COMBINATORICA 7 (1) (1987) 1—22

# THE MONOTONE CIRCUIT COMPLEXITY OF BOOLEAN FUNCTIONS

N. ALON and R. B. BOPPANA

*Received 15 November 1985*

Recently, Razborov obtained superpolynomial lower bounds for monotone circuits that tect cliques in graphs. In particular, Razborov showed that detecting cliques of size $s$ in a graph ith $m$ vertices requires monotone circuits of size $\Omega(m^s/(\log m)^{2s})$ for fixed $s$, and size $m^{\Omega(\log m)}$ for $\lfloor \log m/4 \rfloor$.

In this paper we modify the arguments of Razborov to obtain exponential lower bounds for onotone circuits. In particular, detecting cliques of size $(1/4)(m/\log m)^{2/3}$ requires monotone circuits f size $\exp(\Omega((m/\log m)^{1/3}))$. For fixed $s$, any monotone circuit that detects cliques of size $s$ requires $m^s/(\log m)^s)$ AND gates. We show that even a very rough approximation of the maximum clique e of a graph requires superpolynomial size monotone circuits, and give lower bounds for some ner Boolean functions. Our best lower bound for an NP function of $n$ variables is $\exp(\Omega(n^{1/4}\cdot(\log n)^{1/2}))$, improving a recent result of $\exp(\Omega(n^{1/8-\varepsilon}))$ due to Andreev.

## 1. Introduction

In 1949, Shannon [14] showed that almost all Boolean functions have expontially large circuit complexity. Unfortunately, the best circuit lower bound for a oblem in NP is only $3n$ (Blum [4]). Circuit lower bounds are important since a uperpolynomial circuit lower bound for a problem in NP implies that P$\neq$NP.

Because lower bounds for general circuits seem difficult to prove, many people have studied restricted circuit models. One restriction is to consider only *monotone* circuits, with AND gates and OR gates allowed but no NOT gates allowed. Until recently, however, the best known lower bound for the monotone circuit complexity of a single monotone problem in NP was a $4n$ lower bound (Tiekenheinrich [16]). Wegener [18] gave an $\Omega(n^2/\log n)$ lower bound for simultaneously computing a set of $n$ Boolean functions (in NP) of $n$ variables.

Recently, Razborov [12] achieved a major development, namely obtaining supolynomial lower bounds for monotone circuits. For a Boolean function $f$, let $(f)$ denote the monotone circuit complexity of $f$. For $1 \leqq s \leqq m$, let CLIQUE$(m, s)$ e the function of $n=\binom{m}{2}$ Boolean variables representing the edges of an undirected

First author supported in part by Allon Fellowship, by Bat Sheva de-Rotschild Foundation by the Fund for basic research administered by the Israel Academy of Sciences.

Second author supported in part by a National Science Foundation Graduate Fellowship.

AMS subject classification (1980): 68 E 10, 68 C 25 graph $G$ on $m$ vertices, whose value is 1 iff $G$ contains an $s$-clique. In [12] Razborov shows that

$$L^+(\mathrm{CLIQUE}(m, s)) \geqq m^s(s^3e^s \ln m)^{-2s},$$

and concludes that for fixed $s$

$$L^+(\mathrm{CLIQUE}(m, s)) = \Omega\left(\frac{m^s}{(\log m)^{2s}}\right), \tag{1.1}$$

and that for $s = \left\lfloor \frac{1}{4} \ln m \right\rfloor$

$$L^+(\mathrm{CLIQUE}(m, s)) = m^{\Omega(\log m)}.$$

Here we modify the arguments of [12] to improve the lower bounds. Our main results are exponential lower bounds for the monotone circuit complexity of several Boolean functions. In particular we show that

$$L^+(\mathrm{CLIQUE}(m, s)) \geqq \frac{1}{8}\left(\frac{m}{4s^{3/2}\log m}\right)^{(\sqrt{s}+1)/2},$$

and thus for $s = \lfloor (m/(8 \log m))^{2/3} \rfloor$ we have

$$L^+(\mathrm{CLIQUE}(m, s)) = \exp\left(\Omega((m/\log m)^{1/3})\right).$$

The method also supplies lower bounds on the monotone complexity of Boolean functions that approximate the maximum clique size of a graph. For example, we show that if $f$ is any Boolean function of $n = \binom{m}{2}$ variables representing the edges of a graph $G$ whose value is 0 if $G$ contains no clique of size $\lfloor (\log m)^4 \rfloor$, is 1 if $G$ contains a clique of size $\lfloor m/(8(\log m)^3) \rfloor$, and is arbitrary otherwise, then

$$L^+(f) = m^{\Omega(\log m)}.$$

We also improve (1.1) and show that for fixed $s$

$$L^+(\mathrm{CLIQUE}(m, s)) = \Omega\left(\frac{m^s}{(\log m)^s}\right).$$

In fact, we show that any monotone circuit that computes $\mathrm{CLIQUE}(m, s)$ (for fixed $s$) contains at least $\Omega(m^s/(\log \mathrm{m})^s)$ AND gates.

As mentioned above, our methods are basically a modification of those appearing (without proof) in [12]; however, our paper is self-contained.

Razborov obtains his lower bound for the monotone complexity $L^+(f)$ of a Boolean function $f$ in the following two steps:

(i) For every lattice $K$ from a properly defined family of lattices, he defines the distance $\varrho(f, K)$ from $f$ to $K$ and shows that

$$L^+(f) \geqq \varrho(f, K). \tag{1.2}$$

(ii) For a specific function $f$ (e.g., $f = \mathrm{CLIQUE}(m, s)$) he defines an appropriate lattice $K$ and shows that $\varrho(f, K)$ is large.

Our improved bounds are obtained by choosing different lattices in the second step, which are modified versions of Razborov's lattices.

Very recently, Andreev [2] has obtained exponential lower bounds for the monotone circuit complexity of several problems in NP. His methods are different, though very similar, to those of Razborov. The best lower bound obtained by Andreev for a function of $n$ variables in NP is $\exp(\Omega(n^{1/8-\varepsilon}))$, whereas our best bound mentioned above is $\exp(\Omega(n^{1/6-\varepsilon}))$. We also note that the methods of [2] do not seem to supply good lower bounds for CLIQUE$(m, s)$ for fixed $s$. Applying Razborov's methods together with our ideas to one of the functions $g$ of $n$ variables considered by Andreev, we can improve Andreev's lower bound and show that $L^+(g)=\exp(\Omega(n^{1/4}\cdot(\log n)^{1/2}))$.

The paper is organized as follows. In Section 2 we describe the relatively easy step (i) mentioned above, including Razborov's proof of inequality (1.2). In Section 3 we obtain, using an appropriate lattice, exponential lower bounds for the monotone complexity of the clique function. In Section 4 we obtain the $\exp(\Omega(n^{1/4}\cdot\cdot(\log n)^{1/2}))$ for Andreev's function $g$. Section 5 contains lower bounds for the monotone complexity of some other Boolean functions.

Throughout this paper, the function $\log x$ denotes logarithm base 2 of $x$, whereas $\ln x$ denotes logarithm base $e$ of $x$.

## 2. Monotone complexity and lattices

For $n\geqq 1$, let $B_n$ denote the $n$-dimensional cube $\{0, 1\}^n$. Let $P(B_n)$ denote the power set of $B_n$. The power set $P(B_n)$ is a lattice with respect to union and intersection. Let $\mathscr{L}\subseteq P(B_n)$ be the sublattice of $P(B_n)$ consisting of all monotone families of vectors in $B_n$, i.e., $\mathscr{L}$ is the set of all $F\subseteq B_n$ such that

$$\forall u\in F\,\forall v\in B_n[u \leqq v \Rightarrow v\in F].$$

For a monotone function $f$ of $n$ Boolean variables, put $A(f)=\{v\in B_n:f(v)=1\}$. Clearly if $f$ is a monotone function, then $A(f)\in\mathscr{L}$, and if $f$ and $g$ are monotone functions, then $A(f\vee g)=A(f)\cup A(g)$ and $A(f\wedge g)=A(f)\cap A(g)$.

A subposet $K$ of $\mathscr{L}$ is a *legitimate lattice* if

(i) it is a lattice (i.e. every pair $M, N\in K$ has a *join*, denoted by $M\sqcup N$, and a *meet*, denoted by $M\sqcap N$), and

(ii) $A(x_1), A(x_2), \ldots, A(x_n), A(0)(=\emptyset), A(1)(=B_n)\in K$.

For $M, N\in K$, define $\delta_\sqcup(M, N)=(M\sqcup N)-(M\cup N)$ and $\delta_\sqcap(M, N)= =(M\cap N)-(M\sqcap N)$.

For a monotone function $f$ and a lattice $K$, the *distance* from $f$ to $K$ is the minimum $t$ such that there are $M, M_1, N_1, \ldots, M_t, N_t\in K$ satisfying

$$M\subseteq A(f)\cup\bigcup_{i=1}^{t}\delta_\sqcup(M_i, N_i) \tag{2.1}$$

and

$$A(f)\subseteq M\cup\bigcup_{i=1}^{t}\delta_\sqcap(M_i, N_i). \tag{2.2}$$

Denote this distance by $\varrho(f, K)$.

**Theorem 2.1** ([12]). *For every monotone function $f$ and every legitimate lattice $K$, we have $L^+(f) \geqq \varrho(f, K)$.*

**Proof.** Put $t = L^+(f)$ and consider a monotone straight-line program $P$ for computing $f$ using $t$ operations (each of which is either an $\vee$ or an $\wedge$). Let $f_i$ and $g_i$ be the operands of the $i$th operation, for $1 \leqq i \leqq t$.

Let $M$ be the element of $K$ obtained by running the program $P$ in $K$, replacing each $\vee$ by $\sqcup$, each $\wedge$ by $\sqcap$, each $x_i$ by $A(x_i)$, each 0 by $A(0)$, and each 1 by $A(1)$. Similarly, let $M_i$ and $N_i$ be those elements of $K$ obtained by running the parts of $P$ for computing $f_i$ and $g_i$, respectively, in $K$. We prove, by induction on $t$, that (2.1) and (2.2) hold. For $t=0$, $f$ is either $x_i$ or 0 or 1, and $M = A(f)$ so the result is trivial. Assuming the result for $t-1$, we prove it for $t$. Suppose, for example, that $f = f_t \vee g_t$. By the induction hypothesis,

$$M_t \subseteqq A(f_t) \cup \bigcup_{i=1}^{t-1} \delta_{\sqcup}(M_i, N_i)$$

and

$$N_t \subseteqq A(g_t) \cup \bigcup_{i=1}^{t-1} \delta_{\sqcup}(M_i, N_i).$$

Therefore

$$\begin{aligned} M &= M_t \sqcup N_t = M_t \cup N_t \cup \delta_{\sqcup}(M_t, N_t) \\ &\subseteqq A(f_t) \cup A(g_t) \cup \bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i) \\ &= A(f) \cup \bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i), \end{aligned}$$

which is (2.1).

Equation (2.2) is even easier to prove in this case. By the induction hypothesis

$$A(f_t) \subseteqq M_t \cup \bigcup_{i=1}^{t-1} \delta_{\sqcap}(M_i, N_i)$$

and

$$A(g_t) \subseteqq N_t \cup \bigcup_{i=1}^{t-1} \delta_{\sqcap}(M_i, N_i).$$

Thus

$$\begin{aligned} A(f) = A(f_t) \cup A(g_t) &\subseteqq M_t \cup N_t \cup \bigcup_{i=1}^{t-1} \delta_{\sqcap}(M_i, N_i) \\ &\subseteqq (M_t \sqcup N_t) \cup \bigcup_{i=1}^{t-1} \delta_{\sqcap}(M_i, N_i) \subseteqq M \cup \bigcup_{i=1}^{t} \delta_{\sqcap}(M_i, N_i), \end{aligned}$$

which is (2.2).

The case $f = f_t \wedge g_t$ is proved similarly, so the proof is complete. (Notice that, the proof actually implies a slightly stronger result, namely:

$$M \subseteqq A(f) \cup \bigcup \{\delta_{\sqcup}(M_i, N_i)\colon 1 \leqq i \leqq t, \quad \text{the } i\text{th operation is an } \vee\},$$

and

$$A(f) \subseteqq M \cup \bigcup \{\delta_{\sqcap}(M_i, N_i)\colon 1 \leqq i \leqq t, \quad \text{the } i\text{th operation is an } \wedge\}. \blacksquare$$

## 3. The clique problem

### 3.1. The lattice

In this section we define a legitimate lattice $K$ such that $\varrho(\text{CLIQUE}(m, s), K)$ is large. This will supply, by Theorem 2.1, lower bounds for the monotone circuit complexity of CLIQUE$(m, s)$. As mentioned above, our lattice is only a modification of the lattice given in [12]. Throughout this section, we always assume that $m$ is large enough (e.g., assuming $m \geqq 1000$ is sufficient for all our purposes).

Let $l \geqq 2$ and $r$ be numbers to be chosen later. For not necessarily distinct sets $W, W_1, W_2, \ldots, W_r$, we say that $W_1, W_2, \ldots, W_r$ *imply* $W$ (and write $W_1, W_2, \ldots \ldots, W_r \vdash W$) iff

(i) The sets $W, W_1, W_2, \ldots, W_r$ all have cardinality at most $l$, and

(ii) $W_i \cap W_j \subseteqq W$ for all $1 \leqq i < j \leqq r$.

Notice that if $W_1 \subseteqq W$ and $|W| \leqq l$, then $r$ copies of $W_1$ imply $W$. If $A$ is a collection of sets and $W$ is a set, we say that $A$ implies $W$ (and write $A \vdash W$) iff there exist $W_1, W_2, \ldots, W_r \in A$ that imply $W$. A collection $A$ is *closed* iff $\forall W[A \vdash W \Rightarrow \Rightarrow W \in A]$. The *closure* of a collection $A$, denoted by $A^*$, is given by $A^* = \bigcap\{B : A \subseteqq \subseteqq B$ and $B$ is closed$\}$. One can easily check that $*$ is a closure relation (i.e., $A \subseteqq A^*$, $A \subseteqq B$ implies $A^* \subseteqq B^*$, and $(A^*)^* = A^*$).

For a technical reason, it is convenient to assume, in this section only (and not in Section 4), that if $A$ is a closed set having a member of cardinality 1, then it also has the empty set as a member. Thus in this section we agree that $A \vdash \emptyset$ if there is a set $W \in A$ such that $|W| = 1$.

Put $V = \{1, 2, \ldots, m\}$. Our $n = \binom{m}{2}$ Boolean variables $x_1, x_2, \ldots, x_n$ correspond to the edges of a graph on $V$. For a collection $A$ of subsets of $V$, let $[A]$ denote the family of all graphs on $V$ that contain a clique on some $W \in A$. Each such graph is represented by a characteristic vector on the set of $n$ possible edges, i.e., by an element of $B_n$. Thus $[A]$ is an element of the lattice $\mathscr{L}$, defined in Section 2. Set $\mathscr{V}(l) = \{W \subseteqq V : |W| \leqq l\}$. Finally define $K(m, r, l) = \{[A] : A$ is a closed subset of $\mathscr{V}(l)\}$.

The following lemma asserts that $K(m, r, l)$ is a legitimate lattice. We omit its straightforward proof.

**Lemma 3.1.** *$K$ is a legitimate lattice in which the join $\sqcup$ and the meet $\sqcap$ are given by $[A] \sqcup [B] = [(A \cup B)^*]$ and $[A] \sqcap [B] = [A \cap B]$.* ∎

### 3.2. Some combinatorial lemmas

Let $\mathscr{F}$ be a family of sets. We say that $\mathscr{F}$ has property $P(r, k)$ if

(i) every set $W \in \mathscr{F}$ has cardinality at most $k$, and

(ii) there are no (not necessarily distinct) $W, W_1, W_2, \ldots, W_r \in \mathscr{F}$ and $U \subsetneqq W$ such that $W_i \cap W_j \subseteqq U$ for all $1 \leqq i < j \leqq r$ (i.e., $\mathscr{F} \vdash U$).

Let $h(r, k)$ denote the maximum possible cardinality of a family $\mathscr{F}$ that has property $P(r, k)$.

**Lemma 3.2.** *For all* $r\geqq 2$ *and* $k\geqq 0$, *we have* $h(r, k)=(r-1)^k$.

**Proof.** We first show that $h(r, k)\geqq(r-1)^k$. Let $S_1, S_2, \dots, S_k$ be $k$ pairwise disjoint sets, each of cardinality $r-1$. Define $\mathscr{F}=\{W\subseteq\bigcup_{i=1}^{k} S_i\colon \forall i|W\cap S_i|=1\}$. Clearly $|\mathscr{F}|=(r-1)^k$. One can easily check that $\mathscr{F}$ has property $P(r, k)$. Indeed if $W, W_1, W_2, \dots, W_r\in\mathscr{F}$ and $U\subsetneqq W$, then $U\cap S_i=\emptyset$ for some $i$ with $1\leqq i\leqq k$. But since $|S_i|=r-1$, there are, by the pigeonhole principle, some $1\leqq p<q\leqq r$ such that $W_p\cap W_q\cap S_i\neq\emptyset$. But this means that $W_p\cap W_q\nsubseteq U$, so $\mathscr{F}$ has property $P(r, k)$.

We next prove that $h(r, k)\leqq(r-1)^k$ by induction on $r$. For $r=2$, the result is trivial; for if $\mathscr{F}$ contains two sets $W_1$ and $W_2$, define $U=W_1\cap W_2$. Either $U\subsetneqq W_1$ (and then take $W=W_1$) or $U\subsetneqq W_2$ (and then $W=W_2$), so $\mathscr{F}$ does not have property $P(r, k)$.

Assuming the result for $r-1$, we prove it for $r$. Let $\mathscr{F}$ be a family of sets having property $P(r, k)$. We must show that $|\mathscr{F}|\leqq(r-1)^k$. Suppose $D\in\mathscr{F}$. For each $C\subseteq D$, put

$$\mathscr{F}_C=\{W-C\colon W\in\mathscr{F} \text{ and } W\cap D=C\}.$$

We claim that $\mathscr{F}_C$ has property $P(r-1, k-|C|)$. Indeed, suppose $W', W_1', W_2', \dots$ $\dots, W_{r-1}'\in\mathscr{F}_C$ and $U'\subsetneqq W'$ satisfy $W_i'\cap W_j'\subseteq U'$ for all $1\leqq i<j\leqq r-1$. Let $W=W'\cup C$ and $U=U'\cup C\subsetneqq W$. Define $W_i=W_i'\cup C$ (for $1\leqq i\leqq r-1$) and $W_r=D$. This system satisfies $W_i\cap W_j\subseteq U$ for all $1\leqq i<j\leqq r$, contradicting the fact that $\mathscr{F}$ has property $P(r, k)$. Thus $\mathscr{F}_C$ has property $P(r-1, k-|C|)$. The induction hypothesis says that $|\mathscr{F}_C|\leqq(r-2)^{k-|C|}$, hence

$$\begin{aligned}|\mathscr{F}| &= \sum_{C\subseteq D}|\mathscr{F}_C| \leqq \sum_{C\subseteq D}(r-2)^{k-|C|}\\ &= \sum_{i=0}^{|D|}\binom{|D|}{i}(r-2)^{k-i} \leqq \sum_{i=0}^{k}\binom{k}{i}(r-2)^{k-i}\\ &= (r-1)^k.\end{aligned}$$

This completes the proof. ∎

**Corollary 3.3.** *Let $A$ be a closed set. Then for all $k\leqq l$ there are at most $(r-1)^k$ minimal elements (with respect to containment) of $A$ of cardinality at most $k$.*

**Proof.** Let $\mathscr{F}$ be the family of minimal elements of $A$ of cardinality at most $k$. Clearly $\mathscr{F}$ has property $P(r, k)$. Indeed if $W, W_1, W_2, \dots, W_r\in\mathscr{F}$ and $U\subsetneqq W$ satisfy $W_i\cap W_j\subseteq U$ for all $1\leqq i<j\leqq r$, then $W_1, W_2, \dots, W_r\vdash U$. Thus $U\in A$ since $A$ is closed. But $U\in A$ contradicts the minimality of $W$, so $\mathscr{F}$ must have property $P(r, k)$. The result now follows from Lemma 3.2. (The construction given in the proof of Lemma 3.2 can be used to show that Corollary 3.3 is best possible.) ∎

We now show that for every collection of sets $C$, the closure $C^*$ can be constructed from $C$ using a reasonably small number of operations. For a collection $C$, put $C'=\{W\notin C\colon C\vdash W\}$. Notice that $C'=\emptyset$ iff $C=C^*$, but that in general $C'$

need not equal $C^*-C$. Consider the following algorithm for going from $C$ to $C^*$:

```
algorithm Closure ($C$)
  $C_0 \leftarrow C$
  $i \leftarrow 0$
  while $C_i$ not closed do
    $W_{i+1} \leftarrow$ any minimal element of $C_i'$
    $C_{i+1} \leftarrow C_i \cup \{W\colon W_{i+1} \subseteq W$ and $|W| \leq l\}$
    $i \leftarrow i+1$
  end while
  output $C_i$
end algorithm
```

Clearly, since everything is finite, the above closure algorithm must terminate and produce $C^*$. In fact, for the lattice of subsection 3.1, since each $W_i$ is distinct, the number of iterations is bounded by $|\mathscr{V}(l)| = \sum_{k=0}^{l} \binom{m}{k} \leq m^l$. Below we give a more complicated argument (Lemma 3.5) which improves this bound. Although the weaker bound is sufficient for all our purposes, the stronger bound may be useful sometimes.

A family of $t$ sets $W_1, W_2, \ldots, W_t$ is called a *sunflower* with *center* $W$ and $t$ *petals* $W_1, W_2, \ldots, W_t$ if $W_i \cap W_j = W$ for all $1 \leq i < j \leq t$. The following result was proved by Erdős and Rado.

**Lemma 3.4.** ([6]). *Let $\mathscr{F}$ be a family of sets, each of cardinality at most $l$. If $|\mathscr{F}| > l!(t-1)^l$, then $\mathscr{F}$ contains a sunflower with $t$ petals.* ▮

Using the Erdős—Rado result, it is not too difficult to show that for every collection $C$, the closure algorithm terminates after at most $l!(r+1)^l$ iterations, since the system $\{W_1, W_2, \ldots, W_p\}$ defined in the algorithm cannot contain a sunflower with $r+2$ petals. We can in fact improve this bound using similar arguments to those used in the proof of Lemma 3.2.

**Lemma 3.5.** *For every collection $C$, the closure algorithm terminates after at most $2r^l$ iterations.*

**Proof.** Let $S = (W_1, W_2, \ldots, W_p)$ be a sequence of distinct sets. We say that $S$ has property $T(r, l)$ if

(i) every set $W_i$ has cardinality at most $l$, and

(ii) there are no $i_1 \leq i_2 \leq \ldots \leq i_r < i_{r+1}$ and $U \subsetneqq W_{i_{r+1}}$ such that $W_{i_j} \cap W_{i_k} \subseteq U$ for all $1 \leq j < k \leq r$ (i.e., $W_{i_1}, W_{i_2}, \ldots, W_{i_r} \vdash U$).

Notice that if $S = (W_1, W_2, \ldots, W_p)$ is the sequence of $W_i$'s produced by our algorithm for obtaining $C^*$ from $C$, then $S$ has property $T(r, l)$, since otherwise we get a contradiction to the minimality of $W_{i_{r+1}}$ when it was added. Therefore, to prove Lemma 3.5, it suffices to prove:

**Claim:** *Suppose $r \geq 1$ and $l \geq 0$. If $S = (W_1, W_2, \ldots, W_p)$ has property $T(r, l)$, then $p \leq 2r^l$.*

**Proof of Claim.** By induction on $r$. Consider first the case $r=1$. Suppose that $S$ has property $T(1, l)$ and $p > 2$. Notice that $W_1 \vdash \emptyset$, since $r=1$ makes $\vdash$ trivial.

Since the $W_i$ are distinct, either $W_2$ or $W_3$ is nonempty. But if $W_2\neq\emptyset$, then $W_1\vdash\emptyset\subsetneqq W_2$, contradicting the assumption that $S$ has property $T(1, l)$. Similarly $W_3\neq\emptyset$ contradicts $S$ having property $T(1, l)$. This proves the claim for $r=1$.

Assuming the result for $r-1$, we prove it for $r$. Suppose $S=(W_1, W_2, \dots, W_p)$ has property $T(r, l)$. Put $D=W_1$. For each $C\subseteq D$, let $S_C$ be the sequence of all sets $W_i-C$ such that $W_i\cap D=C$, appearing in the same order that the $W_i$ appear in $S$. As in the proof of Lemma 3.2, it is easy to check that $S_C$ has property $T(r-1, l-|C|)$. By the induction hypothesis $|S_C|\leqq 2(r-1)^{l-|C|}$, and thus

$$|S| = \sum_{C\subseteq D} |S_C| \leqq 2\sum_{i=0}^{|D|}\binom{|D|}{i}(r-1)^{l-i} \leqq 2r^l.$$

This completes the proof. ▮

We conclude this subsection with two probabilistic lemmas. Recall from Section 3.1 that $V=\{1, 2, \dots, m\}$. By a random $g$-coloring $O$ of $V$, we mean a random choice of one of the $g^m$ possible colorings of $V$ using the colors $\{1, 2, \dots, g\}$, where each such choice is equally likely. We say that $W\subseteq V$ is *properly colored* (PC for short) by $O$ if each vertex of $W$ has a different color.

**Lemma 3.6.** *Suppose that $A\subseteq\mathcal{V}(l)$ and $A\vdash W$. Let $O$ be a random g-coloring of V. Then*

$$\Pr[W \textit{ is PC by } O \textit{ and no set in } A \textit{ is PC by } O] \leqq \left(1-\frac{g(g-1)\dots(g-l+1)}{g^l}\right)^r.$$

**Proof.** $A\vdash W$ means that there are $W_1, W_2, \dots, W_r\in A$ such that $W_1, W_2, \dots, W_r\vdash W$. We have

$$\begin{aligned}\Pr[W \text{ is } PC \text{ and no set in } A \text{ is } PC] &\leqq \\ &\leqq \Pr[W \text{ is } PC \text{ and } W_1, W_2, \dots, W_r \text{ are not } PC] \\ &\leqq \Pr[W_1, W_2, \dots, W_r \text{ are not } PC|W \text{ is } PC] \\ &= \prod_{i=1}^{r}\Pr[W_i \text{ is not } PC|W \text{ is } PC],\end{aligned}$$

where the last equality holds since, by the definition of the implication $W_1, W_2, \dots, W_r\vdash W$, the events $\{W_i$ is not $PC|W$ is $PC\}$ are mutually independent. Let $p_i=|W_i\cap W|$ and $q_i=|W_i-W|$. Clearly $p_i+q_i=|W|\leqq l$, so

$$\begin{aligned}\Pr[W_i \text{ is not } PC|W \text{ is } PC] &= 1-\Pr[W_i \text{ is } PC\ |W \text{ is } PC] \\ &= 1-\frac{(g-p_i)(g-p_i-1)\dots(g-p_i-q_i+1)}{g^{q_i}} \\ &\leqq 1-\frac{(g-p_i)(g-p_i-1)\dots(g-l+1)}{g^{l-p_i}} \\ &\leqq 1-\frac{g(g-1)\dots(g-l+1)}{g^l}.\end{aligned}$$

This completes the proof. ▮

For a $g$-coloring $O$ of $V$, let $G(O)$ denote the complete $g$-partite graph on $V$ whose edges are all pairs $\{i, j\}$ with $O(i) \neq O(j)$.

**Lemma 3.7.** *Suppose $C \subseteq \mathscr{V}(l)$, and let $O$ be a random $g$-coloring of $V$. Then*

$$\Pr\,[G(O) \in [C^*] - [C]] \leqq (2r^l)\left(1 - \frac{g(g-1)\dots(g-l+1)}{g^l}\right)^r.$$

**Proof.** Consider the closure algorithm for obtaining $C^*$ from $C$, defined just before Lemma 3.5. By Lemma 3.5, the algorithm must halt after $p \leqq 2r^l$ iterations. Now $G(O) \in [C^*] - [C]$ means that some set in $C^*$ is PC by $O$ but no set in $C$ is PC by $O$. This is equivalent to: some $W_i$ of the algorithm (for $1 \leqq i \leqq p$) is PC but not set in $C$ is PC. This in turn is equivalent to the disjoint union of the $p$ events (for $1 \leqq i \leqq p$)

$$E_i \equiv W_i \text{ is PC and no set in } C \cup \{W_1, W_2, \dots, W_{i-1}\} \text{ is PC.}$$

The definition of the algorithm implies that $C \cup \{W_1, W_2, \dots, W_{i-1}\} \vdash W_i$, so by Lemma 3.6, we have

$$\Pr\,[E_i] \leqq \left(1 - \frac{g(g-1)\dots(g-l+1)}{g^l}\right)^r.$$

Hence

$$\begin{aligned} \Pr\,[G(O) \in [C^*] - [C]] &= \sum_{i=1}^{p} \Pr\,[E_i] \\ &\leqq p\left(1 - \frac{g(g-1)\dots(g-l+1)}{g^l}\right)^r, \\ &\leqq 2r^l\left(1 - \frac{g(g-1)\dots(g-l+1)}{g^l}\right)^r, \end{aligned}$$

as required. ∎

### 3.3. The exponential lower bound

Recall that CLIQUE$(m, s)$ is the function of $n = \binom{m}{2}$ Boolean variables, representing the edges of a graph on $V = \{1, 2, \dots, m\}$, whose value is 1 iff $G$ contains an $s$-clique.

**Lemma 3.8.** *Suppose $3 \leqq s \leqq \frac{1}{4}(m/\log m)^{2/3}$, and let $l = \lceil \sqrt{s} \rceil$ and $r = \lceil 4\sqrt{s} \log m \rceil$. Then the distance from $f =$* CLIQUE$(m, s)$ to the lattice $K = K(m, r, l)$ satisfies

$$\varrho(f, K) \geqq \frac{1}{8}\left(\frac{m}{s(r-1)}\right)^{\lceil (l+1)/2 \rceil} \geqq \frac{1}{8}\left(\frac{m}{4s^{3/2}\log m}\right)^{(\sqrt{s}+1)/2}.$$

**Proof.** Let $t = \varrho(f, K)$. We must show that

$$t \geqq \frac{1}{8}\left(\frac{m}{s(r-1)}\right)^{\lceil (l+1)/2 \rceil}. \tag{3.1}$$

By the definition of $\varrho(f, K)$, there are $M, M_1, N_1, \ldots, M_t, N_t \in K$ such that (2.1) and (2.2) both hold. Put $M = \lceil A \rceil$, where $A$ is a closed subset of $\mathcal{V}(l)$. We consider two possible cases.

**Case 1.** *$M$ is not the set of all graphs.*

Notice that by (2.2), each $s$-clique must belong to $M \cup \bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i)$. To prove (3.1), it is clearly enough to prove the following two claims:

**Claim 1.** *$M$ contains at most one-half of the $\binom{m}{s}$ possible $s$-cliques.*

**Claim 2.** *Each $\delta_{\sqcap}(M_i, N_i)$ contains at most $4 \cdot (s(r-1)/m)^{\lceil (l+1)/2 \rceil} \cdot \binom{m}{s}$ of the $s$-cliques.*

**Proof of Claim 1.** Notice that since $M$ is not the set of all graphs, each element of $A$ has cardinality at least 2. Each $s$-clique that belongs to $M$ contains some minimal element of $A$. By Corollary 3.3, for each $2 \leqq k \leqq l$, the number of minimal elements of cardinality $k$ of $A$ is at most $(r-1)^k$. Each such element is contained in precisely $\binom{m-k}{s-k}$ of the $s$-cliques. Thus the total number of $s$-cliques that belong to $M$ is at most

$$\sum_{k=2}^{l} (r-1)^k \binom{m-k}{s-k} \leqq \sum_{k=2}^{l} (r-1)^k \binom{m}{s} \left(\frac{s}{m}\right)^k$$
$$= \binom{m}{s} \sum_{k=2}^{l} \left(\frac{s(r-1)}{m}\right)^k$$
$$\leqq \binom{m}{s} \sum_{k=2}^{l} \left(\frac{1}{2}\right)^k$$
$$< \frac{1}{2}\binom{m}{s}. \blacksquare$$

**Proof of Claim 2.** Put $M_i = \lceil A_i \rceil$ and $N_i = \lceil B_i \rceil$, where $A_i$ and $B_i$ are closed subsets of $\mathcal{V}(l)$. By Lemma 3.1,

$$\delta_{\sqcap}(M_i, N_i) = (M_i \cap N_i) - (M_i \sqcap N_i) = \lceil A_i \rceil \cap \lceil B_i \rceil - \lceil A_i \cap B_i \rceil.$$

Thus if an $s$-clique on a set $Z$ of vertices belongs to $\delta_{\sqcap}(M_i, N_i)$, then $Z$ contains a minimal element $X \in A_i$ and a minimal element $Y \in B_i$, but no element of $A_i \cap B_i$. If $|X \cup Y| \leqq l$, then, since $A_i$ and $B_i$ are closed, the set $X \cup Y \subseteqq Z$ is an element of $A_i \cap B_i$, which is impossible. Thus $|X \cup Y| > l$, so either $X$ or $Y$ (or both) have cardinality at least $\lceil (l+1)/2 \rceil$. We therefore conclude that each $s$-clique belonging to $\delta_{\sqcap}(M_i, N_i)$ contains a minimal element of cardinality $k \geqq \lceil (l+1)/2 \rceil$ of either $A_i$ or $B_i$ (or both). By Corollary 3.3, the number of such elements is at most $2(r-1)^k$, each of which is contained in $\binom{m-k}{s-k}$ of the $s$-cliques. Hence the total number of

$s$-cliques that belong to $\delta_{\sqcap}(M_i, N_i)$ is at most

$$\sum_{k=\lceil (l+1)/2\rceil}^{l} 2(r-1)^k \binom{m-k}{s-k} \leqq 2\binom{m}{s} \sum_{k=\lceil (l+1)/2\rceil}^{l} \left(\frac{s(r-1)}{m}\right)^k$$
$$< 2\binom{m}{s}\left(\frac{s(r-1)}{m}\right)^{\lceil (l+1)/2\rceil} \sum_{i=0}^{\infty}\left(\frac{1}{2}\right)^i$$
$$= 4\left(\frac{s(r-1)}{m}\right)^{\lceil (l+1)/2\rceil}\binom{m}{s}.$$

This completes the proof of Claim 2, and thus the proof of Case 1. ▮

**Case 2.** *M is the set of all graphs.*

In this case, by (2.1), every $(s-1)$-partite graph on $V$ belongs to $\bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i)$, since these graphs do not contain any $s$-cliques. Put $M_i=\lceil A_i\rceil$ and $N_i=\lceil B_i\rceil$, where $A_i$ and $B_i$ are closed subsets of $\mathcal{V}(l)$. By Lemma 3.1,

$$\delta_{\sqcup}(M_i, N_i) = (M_i \sqcup N_i) - (M_i \cup N_i) = \lceil (A_i \cup B_i)^* \rceil - (\lceil A_i \rceil \cup \lceil B_i \rceil)$$
$$= \lceil (A_i \cup B_i)^* \rceil - \lceil A_i \cup B_i \rceil = \lceil C_i^* \rceil - \lceil C_i \rceil,$$

where $C_i = A_i \cup B_i$ for $1 \leqq i \leqq t$. Suppose that $t$ violates (3.1), i.e., suppose

$$t < \frac{1}{8}\left(\frac{m}{s(r-1)}\right)^{\lceil (l+1)/2\rceil} < m^{\lceil \sqrt{s}\rceil}.$$

Let $O$ be a random $(s-1)$-coloring of $V$. Then $G(O)$ (defined just before Lemma 3.7) is a complete $(s-1)$-partite graph. By Lemma 3.7, for each fixed $i$ such that $1 \leqq i \leqq t$, we have

$$\Pr\left[G(O) \in \lceil C_i^* \rceil - \lceil C_i \rceil\right] \leqq (2r^l)\left(1 - \frac{(s-1)(s-2)\dots(s-\lceil\sqrt{s}\,\rceil)}{(s-1)^{\lceil\sqrt{s}\rceil}}\right)^r$$
$$\leqq m^{\lceil\sqrt{s}\rceil}\left(\frac{2}{3}\right)^{\lceil 4\sqrt{s}\log m\rceil}$$
$$\leqq m^{\lceil\sqrt{s}\rceil} m^{-2\lceil\sqrt{s}\rceil}$$
$$= m^{-\lceil\sqrt{s}\rceil}.$$

Thus

$$\Pr\left[G(O) \in \bigcup_{i=1}^{t} (\lceil C_i^* \rceil - \lceil C_i \rceil)\right] \leqq t m^{-\lceil\sqrt{s}\rceil} < 1,$$

so there is some $G(O)$ that does not belong to $\bigcup_{i=1}^{t} (\lceil C_i^* \rceil - \lceil C_i \rceil) = \bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i)$. But this is a contradiction, since each $(s-1)$-partite graph must belong to $\bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i)$. Hence (3.1) holds, and the assertion of the lemma follows. ▮

Combining Theorem 2.1 with Lemma 3.8, we get the following theorem.

**Theorem 3.9.** *If* $3 \leqq s \leqq \frac{1}{4}(m/\log m)^{2/3}$, *then*

$$L^+(\text{CLIQUE}(m, s)) \geqq \frac{1}{8}\left(\frac{m}{4s^{3/2}\log m}\right)^{(\sqrt{s}+1)/2} \geqq \frac{1}{8}2^{(\sqrt{s}+1)/2}.$$

*In particular, for* $s = \left\lfloor \frac{1}{4}(m/\log m)^{2/3} \right\rfloor$ *the monotone circuit complexity of* CLIQUE$(m, s)$ *is* $\exp(\Omega((m/\log m)^{1/3}))$. ▮

### 3.4. Approximating the maximum clique size

Theorem 3.9 says that a monotone circuit must be large to distinguish between graphs with maximum clique size less than $s$ and graphs with maximum clique size at least $s$. In this section we show that, for $s_1 \leqq s_2$, a monotone circuit must be large to distinguish between graphs with maximum clique size less than $s_1$ and graphs with maximum clique size at least $s_2$, even for some $s_2 \gg s_1$.

For $1 \leqq s_1 \leqq s_2 \leqq m$, let $F(m, s_1, s_2)$ denote the set of all monotone functions $f$ of $\binom{m}{2}$ Boolean variables representing the edges of a graph $G$ on $V = \{1, 2, \dots, m\}$, such that the value of $f$ is 0 if $G$ contains no clique of size $s_1$, is 1 if $G$ contains a clique of size $s_2$, and is arbitrary otherwise. Notice that $F(m, s, s) = \{\text{CLIQUE}(m, s)\}$, but that for $s_1 < s_2$ we have $|F(m, s_1, s_2)| > 1$.

**Lemma 3.10.** *Suppose* $f \in F(m, s_1, s_2)$, *where* $3 \leqq s_1 \leqq s_2$ *and* $\sqrt{s_1 s_2} \leqq m/(8\log m)$. *Let* $l = \lceil \sqrt{s_1} \rceil$ *and* $r = \lceil 4\sqrt{s_1}\log m \rceil$. *Then the distance from* $f$ *to the lattice* $K = K(m, r, l)$ *satisfies*

$$\varrho(f, K) \geqq \frac{1}{8}\left(\frac{m}{s_2(r-1)}\right)^{\lceil (l+1)/2 \rceil} \geqq \frac{1}{8}\left(\frac{m}{4\sqrt{s_1 s_2}\log m}\right)^{(\sqrt{s_1}+1)/2}.$$

**Proof.** The proof is very similar to that of Lemma 3.8. Let $t = \varrho(f, K)$. We must show that

$$t \geqq \frac{1}{8}\left(\frac{m}{s_2(r-1)}\right)^{\lceil (l+1)/2 \rceil}. \tag{3.2}$$

By definition of $\varrho(f, K)$, there are $M$, $M_i$, and $N_i \in K$ (for $1 \leqq i \leqq t$) for which conditions (2.1) and (2.2) hold. Put $M = [A]$, and for $1 \leqq i \leqq t$ put $M_i = [A_i]$ and $N_i = [B_i]$, where $A$, $A_i$, and $B_i$ are closed subsets of $\mathcal{V}(l)$. We consider two possible cases.

**Case 1.** *M is not the set of all graphs.*

By (2.2), each $s_2$-clique belongs to $M \cup \bigcup_{i=1}^{t} \delta_{\sqcap}(M_i, N_i)$, so (3.2) will follow from the following two claims:

**Claim 1.** *M contains at most one-half of the* $\binom{m}{s_2}$ possible $s_2$-cliques.

**Claim 2.** *Each $\delta_\sqcap(M_i, N_i)$ contains at most $4\cdot(s_2(r-1)/m)^{\lceil (l+1)/2\rceil}\cdot\binom{m}{s_2}$ of the possible $s_2$-cliques.*

The proofs of these two claims are analogous to those given in the proof of Lemma 3.8. This completes the proof of Case 1.

**Case 2.** *$M$ is the set of all graphs.*

In this case, by (2.1), every complete $(s_1-1)$-partite graph on $V$ belongs to the set $\bigcup_{i=1}^{t}\delta_\sqcup(M_i, N_i)$. The proof that $t$ satisfies (3.2) for this case is identical to the one given in the proof of Lemma 3.8. ▮

Lemma 3.10 and Theorem 2.1 imply the following.

**Theorem 3.11.** *If $f\in F(m, s_1, s_2)$, where $3\leqq s_1\leqq s_2$ and $\sqrt{s_1}s_2\leqq m/(8\log m)$, then*

$$L^+(f)\geqq\frac{1}{8}\left(\frac{m}{4\sqrt{s_1}\,s_2\log m}\right)^{(\sqrt{s_1}+1)/2}\geqq\frac{1}{8}2^{(\sqrt{s_1}+1)/2}.\quad ▮$$

We specify a special case of the last theorem separately.

**Corollary 3.12.** *Let $f$ be a monotone function of $\binom{m}{2}$ Boolean variables representing the edges of a graph $G$ on $V=\{1, 2, \dots, m\}$, and suppose the value of $f$ is 0 if $G$ contains no clique of size $\lfloor(\log m)^4\rfloor$, is 1 if $G$ contains a clique of size $\lfloor m/(8(\log m)^3)\rfloor$, and is arbitrary otherwise. Then the monotone circuit complexity of $f$ is $m^{\Omega(\log m)}$.* ▮

### 3.5. Small cliques

For fixed $s\geqq 3$, as $m\to\infty$, Theorem 3.9 can be improved using the lattice $K(m, r, l)$ with $l=s-1$ and $r=cse^s\log m$ (for some constant $c>0$). This (with $c=2$) is precisely the lattice used by Razborov in [12] to show that for fixed $s$

$$L^+(\mathrm{CLIQUE}(m, s)) = \Omega\left(\frac{m^s}{(\log m)^{2s}}\right). \tag{3.3}$$

Notice that $L^+(\mathrm{CLIQUE}(m, s))=O(m^s)$, and thus (3.3) is not far from best possible. In this section we improve (3.3) by replacing $(\log m)^{2s}$ by $(\log m)^s$. In fact, we show that, for fixed $s\geqq 3$, every monotone circuit computing $\mathrm{CLIQUE}(m, s)$ contains $\Omega(m^s/(\log m)^s)$ AND gates.

**Lemma 3.13.** *Define $l=s-1$, and let $M$ and $N$ be two elements of the lattice $K=.$ $=K(m, r, l)$. Then the number of $s$-cliques contained in $\delta_\sqcap(M, N)$ is at most $2^s\cdot(r-1)^s$.*

**Proof.** Suppose $M=\lceil A\rceil$ and $N=\lceil B\rceil$, where $A$ and $B$ are closed subsets of $\mathcal{V}(l)$. By Lemma 3.1, we have

$$\delta_\sqcap(M, N) = (M\cap N)-(M\sqcap N) = \lceil A\rceil\cap\lceil B\rceil-\lceil A\cap B\rceil.$$

If an $s$-clique on a set of vertices $Z$ belongs to $\delta_\sqcap(M, N)$, then $Z$ must contain a minimal element $X \in A$ and a minimal element $Y \in B$, but no element of $A \cap B$. Hence $|X \cup Y| = s$, for if $|X \cup Y| \leqq s-1$, then $X \cup Y \subseteqq Z$ would be an element of $A \cap B$, which is impossible. Therefore the number of $s$-cliques in $\delta_\sqcap(M, N)$ is at most the number of pairs $(X, Y)$, where $X$ is a minimal element of $A$ and $Y$ is a minimal element of $B$ such that $|X \cup Y| = s$. Given a minimal element $X$ of $A$, define $\mathscr{F}_X = \{Y : Y$ is a minimal element of $B$ and $|X \cup Y| = s\}$. For $C \subseteqq X$, put $\mathscr{F}_{X,C} = \{Y - C : Y \in \mathscr{F}_X$ and $X \cap Y = C\}$. One can easily check that $\mathscr{F}_{X,C}$ has property $P(r, s-|X|)$, defined in the first paragraph of subsection 3.2. Indeed, if $W, W_1, W_2, \ldots, W_r \in \mathscr{F}_{X,C}$ and $U \subsetneqq W$ satisfy $W_i \cap W_j \subseteqq U$ for all $1 \leqq i < j \leqq r$, then $W_1 \cup C, W_2 \cup C, \ldots, W_r \cup C \vdash U \cup C$. But this implies that $U \cup C \in B$, contradicting the minimality of $W \cup C \in B$. Hence, Lemma 3.2 says that $|\mathscr{F}_{X,C}| \leqq (r-1)^{s-|X|}$, and thus $|\mathscr{F}_X| \leqq 2^{|X|} \cdot (r-1)^{s-|X|}$. By Corollary 3.3, the number of minimal elements $X$ of $A$ of cardinality $k$ is at most $(r-1)^k$. Thus the total number of pairs $(X, Y)$ of the required type is at most

$$\sum_{k=1}^{s-1} (r-1)^k (2^k (r-1)^{s-k}) = (r-1)^s \sum_{k=1}^{s-1} 2^k$$
$$< 2^s (r-1)^s,$$

and the proof is complete. ▮

**Lemma 3.14.** *If* $3 \leqq s \leqq \frac{1}{4} \log m$, *then every monotone circuit that computes the function* CLIQUE$(m, s)$ *contains either at least* $m^s/(8s^2 e^s \log m)^s$ AND *gates or at least* $m^{3s}$ OR *gates.*

**Proof.** Let $t_1$ and $t_2$ denote the number of AND gates and OR gates, respectively, in a monotone circuit that computes $f = \text{CLIQUE}(m, s)$. Set $K = K(m, r, l)$, where $l = s-1$ and $r = \lfloor 4se^s \log m \rfloor$. By the proof of Theorem 2.1, there are $M, M_1, N_1, \ldots, M_{t_1+t_2}, N_{t_1+t_2} \in K$ such that

$$A(f) \subseteqq M \cup \bigcup_{i=1}^{t_1} \delta_\sqcap (M_i, N_i), \tag{3.4}$$

and

$$M \subseteqq A(f) \cup \bigcup_{i=t_1+1}^{t_1+t_2} \delta_\sqcup (M_i, N_i). \tag{3.5}$$

Consider two possible cases.

**Case 1.** *M is not the set of all graphs.*

In this case one can easily check, as in the proof of Lemma 3.8, that $M$ contains at most one-half of the possible $s$-cliques. Hence, by (3.4) and Lemma 3.13, we have

$$t_1 \geqq \frac{1}{2} \binom{m}{s} \Big/ (2^s (r-1)^s) \geqq \frac{m^s}{s^s (2r)^s} \geqq \frac{m^s}{(8s^2 e^s \log m)^s},$$

and Case 1 is settled.

**Case 2.** *M is the set of all graphs.*

In this case, by (3.5), every $(s-1)$-partite graph on $V$ belongs to $\bigcup_{i=t_1+1}^{t_1+t_2} \delta_{\sqcup}(M_i, N_i)$. Put $M_i=[A_i]$ and $N_i=[B_i]$, and let $C_i=A_i\cup B_i$ for $t_1+1\leqq i\leqq t_1+t_2$. Then, as in the proof of Theorem 3.8, we have $\delta_{\sqcup}(M_i, N_i)=[C_i^*]-[C_i]$. Let $O$ be a random $(s-1)$-coloring of $V$. By Lemma 3.7, for each fixed $i$ satisfying $t_1+1\leqq$ $\leqq i\leqq t_1+t_2$, we have

$$\Pr[G(O)\in[C_i^*]-[C_i]] \leqq (2r^l)\left(1-\frac{(s-1)!}{(s-1)^{s-1}}\right)^r$$

$$\leqq m^s(1-e^{-s})^r \leqq m^{-3s}.$$

If $t_2<m^{3s}$, then $\Pr\left[G(O)\in \bigcup_{i=t_1+1}^{t_1+t_2} ([C_i^*]-[C_i])\right]\leqq t_2 m^{-3s}<1$, so some $G(O)$ does not belong to $\bigcup_{i=t_1+1}^{t_1+t_2} \delta_{\sqcup}(M_i, N_i)$. But this is impossible, since $G(O)$ is an $(s-1)$-partite graph. Thus $t_2$, the number of OR gates in the circuit, is at least $m^{3s}$, completing the proof of the lemma. ▮

The next simple lemma is interesting in its own right, showing that the number of AND gates and OR gates in a circuit can always be somewhat balanced, without increasing the complexity of the circuit. For example, exponential lower bounds on monotone circuit complexity imply exponential lower bounds on both the number of AND gates and the number of OR gates required.

**Lemma 3.15.** *Let $f$ be a monotone function of $n$ Boolean variables, and suppose there is a monotone circuit computing $f$ that contains $k$ AND gates. Then there is a monotone circuit computing $f$ that contains $k$ AND gates and at most $(k+1)(n-1)+\binom{k+1}{2}$ OR gates (the dual version of the statement holds as well).*

**Proof.** Consider a monotone straight-line program for computing $f$, and let $f_1, f_2, \ldots$ $\ldots, f_k$ be the $k$ outputs of the $k$ AND gates, in the order in which they are computed. We first prove, by induction on $i$, that there is a monotone circuit that computes $f_1, f_2, \ldots, f_i$ containing $i$ AND gates and at most $i(n-1)+\binom{i}{2}$ OR gates. For $i=1$, $f_1$ is an AND of two operands, each of which is either a constant or an OR of a subset of $\{x_1, x_2, \ldots, x_n\}$. One can easily check that these two operands can be computed with at most $n-1$ OR gates, so the case $i=1$ is settled. Assuming the result for $i-1$, let us prove it for $i$. The functions $f_1, f_2, \ldots, f_{i-1}$ can be computed, by the induction hypothesis, using $i-1$ AND gates and at most $(i-1)(n-1)+\binom{i-1}{2}$ OR gates. The function $f_i$ is an AND of two operands, each of which is either a constant or an OR of a subset of $\{x_1, x_2, \ldots, x_n\}\cup\{f_1, f_2, \ldots, f_{i-1}\}$. These two operands can be computed with at most $n+i-2$ OR gates, and since $(i-1)(n-1)+\binom{i-1}{2}$ $+n+i-2=i\cdot(n-1)+\binom{i}{2}$, the induction step is completed.

Therefore $f_1, f_2, \ldots, f_k$ can be computed with a monotone circuit containing $k$ AND gates and at most $k(n-1)+\binom{k}{2}$ OR gates. The function $f$ itself is either a constant or an OR of a subset of $\{x_1, x_2, \ldots, x_n\} \cup \{f_1, f_2, \ldots, f_k\}$ which can be computed with at most $n+k-1$ additional OR gates. The desired result follows. ▮

A *quadratic function* is a function $f$ on $n \geqq 2$ variables of the form

$$f(x) = \bigvee_{1 \leqq i < j \leqq n} (a_{ij} \wedge x_i \wedge x_j),$$

where the $a_{ij}$ are either 0 or 1. Bloniarz [3] shows that most quadratic functions $f$ satisfy $L^+(f) = \Omega(n^2/\log n)$. Bloniarz also observes that all quadratic functions have monotone circuits with only $n-1$ AND gates. Thus this example shows that Lemma 3.15 is tight up to a logarithmic factor.

The next theorem provides almost optimal lower bounds on the number of AND gates for CLIQUE$(m, s)$, when $s$ is fixed.

**Theorem 3.16.** *If* $3 \leqq s \leqq \frac{1}{4} \log m$, *then every monotone circuit that computes the function* CLIQUE$(m, s)$ *contains at least* $m^s/(8s^2e^s \log m)^s$ AND *gates. In particular, for each fixed* $s \geqq 3$, *the number of* AND *gates in any monotone circuit that computes* CLIQUE$(m, s)$ *is* $\Omega(m^s/(\log m)^s)$.

**Proof.** Suppose this is false, i.e., suppose there is a monotone circuit computing the function CLIQUE$(m, s)$ that contains $k < m^s/(8s^2e^s \log m)^s$ AND gates. Then by Lemma 3.15, there is also a monotone circuit computing CLIQUE$(m, s)$ that contains $k$ AND gates and at most $(k+1)\cdot\left(\binom{m}{2}-1\right)+\binom{k+1}{2} < m^{3s}$ OR gates. This contradicts Lemma 3.14, so our assumption was false and the theorem is proved. ▮

It is worth noting that, as is well known ([5], [9]), the nonmonotone circuit complexity of CLIQUE$(m, s)$ is $O\left(M\left(\binom{m}{\lceil s/3 \rceil}\right)\right) = O(m^{2.5 \lceil s/3 \rceil})$, where $M(t)$ is the nonmonotone circuit complexity of Boolean matrix multiplication. Since it is easy to check whether or not a graph $G$ contains a triangle by squaring its adjacency matrix, the last theorem implies that any monotone circuit that computes the Boolean square of an $m$ by $m$ matrix contains $\Omega(m^3/(\log m)^3)$ AND gates. Better results about the monotone complexity of matrix multiplication appear in [8], [10], and [11].

## 4. A better lower bound for an NP problem

In this section we consider a problem in NP for which we obtain our largest lower bound. Andreev [2] had previously given weaker bounds for this problem.

Let GF$(q)$ denote the finite field with $q$ elements, where $q$ is a prime power. Let $G = (U, V, E)$ be a bipartite graph with $U = \text{GF}(q)$ and $V = \text{GF}(q)$. Define POLY$(q, s)$ to be the function of $n = q^2$ Boolean variables representing the edges of $G$, whose value is 1 iff there is a polynomial $p$ over GF$(q)$ of degree at most $s-1$ such that $\forall i \in U[(i, p(i)) \in E]$. The family of functions $\{\text{POLY}(q, s)\}$ is clearly in NP. Andreev [2] showed that for $s \leqq (1/2)n^{1/8}/\sqrt{\ln n} - 1$, the monotone complexity of POLY$(q, s)$ satisfies

$$L^+(\mathrm{POLY}(q, s)) \geqq \left(\frac{n^{1/2}}{4(s-1)^4(\ln n)^2}\right)^s,$$

so that for $s=(1/2)n^{1/8}/\sqrt{\ln n}-1$ Andreev obtains

$$L^+(\mathrm{POLY}(q, s)) = \exp\left(\Omega\left(n^{1/8}/\sqrt{\ln n}\right)\right).$$

In this section we show that for $s\leqq(1/2)\sqrt{q/\ln q}$,

$$L^+(\mathrm{POLY}(q, s)) = q^{\Omega(s)},$$

so that for $s=(1/2)\sqrt{q/\ln q}$ we have

$$L^+(\mathrm{POLY}(q, s)) = \exp\left(\Omega\left(\sqrt{q \ln q}\right)\right) = \exp\left(\Omega\left(n^{1/4}\sqrt{\ln n}\right)\right).$$

For fixed $s$ we can show that every monotone circuit computing POLY$(q, s)$ has $\Omega(q^s)$ AND gates.

Although Andreev's results were proved without using the lattice framework, we get better results by defining an appropriate lattice following Razborov's method. Our treatment here is analogous to the one given in Section 3.

### 4.1. The polynomial lattice

Recall that $U=\mathrm{GF}(q)$ and $V=\mathrm{GF}(q)$. Let $l\geqq 1$ and $r$ be parameters to be chosen later. We use the same definition of closed sets as that of section 3.1 (except for the technicality mentioned there). Given a collection $A$ of subsets of $U\times V$, define $\lceil A\rceil$ by $\lceil A\rceil=\{G=(U, V, E)\colon E$ contains some $F\in A\}$. Let $\mathscr{E}(l)=$ $=\{F\subseteqq U\times V\colon |F|\leqq l\}$. Define the lattice $K(q, r, l)$ by $K(q, r, l)=\{\lceil A\rceil\colon A$ is a closed subset of $\mathscr{E}(l)\}$. The following claim is straightforward to verify.

**Lemma 4.1.** *$K(q, r, l)$ is a legitimate lattice with lattice operations $\sqcup$ and $\sqcap$ given by $\lceil A\rceil\sqcup\lceil B\rceil=\lceil(A\cup B)^*\rceil$ and $\lceil A\rceil\sqcap\lceil B\rceil=\lceil A\cap B\rceil$.*

### 4.2. Combinatorial lemmas

We will use the following combinatorial lemmas to prove our lower bounds for the function POLY$(q, s)$.

**Lemma 4.2.** *Let $G=(U, V, E)$ be a random bipartite graph, in which each edge appears independently with probability $1-\varepsilon$. Suppose $A\subseteqq\mathscr{E}(l)$* and *$A\vdash F$. Then*

$$\mathrm{Pr}[F \textit{ is contained in } E \textit{ and no set in } A \textit{ is contained in } E]\leqq\left(1-(1-\varepsilon)^l\right)^r\leqq(\varepsilon l)^r.$$

**Proof.** $A\vdash F$ means that there are $F_1, F_2, \ldots, F_r\in A$ satisfying $F_1, F_2, \ldots, F_r\vdash F$. Hence

$$\begin{aligned}\mathrm{Pr}[F \text{ is contained in } E \text{ and no set in } A \text{ is contained in } E] &\leqq \mathrm{Pr}[\forall i\, F_i \subsetneqq E \mid F\subseteqq E]\\ &= \prod_{i=1}^{r} \mathrm{Pr}[F_i \subsetneqq E \mid F\subseteqq E],\end{aligned}$$

where the last equality holds since, by the definition of $\vdash$, the events $\{F_i \nsubseteqq E | F \subseteqq E\}$ are independent. But

$$\Pr[F_i \nsubseteqq E | F \subseteqq E] = 1-(1-\varepsilon)^{|F_i - F|} \leqq 1-(1-\varepsilon)^l,$$

and we are done. ▌

**Lemma 4.3.** *Let $G$ be as in Lemma 4.1, and suppose $C \subseteqq \mathscr{E}(l)$. Then*

$$\Pr[G \in \lceil C^* \rceil - \lceil C \rceil] \leqq 2r^l(1-(1-\varepsilon)^l)^r \leqq 2r^l(\varepsilon l)^r.$$

**Proof.** Consider the closure algorithm for going from $C$ to $C^*$. By Lemma 3.5, the algorithm terminates in at most $2r^l$ iterations. The proof of Lemma 3.7, using Lemma 4.2 in place of Lemma 3.6, gives the required bound. ▌

### 4.3. Lower bounds for the polynomial problem

In this subsection, we give our lower bounds for POLY$(q, s)$, the function defined in the beginning of this section. Recall the lattice $K(q, r, l)$ defined in subsection 4.1.

**Theorem 4.4.** *Let $K = K(q, r, l)$, where $l = s$ and $r \leqq q/3+1$. Set $f =$ POLY$(q, s)$. Then*

$$\varrho(f, K) \geqq \min\left(\frac{1}{6}\left(\frac{q}{r-1}\right)^{s/2}, \quad \frac{1}{4r^l}\left(\frac{q}{2s^2 \ln q}\right)^r\right).$$

**Proof.** Let $t = \varrho(f, K)$. By definition of $\varrho(f, K)$, there are $M, M_1, N_1, \ldots, M_t, N_t \in K$ satisfying

$$A(f) \subseteqq M \cup \bigcup_{i=1}^{t} \delta_{\sqcap}(M_i, N_i) \tag{4.1}$$

and

$$M \subseteqq A(f) \cup \bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i). \tag{4.2}$$

Set $M = \lceil A \rceil$, $M_i = \lceil A_i \rceil$, and $N_i = \lceil B_i \rceil$, where $A$, $A_i$, and $B_i$ are closed subsets of $\mathscr{E}(l)$. The proof is divided into two cases, depending on $M$.

**Case 1.** *$M$ is not the set of all graphs.*

For a polynomial $p$ over GF$(q)$, the graph corresponding to $p$ is defined to be $\{(i, p(i)) \colon i \in U\}$. Using (4.1), we will show that $t$ must be large using the following two claims.

**Claim 1.** *$M$ contains at most one-half of the $q^s$ graphs corresponding to polynomials of degree at most $s-1$.*

**Claim 2.** *Each $\delta_{\sqcap}(M_i, N_i)$ contains at most $3q^{s-\lceil (l+1)/2 \rceil}(r-1)^{\lceil (l+1)/2 \rceil}$ of the graphs corresponding to polynomials of degree at most $s-1$.*

**Proof of Claim 1.** Notice that, since $M$ is not the set of all graphs, every $F \in A$ has cardinality at least 1. By Corollary 3.3, the set $A$ has at most $(r-1)^k$ minimal elements of cardinality $k$. Each of these is contained in either precisely 0 or precisely $q^{s-k}$ graphs corresponding to polynomials of degree at most $s-1$. The total number of such polynomial graphs contained in $M$ is thus at most

$$\sum_{k=1}^{l}(r-1)^k q^{s-k} = q^s \sum_{k=1}^{l}\left(\frac{r-1}{q}\right)^k \leqq q^s \sum_{k=1}^{l}\left(\frac{1}{3}\right)^k < \frac{1}{2}q^s. \ \blacksquare$$

**Proof of Claim 2.** This is analogous to the proof of Claim 2 in the proof of Lemma 3.8. ▮

From these two claims we obtain

$$t \geqq \frac{1}{6}\left(\frac{q}{r-1}\right)^{\lceil (l+1)/2\rceil} \geqq \frac{1}{6}\left(\frac{q}{r-1}\right)^{s/2},$$

as needed.

**Case 2.** *M is the set of all graphs.*

Using (4.2), we have

$$\{\text{all graphs}\} \subseteqq A(f) \cup \bigcup_{i=1}^{t} \delta_{\sqcup}(M_i, N_i).$$

Notice that $\delta_{\sqcup}(M_i, N_i) = [C_i^*] - [C_i]$, where $C_i = A_i \cup B_i$. Let $G$ be a random bipartite graph, with each edge appearing independently with probability $1-\varepsilon$. It is easy to see that

$$\Pr[G \in A(f)] \leqq q^s(1-\varepsilon)^q \leqq q^s e^{-\varepsilon q},$$

so by choosing $\varepsilon = (s \ln q + \ln 2)/q \leqq (2s \ln q)/q$, this probability is at most 1/2. Now by Lemma 4.3,

$$\Pr[G \in [C_i^*] - [C_i]] \leqq 2r^l(\varepsilon l)^r.$$

Thus we have

$$1 \leqq \frac{1}{2} + t(2r^l(\varepsilon l)^r),$$

which means that

$$t \geqq \frac{1}{4r^l}\left(\frac{1}{\varepsilon l}\right)^r \geqq \frac{1}{4r^l}\left(\frac{q}{2s^2 \ln q}\right)^r.$$

Thus Case 2 is finished, and the proof of the theorem is complete. ▮

As an immediate consequence of the last theorem, we obtain the following.

**Corollary 4.5.** *For* $s \leqq 1/2\sqrt{q/\ln q}$, *we have*

$$L^+(\mathrm{POLY}(q, s)) = q^{\Omega(s)}.$$

**Proof.** Take $r=\lceil 4s\ln q\rceil$, and apply Theorem 4.4 and Theorem 2.1. ▌

For fixed $s$ we can prove the following.

**Theorem 4.6.** *For fixed $s$, every monotone circuit computing* POLY$(q, s)$ *must have* $\Omega(q^s)$ AND *gates.*

**Proof.** Choose $l=s$ and $r=10s$, and then use the methods of subsection 3.5 (Theorem 3.16). We omit the details. ▌

## 5. Other Boolean functions

The known reductions of the clique function to several other NP-complete functions are actually monotone reductions. Therefore the lower bounds for the monotone circuit complexity of CLIQUE$(m, s)$ supply exponential lower bounds for other Boolean functions. We list below a few simple examples.

Let $f$ and $g$ be two monotone Boolean functions of $m$ and $n$ variables respectively. The function $f$ is a *monotone projection* of $g$ (see Valiant [17] and Skyum and Valiant [15]) iff there exist $\sigma_1, \sigma_2, \ldots, \sigma_n \in \{0, 1\} \cup \{x_1, x_2, \ldots, x_m\}$, such that $f= =g(\sigma_1, \sigma_2, \ldots, \sigma_n)$. Clearly, if $f$ is a monotone projection of $g$, then $L^+(f) \leqq L^+(g)$, as a lower bound for $f$ implies a lower bound for $g$.

Let HAM$(m)$ denote the monotone function of $\binom{m}{2}$ Boolean variables representing a graph on $m$ vertices, whose value is 1 iff the graph contains a Hamiltonian circuit. The results of Valiant [17] imply that, for $1 \leqq s \leqq m$, the function CLIQUE$(m, s)$ is a monotone projection of HAM$(m^k)$, for some constant $k$. In fact, we can show that CLIQUE$(m, s)$ is a monotone projection of HAM$(25m^2)$. Therefore, by Theorem 3.9, the monotone circuit complexity of HAM$(m)$ is $\exp\left(\Omega(m^{1/6}/(\log m)^{1/3})\right)$.

Let SAT$(m)$ denote the monotone function of $2m^2$ variables $x_{11}, \ldots, x_{mm}, y_{11}, \ldots$ $\ldots, y_{mm}$, whose value is 1 iff there is an assignment $z_1, \ldots, z_m \in \{0, 1\}$ such that the formula

$$\bigwedge_{i=1}^{n} \bigvee_{j=1}^{n} [(x_{ij} \wedge z_j) \vee (y_{ij} \wedge \overline{z_j})]$$

is satisfied. It is easy to show that, for $1 \leqq s \leqq m$, the function CLIQUE$(m, s)$ is a monotone projection of SAT$(5m^2)$. Thus, by Theorem 3.9, the monotone circuit complexity of SAT$(m)$ is $\exp\left(\Omega(m^{1/6}/(\log m)^{1/3})\right)$.

Let $G=(V, E)$ be an undirected graph. A set of vertices $U \subseteqq V$ is a *vertex cover* of $G$ if for each edge $\{i, j\}$ of $E$, either $i \in U$ or $j \in U$. Let VC$(m, k)$ denote the monotone function of $\binom{m}{2}$ Boolean variables representing a graph $G$ on $m$ vertices, whose value is 1 iff $G$ does not have a vertex cover of cardinality $k$.

**Proposition 5.1.** *For* $k=m-\left\lfloor \frac{1}{4}(m/\log m)^{2/3} \right\rfloor$, *the monotone circuit complexity of* VC$(m, k)$ *is* $\exp\left(\Omega((m/\log m)^{1/3})\right)$.

**Proof.** Given a function $f$ of $n$ variables, its *dual* (denoted by $f^*$) is the function of $n$ variables defined by $f^*(x_1, x_2, \ldots, x_n) = \neg f(\neg x_1, \neg x_2, \ldots, \neg x_n)$. If $f$ is a monotone function, then its dual $f^*$ is also monotone, and DeMorgan's laws imply that $L^+(f)=L^+(f^*)$. Notice that the dual of VC$(m, k)$ is CLIQUE$(m; m-k)$, since $G$ has a vertex cover of cardinality $k$ iff its complement $\bar{G}$ has a clique of cardinality $m-k$. The result now follows from Theorem 3.9. ▌

Let $D=(V, E)$ be a directed graph. A set of vertices $U\subseteq V$ is a *feedback vertex cover* of $D$ if each directed cycle of $D$ contains some vertex in $U$. A set of edges $F\subseteq E$ is a *feedback edge cover* if each directed cycle of $D$ contains some edge from $F$. Put $n=m(m-1)$ and let $x_1, x_2, \dots, x_n$ be $n$ Boolean variables representing the edges of a directed graph $D$ on $m$ vertices. Let FV$(m, k)$ denote the monotone function of $x_1; x_2, \dots, x_n$ whose value is 1 iff $D$ does not have a feedback vertex cover of cardinality $k$. Similarly, let FE$(m, k)$ denote the monotone function of $x_1, x_2, \dots, x_n$ whose value is 1 if $D$ does not have a feedback edge cover of cardinality $k$.

**Proposition 5.2.** *For* $k=m-\left\lfloor\frac{1}{16}(m/\log m)^{2/3}\right\rfloor$, *the monotone circuit complexities of* FV$(m, k)$ *and* FE$(m, k)$ *are* $\exp(\Omega((m/\log m)^{1/3}))$.

**Proof.** The standard reductions of Vertex Cover to Feedback Vertex Cover and to Feedback Edge Cover (see for example [1]) are monotone and linear. Thus using Proposition 5.1 the proof is complete. ▌

There are several other monotone reductions of the clique problem to various NP-complete problems which yield exponential lower bounds for the monotone circuit complexities of the corresponding Boolean functions. As observed by P. Frankl, one can also deduce such lower bounds from the proofs of Lemma 3.8 and Theorem 3.9. Indeed, these supply lower bounds for any monotone function $f$ of $\binom{m}{2}$ variables representing $G=(V, E)$, whose value is 1 if $G$ is an $s$-clique, is 0 if $G$ is a complete $(s-1)$-partite graph, and is arbitrary otherwise. For example, if COLOR$(m, s)$ is the function that is 1 iff $G$ is not $s$-colorable, then for $s= =\lfloor(m/(8\log \mathrm{m}))^{2/3}\rfloor$ the monotone circuit complexity of COLOR$(m, s)$ is at least $\exp(\Omega((m/\log m)^{1/3}))$.

Razborov [13] obtained an $m^{\Omega(\log m)}$ lower bound for the monotone circuit complexity of the perfect matching function PM$(m)$. This is the Boolean function of $n=m^2$ variables representing the edges of a bipartite graph $G=(U, V, E)$ such that $|U|=|V|=m$, whose value is 1 iff $G$ contains a perfect matching. The nonmonotone circuit complexity of PM$(m)$ is actually polynomial, using for example the Hopcroft and Karp [7] matching algorithm. So far, we have not been able to improve the $m^{\Omega(\log m)}$ lower bound for the monotone circuit complexity of PM$(m)$. It is worth noting that Perfect Matching has a monotone, linear reduction to various other problems, including Network Flow and Local Connectivity between two vertices in a directed graph. Consequently one obtains $m^{\Omega(\log m)}$ lower bounds for the monotone circuit complexities of the corresponding functions.

## 6. Acknowledgements

We would like to thank P. Frankl for many helpful discussions, especially for his help in the proofs of Lemma 3.2 and Lemma 3.5. We also thank A. Goldberg, V. Rödl and M. Sipser for fruitful discussions.

## 7. References

[1] A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison—Wesley, Reading, 1974.

[2] A. E. Andreev, On a method for obtaining lower bounds for the complexity of individual monotone functions, *Dokl. Ak. Nauk. SSSR* **282** (1985), 1033—1037 (in Russian). English translation in *Sov. Math. Dokl.* **31** (1985), 530—534.

[3] P. A. Bloniarz, *The complexity of monotone Boolean functions and an algorithm for finding shortest paths in a graph*, Ph. D. Dissertation, Technical Report **238**, Laboratory for Computer Science, Massachusetts Institute of Technology, 1979.

[4] N. Blum, A Boolean function requiring $3n$ network size, *Theoretical Computer Science* **28** (1984), 337—345.

[5] F. Chung and R. M. Karp, *in:* Open problems proposed at the NSF Conf. on Complexity Theory, Eugene, Oregon 1984, *SIGACT News* **16** (1984), 46.

[6] P. Erdős and R. Rado, Intersection theorems for systems of sets, *Journal of London Mathematical Society* **35** (1960), 85—90.

[7] J. E. Hopcroft and R. M. Karp, An $n^{5/2}$ algorithm for maximum matching in bipartite graphs, *SIAM Journal on Computing* **4** (1973), 225—231.

[8] K. Mehlhorn and Z. Galil, Monotone switching circuits and Boolean matrix product, *Computing* **16** (1976), 99—111.

[9] J. Nešetřil and S. Poljak, On the complexity of the subgraph problem, *CMUC* **26** (1985), 415—419.

[10] M. S. Paterson, Complexity of monotone networks for Boolean matrix products, *Theoretical Computer Science* **1** (1975), 13—20.

[11] V. R. Pratt, The power of negative thinking in multiplying Boolean matrices, *SIAM Journal on Computing* **4** (1974), 326—330.

[12] A. A. Razborov, Lower bounds for the monotone complexity of some Boolean functions, *Dokl. Ak. Nauk. SSSR*, **281**, (1985), 798—801 (in Russian). English translation in: *Sov. Math. Dokl.*, **31** (1985), 354—357.

[13] A. A. Razborov, Lower bounds on monotone network complexity of the logical permanent, *Mat. Zametki*, **37** (1985), 887—900 (in Russian). English translation in: *Math. Notes of the Academy of Sciences of the USSR* **37** (1985), 485—493.

[14] C. E. Shannon, The synthesis of two-terminal switching circuits, *Bell System Technical Journal*, **28** (1949), 59—98.

[15] S. Skyum and L. G. Valiant, A complexity theory based on Boolean algebra, *Journal of the ACM*, **32: 2** (1985), 484—502.

[16] J. Tiekenheinrich, A $4n$-lower bound on the monotone network complexity of a one-output Boolean function, *Information Processing Letters*, **18** (1984), 201—202.

[17] L. G. Valiant, Completeness classes in algebra, *Proceedings of* **11***th ACM Symposium on Theory of Computing*, (1979), 249—261.

[18] I. Wegener, Boolean functions whose monotone complexity is of size $n^2/\log n$, *Theoretical Computer Science*, **21** (1982), 213—224.

Noga Alon

*Department of Mathematics*
*Tel Aviv University*
*Tel Aviv, Israel*

and

*IBM Almaden Research Center*
*650 Harry Road*
*San Jose, CA 95120, U. S. A.*

Ravi B. Boppana

*Laboratory for Computer Science*
*Massachusetts Inst. of Tech.*
*545 Technology Square*
*Cambridge, Mass. 02139, U. S. A.*