (1990), 79–91 (in Russian). English translation in *Mathematical Notes of the Academy of Sciences of the USSR.*

[13] M. SIPSER, A topological view of some problems in complexity theory. In *Colloquia Mathematica Societatis János Bolyai* **44** (1985), pp 387-391.

[14] M. SIPSER, *Personal communication*, (1991)

[15] A. C. YAO, Circuits and local computations, In *Proc. 21th Ann. ACM Symp. Theor. Comput.,* (1989), 186–196.