Finite Limits and Monotone Computations over the Reals*

Stasys Jukna†‡

June 4, 1996

Abstract

Our main result is a general and easy to apply combinatorial lower bounds criteria for: (a) circuits with *unbounded* fan-in AND and OR gates, and (b) circuits with arbitrary non-decreasing *real* functions of large fan-in as gates. The combinatorial part of our argument is very simple. It combines the "bottlenecks counting" idea of Haken with the notion of "finite limit" due to Sipser.

1 Introduction

In this paper we consider two models of monotone computations: (a) circuits with *unbounded* fan-in AND and OR gates, and (b) circuits with arbitrary non-decreasing *real* functions of large fan-in as gates. Our main result is a general combinatorial lower bound for such circuits (Theorems 3.1 and 3.2). Apparently, this is the first simple and easy to apply lower bounds criterion for monotone computations. When applied to concrete Boolean functions, this criterion directly yields exponential lower bounds for explicit functions in NP.

Our argument combines two ideas: a *bottlenecks counting* idea of Haken [8, 9] and an idea of *finite limits* due to Sipser [20, 21]. The bottlenecks counting idea was

*This paper extends the results of ECCC TR96-026.

†Supported by a DFG grant Me 1077/10-1.

‡Universität Trier, Fachbereich IV - 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/

first used by Haken in the lower bounds proof for resolution [8]. In [9] he applied this idea to monotone circuits and proved 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 [10] this lower bound was extended to constant fan-in monotone real circuits. As shown by Cook and Rosenbloom [7], such circuits are quite powerful in that they can compute any Boolean slice function in linear size, whereas most of such functions require (non-monotone) Boolean circuits of super-polynomial size.

The combinatorial part of our argument is different from that used in the famous *method of approximations* proposed by Razborov [15, 16, 17, 18, 19] (see also [5] or [22] for expositions). But general idea is essentially the same: we map a large set of input vectors to gates in the circuit so that not too many vectors are mapped to any one gate. The mapping manages to hit "bottlenecks" in the circuit by sending an input vector to the first gate in the circuit for which this input is "hard" and which nevertheless classifies this input correctly. To measure the "hardness" we use the concept of *finite limit* due to Sipser [20, 21]. A vector x is a k-limit for a set of vectors A if on every subset of k coordinates, x coincides with at least one vector from A. If $f(x) = 0$ and x is a k-limit for the set $f^{-1}(1)$ then x is a 'hard' instance for any circuit computing f since the value $f(x)$ cannot be determined when looking at only k bits of x. The key of the whole argument is one simple "limit lemma" (Lemma 5.2) saying that in monotone circuits no single gate can make too large progress in classifying such instances. If the function f is such that $f^{-1}(0)$ has many k-limits for $f^{-1}(1)$ (and vice versa) then the progress made by the whole circuit must be large, and hence, there must be many gates.

The paper is organized as follows. In Section 2 we describe the model of monotone circuits over the reals. In Section 3 we formulate the general lower bounds criterion for such circuits (Theorem 3.1) and its modification for unbounded fan-in AND/OR circuits (Theorem 3.2). In Section 4 we define limits and loosely describe the main idea. All necessary combinatorial properties of limits are stated and proved in Section 5. Both theorems are proved in Sections 6 and 7. In the last section we apply our general lower bound to explicit Boolean functions and derive exponential lower bounds for them. For the clique function the bound is exponential in $\Omega(n^{1/6-o(1)})$. For other natural function in NP ('drawing polynomials' function) the bound is exponential in $\Omega(n^{1/4})$. This last bound is almost optimal and was the largest lower bound proved in [1] using the method of approximations. We get these bounds in a unique manner: all we need is to compute several very simple combinatorial characteristics of a given Boolean function. Moreover, these bounds hold for more general and, due to the above mentioned result in [7], exponentially more powerful models:

- circuits with *arbitrary* nondecreasing real functions of large fan-in (up to $n^{1/4}$) as gates, and
- circuits with *unbounded* fan-in AND and OR gates, and arbitrary monotone Boolean functions of large fan-in (up to $n^{1/4}$) on the bottom.

In the Boolean case, this supplements previous result due to Yao [23] that one needs super-polynomial size to determine small clique in a graph even allowing gates capable to perform arbitrary monotone Boolean operation of fan-in at most n^{ϵ}.

The results in the present paper have also an application to cutting plane proofs [6] in the propositional calculus. Cutting plane proofs provide a complete refutation system for unsatisfiable sets of propositional clauses. They efficiently simulate resolution proofs, and in fact are known to provide exponentially shorter proofs on some examples (the pigeonhole clauses). Bonet *et al* [4] and Pudlák [14] reduced the problem to lower bounds for circuits with nondecreasing real functions of fan-in 2 as gates. Thus, our general lower bound for such circuits (Theorems 3.1), as well as lower bounds for explicit functions, are also lower bounds for cutting plane proofs.

2 The model

In this section we recall some (more or less standard) notions concerning Boolean functions and circuits. Let N be a set of n elements, called *bits*. Subsets of N are called *bit sets*. An *input* is a mapping $x : N \to \{0,1\}$. A *Boolean function* is a mapping $f : \{0,1\}^n \to \{0,1\}$. The value $f(x)$ of f on an input x is defined by $f(x) = f(x(1), \dots, x(n))$. A *Boolean variable* is a projection $v_i : \{0,1\}^n \to \{0,1\}$ onto a single coordinate, i.e. $v_i(x) = x(i)$; there are n such variables.

A *real circuit* (or straight–line program) *over the basis* Φ is a sequence $C = (g_1, \dots, g_t)$ of mappings (called *gates*) $g_i : \{0,1\}^n \to \mathbf{R}$ such that for every $i = 1, \dots, t$, gate g_i has the form $g_i = \phi(h_1, \dots, h_{m_i})$ where $\phi : \mathbf{R}^{m_i} \to \mathbf{R}$ is a function from the basis Φ, and each h_j is either a Boolean variable or one of the previous gates

$g_1, \dots, g_{i-1}$. If all the h_j are Boolean variables, then g_i is called the *bottom* gate. The number m_i is a *fan-in* of g_i. The number t is the *size* of C. The function computed by C is the function g_t computed at the last gate.

Remark. The arithmetic structure of real numbers $\mathbf{R}$ will not be used for the lower bounds, one can take any totally ordered set instead of $\mathbf{R}$.

Let, in what follows, f be arbitrary (but fixed) Boolean function. In order to define the monotonicity of circuits, we look at the behavior of their gates g on bipartite graphs $D_g \subseteq f^{-1}(0) \times f^{-1}(1)$ defined by: $(x, y) \in D_g$ iff $g(x) \neq g(y)$. Intuitively, the larger D_g is, the better g 'approximates' the function f. Given a subgraph $E_g \subseteq D_g$ and an input x, let $E_g(x) \subseteq f^{-1}(f(x) \oplus 1)$ denote the set of all neighbors of x in the graph E_g. We say that a graph E_g is *monotone* if, it is possible to order all the inputs $x_1, \dots, x_p$ in $f^{-1}(0)$ so that $E_g(x_1) \subseteq \ldots \subseteq E_g(x_p)$. [1]

One more characteristic of gates will be important for us, namely - their 'degree', which also depends on the properties of associated graphs E_g. If $g = \phi(h_1, \dots, h_m)$ is a gate then clearly $E_g \subseteq E_{h_1} \cup \ldots \cup E_{h_m}$, because $(x, y) \in E$ implies that $g(x) \neq g(y)$, and hence, $h_i(x) \neq h_i(y)$ for at least one i. That is, every edge (x, y) of the resulting graph E_g must appear in at least one of the input graphs $E_{h_1}, \dots, E_{h_m}$. Given a vertex x of the graph E_g we are interested in the minimal number of these input graphs covering all the edges incident to x. Namely, define the *ϵ-degree* of a gate g as the maximum of $\deg(x, g) = \min\{|I| : I \subseteq [m] \text{ and } E_g(x) \subseteq \bigcup_{i \in I} E_{h_i}(x)\}$ over all inputs $x \in f^{-1}(\epsilon)$. The *degree* of a gate is the maximum of its 0- and 1-degrees.

Given a real circuit $C = (g_1, \dots, g_t)$, which computes a Boolean function f, we say that C is a *monotone circuit of degree d* if it is possible to associate with each its gate g_i a monotone graph $E_{g_i} \subseteq f^{-1}(0) \times f^{-1}(1)$ so that $E_{g_t} = f^{-1}(0) \times f^{-1}(1)$ and the degree of each gate is at most d.

Remark. Since the domain $\mathbf{R}$ of gates is totally ordered set, it is always possible to associate with *any* gate g a graph, which is monotone. For example, the graph $E_g \subseteq D_g$ defined by $(x, y) \in E_g$ iff $g(x) < g(y)$ is monotone: list $f^{-1}(0) = \{x_1, \dots, x_p\}$ and $f^{-1}(1) = \{y_1, \dots, y_q\}$ so that $g(x_1) \geq \ldots \geq g(x_p)$ and $g(y_1) \leq \ldots \leq g(y_q)$. Thus, most restrictive condition in the definition of monotone circuit is the requirement that the graph E_{g_t}, associated with the last gate g_t, must be complete.

[1] Note that monotonicity means that we actually can order inputs from *both* sides $f^{-1}(0)$ and $f^{-1}(1)$.

Example 1 (Monotone real circuits). Let Φ be the set of all monotone nondecreasing functions $\phi : \mathbf{R}^m \to \mathbf{R}$, $m \geq 1$. Specifically, if $\alpha_1 \leq \beta_1, \ldots, \alpha_m \leq \beta_m$ are reals then $\phi(\alpha_1, \ldots, \alpha_m) \leq \phi(\beta_1, \ldots, \beta_m)$. Associate with each gate g the graph $E_g \subseteq D_g$ defined by $(x, y) \in E_g$ iff $g(x) < g(y)$. By the remark above, we have only make sure that the graph E_g, associated with the last gate $g = g_t$ of a circuit computing f, is complete. Since $D_g = f^{-1}(0) \times f^{-1}(1)$, we have only to verify that $E_g = D_g$. This can be easily shown by the induction on the number of gates. Take an edge $(x, y) \in D_g$ and let $g = \phi(h_1, \ldots, h_m)$. By the induction hypothesis, $D_{h_i} = E_{h_i}$ for all gates h_i $(i = 1, \ldots, m)$. Since ϕ is nondecreasing, this means that $g(x) \leq g(y)$, which together with the assumption that $(x, y) \in D_g$, implies that $g(x) < g(y)$, meaning that $(x, y) \in E_g$, as desired.

Example 2 (Unbounded fan-in AND/OR circuits). Such circuits are special case of monotone real circuits. Specific property of AND and OR gates is that the ϵ-degree of such a gate $g = \phi(h_1, \ldots, h_m)$ equals 1 if $\phi = \wedge$ and $\epsilon = 0$, or $\phi = \vee$ and $\epsilon = 1$. Indeed, if g is the AND and $g(x) = 0$ then $E_g(x) = E_{h_1}(x) \cap \ldots \cap E_{h_m}(x)$. The same holds if g is the OR and $g(x) = 1$.

3 The result

In this section we state our main result - general combinatorial lower bound for monotone real circuits. Throughout this section, let f be an arbitrary (but fixed) Boolean function.

We want our criterion to work in different situations, so we state it in most flexible form. By a *norm* we will mean any mapping $\mu : 2^N \to \{0, 1, \ldots\}$ which is monotone under the set-theoretic inclusion, i.e. $S \subseteq T$ implies $\mu(S) \leq \mu(T)$. Given such a norm, the *length* of a set S is the number $\mu(S)$. The *deviation* of μ is the function $\lambda(t) = \max\{|S| : \mu(S) \leq t\}$. The *defect* of μ is the maximal length $c = \max\{\mu(\{e\}) : e \in N\}$ of a single bit. These two characteristics connect the length $\mu(S)$ of S with its cardinality: $\mu(S) \leq c \cdot |S|$ and $|S| \leq \lambda(\mu(S))$. For an input x we denote by $I(x)$ the set of all bits e for which $x(e) = f(x)$. We say that a bit set T *respects* a norm μ if we cannot add a bit from outside the set T to no of its subsets without increasing their length, i.e. if $\mu(S \cup \{e\}) \geq \mu(S) + 1$ for any subset $S \subseteq T$ and any bit $e \notin T$. We say that an input x *respects* μ if the set $I(x)$ does this. For example, if we take the trivial norm $\mu(S) = |S|$ then $c = 1$, $\lambda(t) = t$ and *every* input respects μ. In case of graphs, bits correspond to edges and one can, for example, take $\mu(S)$ to be the number of vertices incident to at least one edge from S. In this case $c = 2$, $\lambda(t) = \binom{t}{2}$ and *only* inputs, corresponding to cliques, will respect such a norm.

Given random input $\mathbf{x}$ and a set of inputs $A \subseteq f^{-1}(\epsilon)$, define

- $\mathrm{Min}_b\,[\mathbf{x}, A, \mu] \rightleftharpoons \min \mathrm{Prob}[\mathbf{x} \in A \text{ and } \mathbf{x}(S) \equiv \epsilon \oplus 1]$ over all sets $S \subseteq N$ with $\mu(S) \leq b$,
- $\mathrm{Max}_a\,[\mathbf{x}, A, \mu] \rightleftharpoons \max \mathrm{Prob}[\mathbf{x} \in A \text{ and } \mathbf{x}(S) \equiv \epsilon]$ over all sets $S \subseteq N$ with $\mu(S) \geq a$.

Given a pair (μ_0, μ_1) of (not necessarily different) norms, we will be interested in the following characteristic of $\mathbf{x}$:

$$F_f^\epsilon(\mathbf{x}, a, b, d) \rightleftharpoons \frac{\mathrm{Min}_b\,[\mathbf{x}, X^\epsilon, \mu_{\epsilon\oplus 1}]}{(d \cdot \lambda(bc))^a \cdot \mathrm{Max}_a\,[\mathbf{x}, X^\epsilon, \mu_\epsilon]} \tag{1}$$

where X^ϵ denotes the set of all inputs from $f^{-1}(\epsilon)$ respecting the norm μ_ϵ; c and λ are the defect and the deviation of $\mu_{\epsilon\oplus 1}$. Given a random input $\mathbf{x}$ it is an easy task to find a lower bound for this characteristic. In particular, the numerator in (1) can be estimated by

$$\mathrm{Min}_b\,[\mathbf{x}, X^\epsilon, \mu_{\epsilon\oplus 1}] \geq \mathrm{Prob}[\mathbf{x} \in X^\epsilon] - \lambda(bc) \cdot p(\mathbf{x}, \epsilon) \tag{2}$$

where $p(\mathbf{x}, \epsilon)$ is the maximum of $\mathrm{Prob}[\mathbf{x}(e) = \epsilon]$ over all bits $e \in N$.

Our main result is the following general lower bounds criterion for monotone real circuits.

Theorem 3.1 *Let f be a monotone Boolean function on n variables and let C be a monotone real circuit computing f. Then for any random inputs $\mathbf{x}, \mathbf{y}$, any norms μ_0, μ_1 and any integers $1 \leq a, b \leq n$,*

$$\mathit{size}(C) \geq \min\left\{F_f^0(\mathbf{x}, a, b, d_1), F_f^1(\mathbf{y}, b, a, d_0)\right\} \tag{3}$$

where d_ϵ ($\epsilon \in \{0, 1\}$) is the maximum ϵ-degree of a gate in C.

The lower bound (3) depends on the degree of gates. The degree is always at most the fan-in, and hence, the criterion works well for small fain-in gates. If we want to allow large fan-in gates, we have to restrict their power since otherwise the whole circuit could consist of just one gate. Let us look at the most restrictive case: the case of unbounded fan-in ANDs and ORs. We have seen in Example 2 that for such gates one of degrees d_0 or d_1 is very small: $d_0 = 1$ for AND gates and $d_1 = 1$ for OR gates. But, in general, the dual degree $d_{\epsilon\oplus 1}$ of these gates can be as large as the fan-in. Nevertheless, the proof of Theorem 3.1 can be easily modified so that to get the following theorem.

Theorem 3.2 *Let C be a Boolean circuit with unbounded fan-in AND and OR gates and arbitrary monotone Boolean functions of fan-in ℓ at the bottom. If C computes f then, for any $\ell \leq a, b \leq n$, the bound (3) holds with $d_0 = d_1 = 1$.*

4 Limits, Witnesses and the Idea

In this section we define finite limits and describe the idea. Recall that $I(x)$ denotes the set of all bits e such that $x(e) = f(x)$.

Definition. A *witness* of an input x against a set of inputs A is a set of bits $S \subseteq N$ such that for every $y \in A$ there is a bit $e \in S$ for which $x(e) \neq y(e)$. A witness S is *legal* if $S \subseteq I(x)$. A *k-limit* for a set A under a norm μ is an input x such that $\mu(S) \geq k + 1$ for any legal witness S of x against A.

Before we go to formal proofs, let us first loosely describe the idea in the simplest case when both norms are trivial, i.e. when $\mu_0(S) = \mu_1(S) = |S|$, and we have only fan-in 2 AND and OR gates. (The general case follows the same idea taking more care about the possible deviations of norms from this trivial one.)

Given such a circuit $C = (g_1, \ldots, g_t)$ we associate with every its gate g the graph $E_g \subseteq f^{-1}(0) \times f^{-1}(1)$ defined by: $(x, y) \in E_g$ iff $g(x) = 0$ and $g(y) = 1$. These graphs are clearly monotone (in fact they are complete subgraphs), and $E_{g_t} = f^{-1}(0) \times f^{-1}(1)$. If some input $x \in f^{-1}(0)$ is a k-limit for the set $E_g(x)$ then we can treat x as a "hard instance" for the gate g because g correctly separates x from all its neighbors, even though this requires knowledge of more than k bits. We will use this property (of being a limit for the set of own neighbors) to color the nodes of the graph $f^{-1}(0) \times f^{-1}(1)$. We do this step-by-step going through the graphs $E_{g_1}, \ldots, E_{g_t}$.

Initially no node is colored. At the i-th step ($i = 1, \ldots, t$) we color a node x iff x was not colored so far and if x is a k-limit for the set of all its uncolored neighbors in the i-th graph E_{g_i}. To get a lower bound on the number t of gates in C it is enough to show that:

(i) after t steps most of the nodes in at least one part of E_{g_t} must be colored;

(ii) not too much new nodes are colored at each step.

Towards (i). If all the nodes in at least one of the parts $f^{-1}(0)$ or $f^{-1}(1)$ are colored, there is nothing to do. Suppose therefore that both parts have a uncolored nodes x. Take an uncolored node $x \in f^{-1}(0)$ and let Y be the set of all colored nodes in $f^{-1}(1)$. The fact that x remains uncolored means, in particularly, that x was *not* a k-limit for the set $E_{g_t}(x) \setminus Y = f^{-1}(1) \setminus Y$, where g_t is the last gate. This means that x must have a legal witness of length k against the set of uncolored nodes $f^{-1}(1) \setminus Y$. I.e. there must be a set of bits $S \subseteq I(x)$ such that $|S| \leq k$ and every uncolored input input from $f^{-1}(1)$ takes the value $f(x) \oplus 1 = 1$ on at least one bit in S. Thus, all the remaining inputs $y \in f^{-1}(1)$ with $y(S) \equiv 0$, must be already colored.

Towards (ii). Consider the i-th step of our coloration procedure. Take a gate $g_i = \phi(h_1, h_2)$ and assume w.l.o.g. that $\phi = \wedge$ (the case of $\phi = \vee$ is dual). First, observe that *no* new input $x \in f^{-1}(0)$ is colored at the i-th step. This is because in this case we have that $E_{g_i}(x) = E_{h_1}(x) \cap E_{h_2}(x)$, and hence, if x would be a limit for the set of its uncolored neighbors in the graph E_g, then x would also be a limit for the sets of neighbors in both previous graphs E_{h_1} and E_{h_2}, meaning that x should be already colored at some previous step. We have therefore only to show that not too much inputs from the other part $f^{-1}(1)$ are colored at the i-th step. Let $A \subseteq f^{-1}(1)$ be the set of all inputs which are colored at the i-th step, and let $B \subseteq f^{-1}(0)$ be the set of those inputs from the other side, which were not colored in previous steps. In terms of limits this means the following: *every* input from A is a k-limit for the set B and *no* input from B is a k-limit for A. It appears that this information is enough to show that A cannot be too large. This is the content of the 'limit lemma' (Lemma 5.2) which we prove in the next section. In our simplest case (of trivial norms), they state that $|A|$ is at most k^k times the maximum number of inputs from A, all of which take the value 1 on some fixed set of k bits.

We now turn to formal proofs. The notations and statements are somewhat more cumbersome because now we allow arbitrary norms. We first prove desired limit lemma.

5 Limit lemma

We will make use of the following simple lemma about transversals. Let $\mathcal{F} = \{S_1, \ldots, S_t\}$ be a sequence of bit sets and let μ be a norm. A *k-critical transversal* for $\mathcal{F}$ under the norm μ is a set T, which respects μ and for which there is an index $l \in \{1, \ldots, t\}$ such that T intersects all the sets $S_1, \ldots, S_l$ but no its subset $T' \subseteq T$ with $\mu(T') \leq k$ does this. We also say that a set T *covers* a set S if $T \supseteq S$.

Lemma 5.1 *Let $\mathcal{F}$ be a sequence of bit sets, each of cardinality at most r. Let μ be a norm and c be its defect. Let $\mathcal{T}$ be a family of ac-critical under μ transversals for $\mathcal{F}$. Then there is a family $\mathcal{H}_a$ of bit sets such that:* (i) $|\mathcal{H}_a| \leq r^a$, (ii) $a \leq \mu(H) \leq ac$ *for all $H \in \mathcal{H}_a$, and* (iii) *every set from $\mathcal{T}$ covers at least one set from $H \in \mathcal{H}_a$.*

Proof. Let $\mathcal{F} = \{S_1, \ldots, S_t\}$. We will construct the desired family $\mathcal{H}_a$ by induction on a. For $a = 1$ we can choose the first set S_i such that $\mu(\{e\}) \neq 0$ for all $e \in S_i$, and take as $\mathcal{H}_1$ the family of all one element sets $\{e\}$ with $e \in S_i$. This family has at most $|S_i| \leq r$ sets, each of which has length at most c, as desired. Suppose now that the family $\mathcal{H}_{a-1}$ is already constructed. For a set of bits H, let $\mathrm{ext}(H)$ denote the set of all transversal in $\mathcal{T}$ covering H. We can assume w.l.o.g. that $\mathrm{ext}(H) \neq \emptyset$ for every set H in $\mathcal{H}_{a-1}$ (if not, remove all other sets). We construct the desired family $\mathcal{H}_a$ by applying the following procedure to the family $\mathcal{H}_{a-1}$.

Take a set H in $\mathcal{H}_{a-1}$ and choose the first index i such that $H \cap S_i = \emptyset$ but $T \cap S_i \neq \emptyset$ for all $T \in \mathrm{ext}(H)$ (such an i exists since $\mu(H) \leq (a-1)c < ac$ and H is a subset of an ac-critical transversal). There are two possibilities: either there is some bit $e \in S_i$ for which $\mu(H \cup \{e\}) = \mu(H)$, or not. In the first case replace the set H in $\mathcal{H}_{a-1}$ by $H \cup \{e\}$. Since all the transversals in $\mathrm{ext}(H)$ respect the norm μ, we have that $\mu(H \cup \{e\}) = \mu(H)$ implies $\mathrm{ext}(H \cup \{e\}) = \mathrm{ext}(H)$. Hence, no transversal gets lost during this step, and we can repeat the procedure with the new family. In the second case include in $\mathcal{H}_a$ all the sets $H \cup \{e\}$ with $e \in S_i$, remove H from $\mathcal{H}_{a-1}$ and repeat the procedure to this smaller family $\mathcal{H}_{a-1} \setminus \{H\}$. No transversal gets lost also during this step, since every transversal covering H, must cover at least one of these new sets $H \cup \{e\}$ with $e \in S_i$. Moreover, we have that $\mu(H \cup \{e\}) \geq \mu(H) + 1 \geq (a-1) + 1 = a$

and $\mu(H \cup \{e\}) \leq \mu(H) + c \leq (a-1)c + c = ac$, as desired. Since every set in $\mathcal{H}_{a-1}$ produces at most $|S_i| \leq r$ new sets, the resulting family $\mathcal{H}_a$ will have at most $r \cdot |\mathcal{H}_{a-1}| \leq r^a$ sets, as desired. ■

Main property of finite limits, which we will use in our lower bounds argument is expressed by the following 'limit lemma'.

Lemma 5.2 *Let μ_1 and μ_2 be norms; c be the defect of μ_1 and λ be the deviation of μ_2. Let $A = \{x_1, \ldots, x_t\}$ be a sequence of inputs from $f^{-1}(\epsilon)$, each of which respects the norm μ_1, and suppose that there is a sequence of sets $\emptyset \neq B_1 \subseteq \ldots \subseteq B_t \subseteq f^{-1}(\epsilon \oplus 1)$ such that, for every $i = 1, \ldots, t$*

(i) *input x_i is an ac-limit for B_i under the norm μ_1,*

(ii) *no input from B_i is a b-limit for the set $A_i = \{x_i, \ldots, x_t\}$ under the norm μ_2.*

Then for any random input $\mathbf{x}$, $\mathrm{Prob}[\mathbf{x} \in A] \leq \lambda(b)^a \cdot \mathrm{Max}_a\,[\mathbf{x}, A, \mu_1]$.

Proof. By (ii), every input from B_i has a legal witness of length at most b against the set A_i. That is, for every input $y \in B_i$ there is a subset of bits $S_{i,y}$ such that $|S_{i,y}| \leq \lambda(b)$ and every input $x \in A_i$ takes the value $x(e) = y(e) \oplus 1 = \epsilon$ on at least one bit $e \in S_{i,y}$. This, in particular, means that for every $x \in A_i$, the set $I(x)$ intersects all the sets in the sequence $\mathcal{F}_i = \{S_{i,y} : y \in B_i\}$ (with sets $S_{i,y}$ arranged in arbitrary order). Now, for each $j = 1, \ldots, t$ the input x_j belongs to all the sets $A_1, \ldots, A_j$, and hence, the set $I(x_j)$ must intersect all the sets in the sequence $\mathcal{F}^j = \{\mathcal{F}_1, \ldots, \mathcal{F}_j\}$. On the other hand, by (i), no subset S of $I(x_j)$, such that $\mu(S) \leq ac$, can do this, since any such S would be a legal witness of x_j against B_j. Since x_j respects the norm μ_1, the set $I(x_j)$ also respects it. Thus, for every $j = 1, \ldots, t$, the set $I(x_j)$ is an ac-critical transversal for the sequence $\mathcal{F}^j$, and hence, is such a transversal for the whole sequence $\mathcal{F}^t$. By Lemma 5.1 there must be a family $\mathcal{H}$ consisting of $\lambda(b)^a$ sets H such that $\mu_1(H) \geq a$ and every set $I(x)$ with $x \in A$, covers at least one of these sets. Thus,

$$\begin{aligned}
\mathrm{Prob}[\mathbf{x} \in A] &\leq \sum_{x \in A} \mathrm{Prob}[\mathbf{x} \in A \text{ and } \mathbf{x}(e) = \epsilon, \forall e \in I(x)] \\
&\leq \sum_{H \in \mathcal{H}} \mathrm{Prob}[\mathbf{x} \in A \text{ and } \mathbf{x}(H) \equiv \epsilon] \leq \lambda(b)^a \cdot \mathrm{Max}_a\,[\mathbf{x}, A, \mu_1],
\end{aligned}$$

as desired. ■

We finish this section with one trivial but useful fact.

Lemma 5.3 *If x is an sd-limit for a set A then, for any partition $A = A_1 \cup \ldots \cup A_d$ of A into d sets, x is an s-limit for at least one of these sets.*

Proof. If x would have a (legal) witness S_i of length s against A_i, for all $i = 1, \ldots, d$, then $S = S_1 \cup \ldots \cup S_d$ would be a (legal) witness of x against the whole set A, and (by the monotonicity of norms) this witness would have length at most ds. ■

6 Proof of Theorem 3.1

To unify notations, set $k_0 \rightleftharpoons a \cdot c_0$ and $k_1 \rightleftharpoons b \cdot c_1$, where parameters a and b are from the statement of Theorem 3.1, and c_ϵ is the defect of the norm μ_ϵ. Let $C = (g_1, \ldots, g_t)$ be a monotone real circuit computing f. For $\epsilon \in \{0,1\}$, let X^ϵ denote the set of all the inputs in $f^{-1}(\epsilon)$ which respect the norm μ_ϵ. For a gate g, let $E'_g(x) = E_g(x) \cap X^{f(x)\oplus 1}$. Say that an input x is *hard* for a gate g if $x \in X^{f(x)}$ and g is the first gate (in C) such that x is a $k_{f(x)}$-limit for the set of all those inputs in $E'_g(x)$ which were hard for no previous gate. Let Y_g denote the set of all inputs which are hard for a gate g, and set $Y^\epsilon = Y^\epsilon_{g_1} \cup \cdots Y^\epsilon_{g_t}$ where $Y^\epsilon_g = Y_g \cap f^{-1}(\epsilon)$, $\epsilon \in \{0,1\}$. Thus, $Y = Y^0 \cup Y^1$ is the set of inputs which were hard for at least one gate of C. Theorem 3.1 follows directly from the following two claims.

Claim 1: There is an $\epsilon \in \{0,1\}$ such that for any random input $\mathbf{x}$ we have that

$$\text{Prob}[\mathbf{x} \in Y^\epsilon] \geq \text{Min}_b\left[\mathbf{x}, X^\epsilon, \mu_{\epsilon\oplus 1}\right]. \tag{4}$$

Claim 2: For every gate g of C, any random input $\mathbf{x}$ and both $\epsilon = 0,1$ we have that

$$\text{Prob}\left[\mathbf{x} \in Y^\epsilon_g\right] \leq \lambda(d_{\epsilon\oplus 1} \cdot k_{\epsilon\oplus 1})^r \cdot \text{Max}_r\left[\mathbf{x}, X^\epsilon, \mu_\epsilon\right] \tag{5}$$

where $r = k_\epsilon / c_\epsilon$ and λ is the deviation of the norm $\mu_{\epsilon\oplus 1}$.

Proof of Claim 1. If $Y^\epsilon = X^\epsilon$ for some $\epsilon = 0,1$ then (4) is trivial. Otherwise, we have that $X^\epsilon \setminus Y \neq \emptyset$ for both $\epsilon = 0$ and $\epsilon = 1$. This, in particular, means that (for both $\epsilon = 0,1$) there is at least one input x such that $f(x) = \epsilon \oplus 1$, x respects the norm $\mu_{\epsilon\oplus 1}$ and x is hard for *no* gate of C, including the last gate g_t. By the definition of hardness, x must have a legal witness S of length $\mu_{\epsilon\oplus 1}(S) \leq k_{\epsilon\oplus 1}$

against the set $E'_{g_t}(x) \setminus Y = X^\epsilon \setminus Y$. Here $E'_{g_t}(x) = X^\epsilon$ because C computes f which means that $E_{g_t}(x) = f^{-1}(f(x) \oplus 1)$ for all inputs x. The legality of S means that $x(e) = f(x) = \epsilon \oplus 1$ for all $e \in S$, and hence, every input in $X^\epsilon \setminus Y$ must take a value ϵ on at least one bit from S. Thus, $\mathrm{Prob}[\mathbf{x} \in Y^\epsilon] = \mathrm{Prob}[\mathbf{x} \in X^\epsilon] - \mathrm{Prob}[\mathbf{x} \in X^\epsilon \setminus Y] \geq \mathrm{Prob}[\mathbf{x} \in X^\epsilon] - \mathrm{Prob}[\mathbf{x} \in X^\epsilon \text{ and } \mathbf{x}(S) \not\equiv \epsilon \oplus 1] = \mathrm{Prob}[\mathbf{x} \in X^\epsilon \text{ and } \mathbf{x}(S) \equiv \epsilon \oplus 1] \geq \mathrm{Min}_b\left[\mathbf{x}, X^\epsilon, \mu_{\epsilon\oplus 1}\right]$, as desired. ■

Proof of Claim 2. If g is a bottom gate then $Y_g^0 = Y_g^1 = \emptyset$. This is because for *every* monotone function g and for every input $x \in g^{-1}(\epsilon)$ the set of bits $S = \{e : x(e) = \epsilon\}$ is a legal witness of x against $g^{-1}(\epsilon \oplus 1)$. Since, by the assumption, g depends on at most ℓ variables and $\ell \leq \min\{a, b\}$, the length $\mu_\epsilon(S)$ of this witness does not exceed k_ϵ, and hence, x cannot be hard for g.

Now, let $g = \phi(h_1, \ldots, h_m)$ be an arbitrary gate of C, and let Z be the set of all inputs which were hard for at least one previous gate. Thus,

$$Y_g^\epsilon = \left\{x \in X^\epsilon : x \notin Z \text{ and } x \text{ is a } k_\epsilon\text{-limit for } E'_g(x) \setminus Z\right\}.$$

By the monotonicity of the gate g, we can list the inputs $Y_g^\epsilon = \{x_1, \ldots, x_t\}$ in such a way that $E'_g(x_1) \subseteq \ldots \subseteq E'_g(x_t)$.

We are going to apply Lemma 5.2 with $A \rightleftharpoons Y_g^\epsilon$, $a \rightleftharpoons k_\epsilon / c_\epsilon$, $b \rightleftharpoons d_{\epsilon\oplus 1} \cdot k_{\epsilon\oplus 1}$ and $B_i \rightleftharpoons E'_g(x_i) \setminus Z$, for $i = 1, \ldots, t$. The first condition (i) of this lemma is satisfied by the definition of Y_g^ϵ. To verify the second condition (ii), assume for the sake of contradiction, that some input $y \in B_i$ *is* a b-limit for the set $A_i = \{x_i, \ldots, x_t\}$. Since $A \cap Z = \emptyset$ and $E'_g(x_i) \subseteq \ldots \subseteq E'_g(x_t)$, we have that $A_i \subseteq E'_g(y) \setminus Z$. Since $f(y) = \epsilon \oplus 1$ and the $(\epsilon \oplus 1)$-degree of g is at most $d_{\epsilon\oplus 1}$, there must be a subset $I \subseteq [m]$ such that $|I| \leq d_{\epsilon\oplus 1}$ and $A_i = \bigcup_{j\in I} A_i \cap E'_{h_j}(y)$. Hence, if y would be a b-limit for the whole set A_i then, by Lemma 5.3, y would also be a $\frac{b}{d_{\epsilon\oplus 1}}$-limit for at least one of the sets $A_i \cap E'_{h_j}(y)$, $j \in I$. Since $\frac{b}{d_{\epsilon\oplus 1}} = k_{\epsilon\oplus 1} = k_{f(y)}$ and $A_i \cap E'_{h_j}(y) \subseteq E'_{h_j}(y) \setminus Z$, this would mean that y should already be hard for this gate h_j (or some previous gate), and hence, should belong to Z, which is impossible since $y \in B_i$, a contradiction. Thus, we can apply Lemma 5.2 to the set $A = Y_g^\epsilon$ with $a = k_\epsilon / c_\epsilon$ and $b = d_{\epsilon\oplus 1} \cdot k_{\epsilon\oplus 1}$, and the desired upper bound (5) follows. This completes the proof of Claim 2, and thus the proof of Theorem 3.1. ■

7 Proof of Theorem 3.2

The argument is the same as in the proof of Theorem 3.1, exploiting essentially one particular property of AND and OR gates (mentioned already in Example 2 of Section 2). The reason why we have to be more careful here is that now we have unbounded fan-in AND/OR gates, one of the two degrees d_0 or d_1 of which can be as large as the fan-in. To unify notations, we say that $g = \phi(h_1, \ldots, h_m)$ is 1-gate if $\phi = \wedge$ and 0-gate $\phi = \vee$. What we need is to prove the following stronger version of Claim 2 (under the same notations).

Claim 2': For every gate g of C, random input $\mathbf{x}$ and both $\epsilon = 0, 1$ we have that

$$\mathrm{Prob}[\mathbf{x} \in Y^{\epsilon}] \leq \lambda(k_{\epsilon\oplus 1})^{r} \cdot \mathrm{Max}_r\left[\mathbf{x}, X^{\epsilon}, \mu_{\epsilon}\right] \tag{6}$$

where $r = k_{\epsilon}/c_{\epsilon}$ and λ is the deviation of the norm $\mu_{\epsilon\oplus 1}$.

Proof of Claim 2'. Let g be a δ-gate for some $\delta \in \{0, 1\}$. Then $E'_g(x) = E'_{h_1}(x) \cup \ldots \cup E'_{h_m}(x)$ if $f(x) = \delta$, and $E'_g(x) = E'_{h_1}(x) \cap \ldots \cap E'_{h_m}(x)$ if $f(x) = \delta \oplus 1$. Hence, if some input $x \in f^{-1}(\delta \oplus 1)$ would be a limit for $E'_g(x)$ then this input would be also a limit for all the sets $E'_{h_1}(x), \ldots, E'_{h_m}(x)$, meaning that this input should already be hard for some (previous to g) gate. Thus, $Y^{\delta\oplus 1} = \emptyset$ which, in particular, means that (6) holds for $\epsilon = \delta \oplus 1$. But for $\epsilon = \delta$ the $(\epsilon \oplus 1)$-degree of the gate g equals 1 and the bound (6) follows from (5) with $d_{\epsilon\oplus 1} = 1$. This completes the proof of Claim 2', and thus, the proof of Theorem 3.2. ■

8 Two applications

8.1 Detecting cliques

Let N be the family of all $n = \binom{m}{2}$ 2-element subsets (*edges*) of some set V of m vertices. This way every input $x : N \to \{0, 1\}$ can be identified with the undirected graph $G_x = (V, E)$ where $(u, v) \in E$ iff $x(u, v) = 1$. The *clique function* $\mathrm{CLIQUE}_{m,k}$ 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 [15] proved the first 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 $2^{\Omega(k^{1/2})}$ for any $k \leq (m/8\log m)^{2/3}$. These bounds in [1] were proved for usual model of fan-in 2 AND/OR gates but Pudlák in [14] has shown that in fact Razborov's argument works for circuits with arbitrary monotone fan-in 2 real functions as gates. Yao [23] considered monotone circuits with arbitrary monotone Boolean functions of fan-in $\leq n^{\epsilon}$ as gates, and proved that any such circuits computing $\mathrm{CLIQUE}_{m,k}$ with $k = \log\log m$, requires super-polynomial size. It appears that in case of AND and OR gates even unbounded fan-in does not help. Applying theorems 3.1 and 3.2 we extend the lower bounds of [1, 14] to more general circuits and the result of [23] to unbounded fan-in AND/OR gates.

Corollary 8.1 *Let $k \leq m^{2/3}(\ln m)^{1/3}/d^{1/3}$. Let C be a monotone real circuit and d be the maximum degree of its gate. If C computes $\mathrm{CLIQUE}_{m,k}$ then it has size exponential in $\Omega\left(\sqrt{\frac{k}{d\ln m}}\right)$. If C consists of unbounded fan-in AND/OR gates and has arbitrary monotone Boolean functions of fan-in at most $k^{1/2-o(1)}$ at the bottom, then the same lower bound holds with $d = 1$.*

Proof. Let $f = \mathrm{CLIQUE}_{m,k}$. Let $\mathbf{x}$ be a random input, which on every bit takes independently the value 1 with probability $1-\gamma$ where $\gamma = 4k^{-1}\ln(m/k)$. This input corresponds to a random graph $G_{\mathbf{x}}$ on m vertices, in which every edge appears independently with probability $1-\gamma$. Let $\mathbf{y}$ be a random input, uniformly distributed in the set of all (inputs corresponding to) k-cliques; thus $\mathbf{y}$ is k-clique with probability $\binom{m}{k}^{-1}$. We are going to apply Theorem 3.1 with the following pair of norms: $\mu_0(S) = |S|$ and $\mu_1(S) =$ the number of vertices incident to at least one edge from S. The defect and deviation for these norms are: $c_0 = 1$ and $\lambda_0(t) = t$ for μ_0, and $c_1 = 2$ and $\lambda_1(t) = \binom{t}{2}$ for μ_1. We have only to calculate the values of F_f^0 and F_f^1 in (3).

For the first input $\mathbf{x}$ we have that $p(\mathbf{x},0)$ is the probability that the graph $G_{\mathbf{x}}$ avoids a single edge, and hence, $p(\mathbf{x},0) = \gamma$; $\mathrm{Max}_a\left[\mathbf{x}, X^0, \mu_0\right]$ is at most the probability that $G_{\mathbf{x}}$ avoids some fixed set of a edges, and hence, is at most γ^a. Since $f(\mathbf{x}) = 1$ iff $G_{\mathbf{x}}$ contains a k-clique, we have, by the choice of γ, that $\mathrm{Prob}[f(\mathbf{x}) = 0] \geq 1 - \binom{m}{k}(1-\gamma)^{\binom{k}{2}} \geq 2/3$. Moreover, $X^0 = f^{-1}(0)$ since μ_0 is the trivial norm. Since $\lambda_1(2b)\cdot\gamma \leq 1/3$ for any $b \leq (k/24\ln(m/k))^{1/2}$, we have by (2) that the first term $F_f^0(\mathbf{x},a,b,d)$ in (3) is at least

$$\frac{\mathrm{Prob}[\mathbf{x} \in X^0] - \lambda_1(2b)\cdot p(\mathbf{x},0)}{(d\cdot\lambda_1(2b))^a \cdot \mathrm{Max}_a\left[\mathbf{x}, X^0, \mu_0\right]} \geq \frac{1}{3}\left(\frac{1}{4db^2\gamma}\right)^a \geq \frac{1}{3}\left(\frac{k}{8db^2\ln(m/k)}\right)^a. \qquad (7)$$

For the second input $\mathbf{y}$ we have that $\mathrm{Prob}[\mathbf{y} \in X^1] = 1$ (since cliques respect the norm μ_1), and $p(\mathbf{y}, 1)$ is the probability that a random k-clique contains a fixed edge, and hence, is at most $\binom{m-2}{k-2}/\binom{m}{k} \leq (k/m)^2$; $\mathrm{Max}_b\,[\mathbf{y}, X^1, \mu_1]$ is the probability that a random k-clique contains some fixed set of b vertices, and hence, is at most $\binom{m-b}{k-b}/\binom{m}{k}$. Thus, for any $a \leq (m/k)^2/2$, the second term $F_f^1(\mathbf{y}, b, a, d)$ in (3) is

$$\frac{\mathrm{Prob}[\mathbf{x} \in X^1] - \lambda_0(a) \cdot p(\mathbf{y}, 1)}{(d \cdot \lambda_0(a))^b \cdot \mathrm{Max}_b\,[\mathbf{y}, X^1, \mu_1]} \geq \frac{\binom{m}{k}\left(1 - a(k/m)^2\right)}{(da)^b \cdot \binom{m-b}{k-b}} \geq \frac{1}{2}\left(\frac{m}{dak}\right)^b . \tag{8}$$

Take $a = \lceil m/(2dk) \rceil$ and $b = \lceil (k/24d \ln(m/k))^{1/2} \rceil$. For these values of a and b, estimate in (7) is $2^{\Omega(a)} = 2^{\Omega(m/dk)}$, and in (8) is $2^{\Omega(b)} = 2^{\Omega\left(\sqrt{k/d \ln m}\right)}$, which by (3) gives the desired lower bound. ∎

8.2 Drawing polynomials

Let $GF(q)$ denote the finite field with q elements, where q is a prime power, and consider the square $N = GF(q) \times GF(q)$. This way bits are points (i, j) in this square, and every input $x : N \to \{0, 1\}$ corresponds to a 2-coloring of points. Given such a coloring, we are interested in the possibility to draw the graph of some small-degree polynomial using only points colored by "1". Namely, define $\mathrm{POLY}_{q,s}$ to be the Boolean function on $n = q^2$ variables, whose value on an input x is 1 iff there exists a polynomial $p(z)$ over $GF(q)$ of degree at most $s - 1$ such that $\forall (i, j) \in N$: $x(i, j) = 1$ iff $p(i) = j$.

Andreev [2], using the argument similar to the method of approximations, showed that any fan-in 2 AND/OR circuit computing this function (for appropriate values of s) requires size at least $\exp(\Omega(n^{1/8-\epsilon})$. Using Razborov's method of approximations, Alon and Boppana [1] were able to essentially improve this bound until $q^{\Omega(s)}$ for any $s \leq (q/\ln q)^{1/2}/2$; for maximal possible s this bound is exponential in $\Omega(n^{1/4}\sqrt{\ln n})$, and this is the largest[2] known lower bound for 'natural' function in NP. This bound is almost optimal because q^{s+1} is the trivial upper bound for $\mathrm{POLY}_{q,s}$ (this function is an OR of q^s monomials, each of q literals). Using our criterion we extend this lower bound to circuits with unbounded fan-in AND/OR gates and monotone circuits over the reals.

[2] Numerically, the largest is the lower bound $\exp(n^{1/3-o(1)})$ proved in [3] for a somewhat contrived version of $\mathrm{POLY}_{q,s}$. When applied to that function, our criterion also gives the same lower bound.

Corollary 8.2 *Let $s \le (q/\ln q)^{1/2}/2$ and let C be a monotone real circuit computing $\mathrm{POLY}_{q,s}$. Then C has size $q^{\Omega(s/d)}$ where $d = 1$ if C has only unbounded fan-in AND/OR gates and arbitrary monotone Boolean functions of fan-in at most s at the bottom, and d is the maximal degree of a gate in C, otherwise.*

Proof. Let $f = \mathrm{POLY}_{q,s}$. We will apply Theorem 3.1 with trivial norms: $\mu_0(S) = \mu_1(S) = |S|$. Since all the inputs respect such norm, we have that $X^0 = f^{-1}(0)$ and $X^1 = f^{-1}(1)$. Let $\mathbf{x}$ be a random input, which on each point (i,j) independently takes the value 0 with probability γ and takes the value 1 with probability $1-\gamma$ (where γ is a parameter to be fixed later). Let $\mathbf{y}$ be a random input distributed uniformly on the set of graphs of all polynomials over $GF(q)$ of degree at most $s-1$.

For the first input $\mathbf{x}$ we have that $p(\mathbf{x},0) = \gamma$, $\mathrm{Max}_a\,[\mathbf{x}, X^0, \mu_0] \le \gamma^a$ and $\mathrm{Prob}[\mathbf{x} \in X^0] = \mathrm{Prob}[f(\mathbf{x}) = 0] = 1 - \mathrm{Prob}[f(\mathbf{x}) = 1] \ge 1 - q^s(1-\gamma)^q$ which is at least $1/2$ for $\gamma = (s \ln q + \ln 2)/q \le (2s \ln q)/q$. For the second input $\mathbf{y}$ we have that $\mathrm{Prob}[\mathbf{y} \in X^1] = \mathrm{Prob}[f(\mathbf{y}) = 1] = 1$, $p(\mathbf{y},1) \le 1/q$ and $\mathrm{Max}_b\,[\mathbf{y}, X^1, \mu_1]$ is the maximum fraction of polynomials of degree at most $s-1$, all of which coincide on some fixed set of b elements from $GF(q)$; hence, $\mathrm{Max}_b\,[\mathbf{y}, X^1, \mu_1] \le q^{-b}$ for any $b \le s$. Taking $a = \lceil (s \ln q)/d \rceil$, $b = \lceil s/d \rceil$, and $\gamma = (2s \ln q)/q$ we get

$$F_f^0(\mathbf{x}, a, b, d) \ge \frac{1/2 - b\gamma}{(db)^a \gamma^a} \ge \frac{1}{6}\left(\frac{q}{2dbs \ln q}\right)^a \ge q^{\Omega(s/d)},$$

and

$$F_f^1(\mathbf{y}, b, a, d) \ge \frac{1 - a/q}{(da)^b q^{-b}} = \frac{1}{2}\left(\frac{q}{da}\right)^b \ge q^{\Omega(s/d)}$$

and Theorem 3.1 gives the desired lower bound. ■

9 Conclusion

Finite limits have already been shown to provide a convenient framework in which to prove lower bounds for different models of computation: AC^0-circuits [11], depth-three threshold circuits [13], multi-party protocols and syntactic read-k-times branching programs [12]. All these applications are based on an appropriate 'limit lemma' about the existence of inputs in $f^{-1}(0)$ which are limits for $f^{-1}(1)$. In some cases (like bounded depth circuits) this leads to new lower bounds, in other (like read-k-times programs or multiparty games) we get simpler proofs of known bounds.

In this paper we have argued that finite limits are also appropriate objects to capture 'bottlenecks' in the information flow during a monotone computation. It would be interesting to understand to what extend they can do this without the monotonicity constrain. One possibility here would be to relax the legality constrain for witnesses. The legality we used in this paper enables one to treat differently $0'$s and $1'$s in inputs from different parts $f^{-1}(0)$ and $f^{-1}(0)$. This makes the criterion easy to apply, but cannot handle negation gates, i.e. gates switching the role of $0'$s and $1'$s.

References

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

[2] A. E. Andreev, On a method for obtaining lower bounds for the complexity of individual monotone functions, *Doklady Akademii Nauk SSSR,* 282:5 (1985), pp. 1033-1037. English translation in: *Soviet Mathematics Doklady,* 31, pp. 530-534.

[3] A. E. Andreev, On a method for obtaining effective lower bounds on the monotone complexity, *Algebra i Logika,* **26**:1 (1987), 3-26.

[4] M. Bonet, T. Pitassi, and R. Raz, Lower bounds for cutting planes proofs with small coefficients. In *Proc. Twenty-seventh Ann. ACM Symp. Theor. Comput.*, pages 575–584, 1995.

[5] R. B. Boppana and M. Sipser, The complexity of finite functions. In *Handbook of Theoretical Computer Science*, Vol. A, *Algorithms and Complexity*, J. van Leeuwen, Ed., MIT Press, pages 757–804, 1990.

[6] W. Cook, C. R. Coullard, and Gy. Turán, On the complexity of cutting plane proofs. *Disc. Appl. Math.*, pages 25–38, 1987.

[7] S. Cook and A. Rosenbloom, Some results on monotone real circuits, (manuscript)

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

[9] A. Haken, Counting Bottlenecks to Show Monotone P$\neq$NP, In *Proc. of the 36th Ann. IEEE Symp. Found. Comput. Sci.*, 1995.

[10] A. Haken and S. Cook, An exponential lower bound for the size of monotone real circuits, (manuscript).

[11] J. Håstad, S. Jukna and P. Pudlák, Top-down lower bounds for depth-three circuits, *Computational Complexity*, **5** (1995), 99–112.

[12] S. Jukna, Finite limits and lower bounds for circuit size, Tech. Rep. Nr. 94-06, Informatik, University of Trier, 1994.

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

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

[15] 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

[16] A. A. Razborov, *A lower bound on the monotone network complexity of the logical permanent,* Matematicheskie Zametki, 37:6 (1985) pp. 887-990 (in Russian); English translation in: Math. Notes Acad. of Sci. USSR, 37:6, pp. 485-493.

[17] 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.

[18] A. A. Razborov, On the method of approximations, In *Proc. of the 21th Ann. ACM Symp. Theor. Comput.,* (1989), pp. 167–176.

[19] A. A. Razborov, On small size approximation models. To appear in the volume *Mathematics of Paul Erdös.*

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

[21] M. Sipser, *Personal communication*, (1991)

[22] I. Wegener, *The Complexity of Boolean Functions*, B.G. Teubner and John Wiley & Sons, 1987.

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