COMBINATORICA
Akadémiai Kiadó — Springer-Verlag

COMBINATORICA 10 (1) (1990) 81—93

APPLICATIONS OF MATRIX METHODS TO THE THEORY OF LOWER BOUNDS IN COMPUTATIONAL COMPLEXITY

A. A. RAZBOROV

Received August 8, 1988
Revised August 22, 1989

We present some criteria for obtaining lower bounds for the formula size of Boolean functions. In the monotone case we get the bound $n^{\Omega(\log n)}$ for the function "MINIMUM COVER" using methods considerably simpler than all previously known. In the general case we are only able to prove that the criteria yield an exponential lower bound when applied to almost all functions. Some connections with graph complexity and communication complexity are also given.

Introduction

One of the main tasks of the lower bounds theory is to discover some combinatorial or algebraic properties of boolean functions which would imply high complexity in interesting computational models. In the present paper we give a series of such properties for formula size. We deal with three different versions of this complexity measure, namely monotone formula size, formula size over a complete basis and formula size within graph complexity (the last notion was considered in [19, 6]). The starting point for our methods is Theorem 1.3 implicitly used in [8] and first proved in [7]. We give a new proof of this theorem based on an interpretation of the formula size as existence of a winning strategy for one of the players in a two-person game and an incomplete converse to it. This game, in turn, is a modification of that considered in [14].

In the monotone case we prove the bound $n^{\Omega(\log n)}$ for the monotone formula size of the function "MINIMUM COVER" using one of our criteria. Note that previously there were known two methods for obtaining superpolynomial lower bounds for monotone formula size: the method of approximations [3, 4, 1, 10, 21, 2] (actually suitable for arbitrary monotone circuits) and the method of restrictions [14]. In particular, for the function "MINIMUM COVER" it is possible to prove a much stronger result using approximations (see [10, Prop. 5.1]). The method presented here is essentially simpler than both previous methods and seems to be interesting in its own right.

We design, as an intermediate step, a non-singular matrix over $\mathbf{F}_2$ of size $m^{\Omega(\log m)}$ which possesses a covering by $m^{O(1)}$ monochromatic submatrices. Similar matrices (with a bit worse estimate for the order) were used in [17] for constructing a predicate such that both it and its complement have nondeterministic communication complexity $O(t)$ whereas its deterministic communication complexity is

AMS subject classification (1980): 68Q30

$\Omega(t^2/\log^2 t)$. As a by-product we obtain the improvement of this gap to $\Omega(t^2)$ (it is achieved for the predicate "DISJOINTNESS OF $O(\log m)$-SUBSETS OF AN m-SET"); the quadratic gap matches the upper bound $O(t^2)$ from [9]. Conversely, we show that *any* example of a *superlinear* gap between $DCC(A)$ and

$$\max(NCC(A), NCC(\neg A))$$

can be used for obtaining *superpolynomial* lower bounds for the monotone formula size of a monotone Boolean function.

The quadratic gap between deterministic and non-deterministic communication complexities (but for a more complicated predicate) was also proved in [13].

One of the criteria considered in the present paper for formula size over a complete basis and formula size in graph complexity is similar to that communicated to me (without proof) by P. Pudlak (see [18]). We deduce below this criterion from other ones (see Corollary 3.6). We also prove that this criterion is partially invertible and hence yields exponential lower bounds when applied to "almost all" bipartite graphs and "almost all" boolean functions. This can be extended to all other criteria from which the criterion is deduced. But by now I have failed to prove a nontrivial lower bound for an explicitly given boolean function (or a graph) based on these criteria.

The paper is organized as follows. In Section 1 we define a two-person game and prove the initial criterion (Theorem 1.3). In Section 2 we consider monotone and communication complexities; in Section 3 — the complexity over the standard complete basis and the complexity of bipartite graphs. In Section 4 we present two open questions.

1. The game "FORMULA" and coverings of matrices

Throughout the paper B^n denotes an n-dimensional boolean cube and $F_n[F_n^{mon}]$ the set of all boolean functions [the set of all monotone boolean functions respectively] in n variables. For $u \in B^n$ u^i $(1 \leqq i \leqq n)$ means the ith bit in u. Let $X_i^\varepsilon = \{u \in B^n | u^i = \varepsilon\}$ for $1 \leqq i \leqq n$, $\varepsilon \in \{0, 1\}$. Given a variable x_i, set $x_i^1 = x_i$; $x_i^0 = (\neg x_i)$. Given $f \in F_n$, $U \subseteq B^n$, $\varepsilon \in \{0, 1\}$, the statement $\forall u \in U(f(u) = \varepsilon)$ will be written in the simplified form $f(U) = \varepsilon$.

By a formula (over the standard basis) we mean a usual expression of the propositional calculus constructed from variables $x_1, x_2, \ldots, x_n$ with connectives $\vee$, $\&$, $\neg$; every formula $\Phi(x_1, x_2, \ldots, x_n)$ computes in a natural way some function from F_n. The *size* $s(\Phi)$ of a formula Φ is the total number of occurrences of variables in Φ. Using De Morgan's laws we can transform every formula into a *formula with tight negations* (i.e. such a formula in which negations occur only in the form $(\neg x_i)$) without enlarging its size. Given $f \in F_n$, the *formula size* $L(f)$ is $\min\{s(\Phi) | \Phi \text{ computes } f\}$. A formula is *monotone* if it contains no negations at all; the *monotone formula size* $L_{mon}(f)$ of an $f \in F_n^{mon}$ is defined by analogy with $L(f)$. The *depth* of a formula is defined in the standard way; we denote the corresponding complexity measure by $D(f)$ [$D_{mon}(f)$ for the monotone case]. It is clear that $L(f) \leqq \exp(O(D(f)))$, the opposite inequality $D(f) \leqq O(\log L(f))$ is the deep result due to Spira [20].

The game *"FORMULA"* is a game of two players Up (upper) and Lo (lower). Up will try to prove an upper bound for the formula size of a Boolean function;

Lo will try to interfere him. A *position* is a triplet (U, V, t) where $U, V \subseteq B^n$, $U \cap V = \emptyset$, $t \geqq 1$ is an integer. Up begins the game. He obtains a position (U, V, t), chooses one of the two sets U, V (say, U), somehow represents U and t in the form

$$U = U' \cup U'', \quad t = t' + t'' \quad (t', t'' \geqq 1) \tag{1}$$

and hands to Lo the two positions (U', V, t') and (U'', V, t''). If Up chooses the set V, the description of his actions is given in the analogous way.

Lo chooses one of the two positions offered to him and returns it to Up (the remaining position is thrown out). Then Up moves as above (in the new position) and so on. The game is over when Up receives a position of the form $(U^*, V^*, 1)$. Up wins if

$$\exists i, \varepsilon (1 \leqq i \leqq n \ \& \ \varepsilon \in \{0, 1\} \ \& \ U^* \subseteq X_i^{\varepsilon} \ \& \ V^* \subseteq X_i^{1-\varepsilon}) \tag{2}$$

otherwise Lo wins.

Theorem 1.1. Up *has a winning strategy in a position* (U, V, t) *iff there exists* $f \in F_n$ *such that*

$$f(U) = 0, \quad f(V) = 1, \quad L(f) \leqq t. \tag{3}$$

Proof. By induction on t.

Base $t = 1$ is clear because (2) just means that $x_i^{\varepsilon}(U^*) = 0$, $x_i^{\varepsilon}(V^*) = 1$ holds for a variable or its negation x_i^{ε}.

Inductive step. Assume that the theorem is proved for all values of t less than a given one. First assume that Up has a winning strategy in (U, V, t) and this strategy requires Up to make the move (1). Then Up has winning strategies in both positions (U', V, t'), (U'', V, t''), hence, by the inductive hypothesis, there are $f', f'' \in F_n$ such that $f'(U') = 0$, $f'(V) = 1$, $L(f') \leqq t'$ and $f''(U'') = 0$, $f''(V) = 1$, $L(f'') \leqq t''$. Then the function $f = f' \ \& \ f''$ [$f' \vee f''$ if Up chooses V] satisfies (3).

To prove this in the other direction, assume that $f \in F_n$ satisfies (3) and Φ is a formula with tight negations computing f such that $s(\Phi) \leqq t$. Suppose that Φ is of the form $\Phi' \ \& \ \Phi''$ (the case when Φ is a disjunction is treated with a dual argument). Then, by the inductive hypothesis, Up wins if he makes the move (1) where $U' = (\Phi')^{-1}(0) \cap U$; $U'' = (\Phi'')^{-1}(0) \cap U$; $t' = s(\Phi')$; $t'' = s(\Phi'')$. ∎

Consider now a modification "*FORMULA* 1" of this game. The only difference from the game "FORMULA" is that Up is obliged to make only those moves (1) for which $U' \cap U'' = \emptyset$.

Lemma 1.2. *Given a position,* Up *has a winning strategy in "FORMULA* 1" *iff he has such a strategy in "FORMULA".*

Proof. Clearly, each winning strategy of Up in the game "FORMULA 1" wins also in "FORMULA". Conversely, given a winning strategy of Up in the game "FORMULA" with move (1) required in a position (U, V, t), we obtain a move permitted in the game "FORMULA 1" by replacing U'' with $U \setminus U' (\subseteq U'')$. It is easy to see that this strategy of Up in the game "FORMULA 1" is winning. ∎

Assume now that we are given two finite sets U and V (in general, of arbitrary nature). A *rectangle* (over U, V) is an arbitrary subset of the cartesian product

$U\times V$ which has the form $U_0\times V_0$ where $U_0\subseteq U, V_0\subseteq V$. Every set $\mathscr{R}$ of rectangles such that $\cup\mathscr{R}=U\times V$ will be called a *covering* (over U, V). A covering $\mathscr{R}$ is *disjoint* if the intersection of any two rectangles from $\mathscr{R}$ is empty. A covering $\mathscr{R}_1$ is *embedded* in a covering $\mathscr{R}_2$ if $\forall R_1\in\mathscr{R}_1\ \exists R_2\in\mathscr{R}_2\ (R_1\subseteq R_2)$. Finally, set

$$\alpha(\mathscr{R}) = \min\{|\mathscr{R}'|\,|\,\mathscr{R}' \text{ is a disjoint covering embedded in } \mathscr{R}\}. \tag{4}$$

Given $U, V\subseteq B^n$ such that $U\cap V=\emptyset$, we can define a special covering over U, V by letting $\mathscr{R}_{can}(U, V)=\{R_{01}, R_{02}, \ldots, R_{0n}, R_{11}, R_{12}, \ldots, R_{1n}\}$ where

$$R_{\varepsilon i} = (U\cap X_i^{\varepsilon})\times(V\cap X_i^{1-\varepsilon}) \quad (1\leqq i\leqq n,\ \varepsilon\in\{0, 1\}). \tag{5}$$

$\mathscr{R}_{can}(U, V)$ is a covering because for any $u\in U, v\in V$ there exists i such that $u^i\neq v^i$. We call this covering *canonical*. Given $f\in F_n$, set $\mathscr{R}_{can}(f)=\mathscr{R}_{can}(f^{-1}(0), f^{-1}(1))$.

Now we are in position to formulate the initial criterion.

Theorem 1.3 [8, 7]. *Given $U, V\subseteq B^n$ such that $U\cap V=\emptyset$ and given $f\in F_n$ such that $f(U)=0, f(V)=1$, the inequality $L(f)\geqq\alpha(\mathscr{R}_{can}(U, V))$ holds. In particular, $L(f)\geqq\alpha(\mathscr{R}_{can}(f))$.*

Proof. Let $f(U)=0, f(V)=1, L(f)=t$. Then, by Theorem 1.1 and Lemma 1.2, Up has a winning strategy in the position (U, V, t) in the game "*FORMULA* 1". Fix one of these strategies S. Call the protocol of a game *regular* if Up was using the strategy S throughout this game. It can be proved by an obvious induction on t that the total number of regular protocols is just t. Given $u\in U$ and $v\in V$, denote by $L(u, v)$ the strategy of the player Lo which, after a move (1) of Up, consists in choosing the position (U', V, t') if $u\in U'$ and (U'', V, t'') if $u\in U''$. If Up has splitted the set V, Lo makes his decision by using v in an analogous manner. Let $P(u, v)$ be the (regular) protocol resulting from competition between the strategies S and $L(u, v)$. Finally, for any regular protocol P set $R_p=\{(u, v)|P(u, v)=P\}$. Then $\mathscr{R}=\{R_p|P \text{ is a regular protocol}\}$ is a disjoint covering of $U\times V$. Moreover, the R_p's are rectangles because it is easy to see that $R_p=U^*(P)\times V^*(P)$ where $(U^*(P), V^*(P), 1)$ is the final position of a protocol P. Hence $\mathscr{R}$ is a disjoint covering by rectangles over U, V of cardinality t. Finally, by (2) and the fact that S is a winning strategy, $\mathscr{R}$ is embedded into $\mathscr{R}_{can}(U, V)$. So, $\alpha(\mathscr{R}_{can}(U, V))\leqq t$. ∎

Remark 1.4. This theorem was proved in [8, 7] by using an analysis on so-called Π_1-networks (these are a special form of common boolean formulas). It is also possible to give a very short proof just by a straightforward induction on t. We have chosen the bit longer way above to clarify the connection with communication complexity and especially with the paper [14].

Remark 1.5. Two rectangles $(U\setminus U_0)\times(V\setminus V_0)$ and $U_0\times V_0$ will be called *complementary*. A covering $\mathscr{R}$ is *self-complementary* if it contains $(U\setminus U_0)\times(V\setminus V_0)$ whenever it contains $U_0\times V_0$. For instance, any canonical covering is self-complementary. On the other hand, we can assign to any self-complementary covering

$$\mathscr{R} = \{U_1\times V_1, (U\setminus U_1)\times(V\setminus V_1), U_2\times V_2, (U\setminus U_2)\times(V\setminus V_2), \ldots$$
$$\ldots, U_n\times V_n, (U\setminus U_n)\times(V\setminus V_n)\}$$

over U, V of cardinality $2n$ a mapping i: $U\cup V\to B^n$ such that $i(U)\cap i(V)=\emptyset$ and $\mathscr{R}_{can}(i(U), i(V))=\mathscr{R}$ (in order to determine i, we set the v'th bit in $i(u)$ to be

1 iff $u \in U_v$ and the v'th bit in $i(v)$ to be 1 iff $v \notin V_v$). So, Theorem 1.3 would imply good lower bounds for the formula size of a boolean function as soon as such bounds were proved for the value $\alpha(\mathscr{R})$ where $\mathscr{R}$ is any covering over sets U, V of arbitrary nature.

We conclude this section with the following statement which is an incomplete converse to the Theorem 1.3:

Theorem 1.6. *Given $U, V \subseteq B^n$ such that $U \cap V = \emptyset$, there exists $f \in F_n$ such that $f(U)=0$, $f(V)=1$ and $D(f) \leqq O((\log \alpha(\mathscr{R}_{can}(U, V)))^2)$. In particular, $D(f) \leqq O((\log \alpha(\mathscr{R}_{can}(f)))^2)$.*

Proof. Fix a disjoint covering $\mathscr{R}$ embedded into $\mathscr{R}_{can}(U, V)$ with $|\mathscr{R}| = \alpha(\mathscr{R}_{can}(U, V))$. Assign to any $R \in \mathscr{R}$ the number $i(R) \in \{1, \ldots, n\}$ such that $\exists \varepsilon \in \{0, 1\}$ $(R \subseteq R_{\varepsilon, i(R)})$. Assign to any pair (u, v) the number $i(u, v) = i(R)$ where R is the rectangle containing (u, v). Note that $\mathscr{R}$ is a disjoint covering by rectangles which are monochromatic with respect to the function $i(u, v)$. Therefore, by the result of Aho, Ullman, Yannakakis [9], there exists a communication (cooperative) protocol which runs within $O((\log |\mathscr{R}|)^2)$ communications and, given u and v, outputs $i(u, v)$. Note also that, by definitions, u and v differ at $i(u, v)$. Now the theorem follows from [14]. ∎

Remark 1.7. Let us note that Theorems 1.3 and 1.6 together imply $D(f) \leqq O((\log L(f))^2)$ and this was proved *without* appealing to the construction of Spira [20]. Apparently this shows the deep analogy between the simulation $D(f) \leqq O(\log L(f))$ and the result by Aho, Ullman and Yannakakis [9].

2. Monotone and communication complexities

In this section we put on $U, V \subseteq B^n$ a restriction stronger than $U \cap V = \emptyset$, namely

$$\forall u \in U \forall v \in V \exists i \quad (u^i = 0 \ \& \ v^i = 1). \tag{6}$$

Note that (6) holds iff $\exists f \in F_n^{mon}(f(U)=0 \ \& \ f(V)=1)$. Consider the following collection of rectangles:

$$\mathscr{R}_{mon}(U, V) = \{R_{01}, R_{02}, \ldots, R_{0n}\},$$

where R_{0i} was defined in (5). By (6) this collection is a covering over U, V. We can define the game *"MONOTONE FORMULA"* by replacing (2) with $\exists i (1 \leqq i \leqq n \ \& \ U^* \subseteq X_i^0 \ \& \ V^* \subseteq X_i^1)$. After this all arguments of the Section 1 can be word-by-word transferred to the monotone case and we obtain the following theorem:

Theorem 2.1. *Let $U, V \subseteq B^n$ be such that (6) holds. Then for any $f \in F_n^{mon}$ such that $f(U)=0$, $f(V)=1$, $L_{mon}(f) \geqq \alpha(\mathscr{R}_{mon}(U, V))$.* ∎

The monotone analog of the Theorem 1.6 also holds.

This time, however, *any* covering (not necessarily self-complementary) can be represented in the form $\mathscr{R}_{mon}(U, V)$ in the sense of Remark 1.5 (we shall see below an example of such an encoding). So, we assume that U, V are finite sets of an arbitrary nature.

By a *matrix over U, V* we mean a matrix over a field $\mathcal{k}$ whose rows are indexed by elements of the set U and columns by elements of the set V. Given a rectangle R, we denote by A_R the corresponding submatrix of a matrix A. $\hat{A}_R$ is the matrix over U, V obtained from A by replacing those a_{uv} for which $(u, v) \notin R$ by 0.

Theorem 2.2. *For any covering $\mathcal{R}$ over U, V and any non-zero matrix A over U, V (over an arbitrary field), the inequality*

$$\alpha(\mathcal{R}) \geqq \frac{\operatorname{rk}(A)}{\max\limits_{R \in \mathcal{R}} \operatorname{rk}(A_R)}$$

holds.

Proof. Let $\mathcal{R}'$ be a disjoint covering embedded in $\mathcal{R}$ such that $|\mathcal{R}'| = \alpha(\mathcal{R})$. Then $A = \sum\limits_{R \in \mathcal{R}'} \hat{A}_R$ therefore $\operatorname{rk}(A) = \operatorname{rk}\left(\sum\limits_{R \in \mathcal{R}'} \hat{A}_R\right) \leqq \sum\limits_{R \in \mathcal{R}'} \operatorname{rk}(\hat{A}_R)$. On the other hand, for any $R \in \mathcal{R}'$ we can find some $R_1 \in \mathcal{R}$ such that $R \subseteqq R_1$. Hence $\operatorname{rk}(\hat{A}_R) = \operatorname{rk}(A_R) \leqq$ $\leqq \operatorname{rk}(A_{R_1})$ and $\operatorname{rk}(A) \leqq |\mathcal{R}'| \cdot \max\limits_{R_1 \in \mathcal{R}} \operatorname{rk}(A_{R_1})$. ∎

Corollary 2.3. *Given a covering $\mathcal{R}$ and a matrix A such that for any $R \in \mathcal{R}$ all entries of the matrix A_R coincide, we have $\alpha(\mathcal{R}) \geqq \operatorname{rk}(A)$.* ∎

Assume now that $U = V = [m]^{\leqq k}$ (the family of all subsets of the set $\{1, 2, \ldots, m\}$ whose cardinality is at most k) and let A_{mk} be the matrix over U, V defined by

$$a_{uv} = \begin{cases} 0, & \text{if } u \cap v \neq \emptyset \\ 1, & \text{if } u \cap v = \emptyset. \end{cases}$$

Lemma 2.4. *A_{mk} is non-singular over any field.*

Proof. It follows from a general result [15, Theorem 2] that $\det(A_{mk}) = 1$ or -1 (another proof for the field $\mathbf{F}_2$ can be found in [5, Lemma 4]). ∎

Set now $R_i^0 = \{u \mid i \in u\} \times \{v \mid i \in v\}$ $(1 \leqq i \leqq m)$. The collection of rectangles $\{R_i^0 \mid 1 \leqq i \leqq m\}$ covers all zeros of A_{mk}. Given $\varepsilon \in B^m$, set $R_\varepsilon^1 = \{u \mid \forall i \in u (\varepsilon^i = 1)\} \times$ $\times \{v \mid \forall i \in v (\varepsilon^i \leqq 0)\}$. It is clear that all elements of $(A_{mk})_{R_\varepsilon^1}$ equal 1.

Lemma 2.5. *There exist $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_l \in B^m$ where*

$$l = \lfloor 2k 4^k \ln m \rfloor \tag{7}$$

such that $\bigcup\limits_{i=1}^{l} R_{\varepsilon_i}^1$ covers all ones of A_{mk}.

Proof. Pick independently at random $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_l \in B^m$. Then

$$\mathbf{P}\left[\exists (u, v) \in U \times V \left(u \cap v = \emptyset \quad \& \quad (u, v) \notin \bigcup_{i=1}^{l} R_{\varepsilon_i}^1\right]\right] \leqq$$

$$\leqq |U| \cdot |V| \cdot \max_{u \cap v = \emptyset} \mathbf{P}\left[(u, v) \notin \bigcup_{i=1}^{l} R_{\varepsilon_i}^1\right] <$$

$$< m^{2k} \cdot \max_{u \cap v = \emptyset} (1 - 2^{-|u|-|v|})^l \leqq m^{2k} \exp l(- \cdot 2^{-2k}) \leqq 1. \quad ∎$$

Remark 2.6. As observed by one of the referees, a weaker (but sufficient for our purposes) statement can be proved constructively using properties of the so-called Paley graphs. Namely, if m is a prime and $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m \in B^m$ are given by $\varepsilon_i^j = 1$ iff $i-j$ is a quadratic residue mod m then the conclusion of Lemma 2.5 holds for $l=m$ and $k=\Omega(\log m)$.

So, when $k=\Theta(\log m)$ we see (either by Lemma 2.5 or by Remark 2.6) that there exists a covering $\mathscr{R}$ of cardinality $m^{O(1)}$ for which the assumptions of the Corollary 2.3 hold and thus $\alpha(\mathscr{R}) \geqq m^{\Omega(\log m)}$. This implies the corresponding lower bound for the monotone formula size of a boolean function. Let us check that this function actually is a subfunction of the function "MINIMUM COVER"

MINIMUM COVER

Instance. A bipartite graph $H=(P, Q, E)$ and an integer k.

Question. Does there exist some $P_0 \subseteq P$ such that $|P_0|=k$ and $\forall q \in Q\ \exists p \in P_0\ ((p, q) \in E)$?

Fix P, Q, k and assign a boolean variable x_{pq} to any potential edge (p, q). Then "MINIMUM COVER" corresponds to the boolean function

$$MC(x) = \bigvee_{\substack{P_0 \subseteq P \\ |P_0|=k}} \ \& \ _{q \in Q} \bigvee_{p \in P_0} x_{pq}. \tag{8}$$

Suppose now that a set of edges $E \subseteq P \times Q$ is fixed. Let $\{e^{pq}\}$ be the boolean vector corresponding to E. Given $P' \subseteq P$, $Q' \subseteq Q$, consider the instance of the function "MINIMUM COVER" obtained by replacing the graph $H=(P, Q, E)$ by the induced graph $(P', Q \setminus Q', E \cap (P' \times Q \setminus Q'))$. The corresponding boolean function in variables $\{y_p | p \in P\}$, $\{z_q | q \in Q\}$ (representing the sets P' and Q' respectively) is monotone and can be written in the form

$$MC'_E(y, z) = \bigvee_{\substack{P_0 \subseteq P \\ |P_0|=k}} \ \& \ _{q \in Q} \bigvee_{p \in P_0} ((y_p \& e^{pq}) \vee z_q). \tag{9}$$

Comparing (8) and (9) we see that for any E,

$$2L_{mon}(MC) \geqq L_{mon}(MC'_E). \tag{10}$$

Let now $P=\{p_1, p_2, \ldots, p_m\}$, $Q=\{q_1, q_2, \ldots, q_l\}$ where l is given by (7). Choose $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_l \in B^m$ in accordance with the Lemma 2.5 and set $E=\{(p_i, q_j) | \varepsilon_j^i = 1\}$. Define two injective mappings i_U, i_V from $[m]^{\leqq k}$ to $\mathscr{P}(P \cup Q)$ by

$$i_U(x) = \{p_i | i \notin x\} \cup \{q_j | \exists i \in x (p_i, q_j) \notin E\};$$

$$i_V(x) = \{p_i | i \in x\} \cup \{q_j | \forall i \in x (p_i, q_j) \notin E\}.$$

After identifying $\mathscr{P}(P \cup Q)$ and B^{m+l} we see that $MC'_E(i_V(x))=1$ (we have to take the set $\{p_i | i \in x\}$ itself as P_0) and $MC'_E(i_U(x))=0$ (for any $P_0 \subseteq \{p_i | i \notin x\}$, by our choice of E, there exists $q \in Q$ such that $\forall i \in x (p_i, q) \in E$ and $\forall p \in P_0 (p, q) \notin E$). It is easy to see that $\mathscr{R}_{mon}(i_U([m]^{\leqq k}), i_V([m]^{\leqq k}))$ is just the covering

$$\{R_1^0, R_2^0, \ldots, R_m^0, R_{\varepsilon_1}^1, \ldots, R_{\varepsilon_l}^1\}$$

defined above. Hence (10), Theorem 2.1, Corollary 2.3 and Lmem a 2.4 impl the following result:

Theorem 2.7. *Under the condition* $|Q| \geqq 2k4^k \ln |P|$ *the bound* $L_{mon}(MC) \geqq \frac{1}{2}\binom{|P|}{k}$ *holds. In particular, when* $k=\Theta(\log |P|)$, *we obtain* $L_{mon}(MC) \geqq n^{\Omega(\log n)}$ *where* $n=|P| \cdot |Q|$ *is the total number of variables in the function MC.* ∎

We turn now to connections with communication complexity. The underlying concepts of deterministic and nondeterministic protocols were introduced by A. Yao [23] and R. Lipton, R. Sedgewick [16] respectively. There are different versions of these notions but all of them coincide up to a constant factor. From the combinatorial point of view, the *nondeterministic communication complexity* $NCC(A)$ of a 0—1 matrix A is $\lfloor \log_2 \rfloor$ of the minimal possible number of rectangles covering all ones of the matrix A [16]. The deterministic communication complexity $DCC(A)$ is harder to describe in combinatorial terms. It can be estimated from below by $\log_2$ of the minimal possible number of *disjoint* rectangles covering all ones of the matrix A [23], the last number being estimated, in turn, by $\log_2$ of the rank of A over any field [17]. Taking as A the matrix A_{mk} when $k=\Theta(\log m)$, we obtain

Theorem 2.8. *The nondeterministic communication complexity of both the predicate "DISJOINTNESS OF TWO* $O(\log m)$*-SUBSETS OF A m-SET" and its complement is* $O(\log m)$ *whereas the deterministic communication complexity of the same predicate is* $\Omega((\log m)^2)$. ∎

The first result of such kind was the gap $\Omega((t/\log t)^2)$ shown in [17]. The truly quadratic gap (but for a predicate more complicated than the "DISJOINTNESS OF TWO $O(\log m)$-SUBSETS OF A m-SET") was independently proved in [13]. Let us also note that this gap never exceeds $\Omega(t^2)$ [9], i.e. the bound of [13] and Theorem 2.8 is tight. In the other direction, the result of the paper [9] implies the following theorem restricting possibilities of the Corollary 2.3:

Theorem 2.9. *Given a covering* $\mathscr{R}$ *and a matrix* A *(not necessary* 0—1*) such that for any* $R \in \mathscr{R}$ *all elements of* A_R *are equal, we have* $rk(A) \leqq |\mathscr{R}|^{O(\log |\mathscr{R}|)}$. ∎

We conclude this section with an important observation made by one of the referees. We have already seen that any 0—1 matrix A gives rise to a monotone Boolean function f in $2^{NCC(A)}+2^{NCC(\neg A)}$ variables with the lower bound $L_{mon}(f) \geqq \geqq \mathrm{rk}(A)$ for its monotone formula size. The observation is that actually this lower bound can be improved to $L_{mon}(f) \geqq 2^{\Omega(DCC(A))}$. This follows from $L_{mon}(f) \geqq \geqq 2^{\Omega(D_{mon}(f))}$ [22] and the Theorem 2.2 from [14].

So, *any* example of a *superlinear* gap between $DCC(A)$ and

$$\max\left(NCC(A), NCC(\neg A)\right)$$

can be used for obtaining *superpolynomial* lower bounds for the monotone formula size of a monotone Boolean function.

3. Complexity over the standard basis and complexity of bipartite graphs

A *partial matrix* over U, V is a usual matrix over U, V with the exception that some entries can be left empty, without placing into them any elements of the underlying field. The *rank* of a partial matrix A is defined to be the minimal rank of all possible full extensions of the partial matrix A.

Theorem 3.1. *Let $\mathscr{R}$ be a covering over U, V represented in the form $\mathscr{R}=\mathscr{R}_1\cup\mathscr{R}_2$, let k be a field and let $a_1, a_2\in k$. Define the partial matrix A by*

$$a_{uv}=\begin{cases}a_1, & \text{if } \langle u,v\rangle\notin\cup\mathscr{R}_1\\ a_2, & \text{if } \langle u,v\rangle\notin\cup\mathscr{R}_2\\ \text{left empty} & \text{otherwise.}\end{cases}$$

Then $\alpha(\mathscr{R})\geqq\mathrm{rk}(A)$.

Proof. Let $\mathscr{R}'$ be a disjoint covering embedded in $\mathscr{R}$ such that $|\mathscr{R}'|=\alpha(\mathscr{R})$. Let $\mathscr{R}'=\mathscr{R}'_1\cup\mathscr{R}'_2$; $\mathscr{R}'_1\cap\mathscr{R}'_2=\emptyset$ where $\mathscr{R}'_1$ is embedded in $\mathscr{R}_2$ and $\mathscr{R}'_2$ is embedded in $\mathscr{R}_2$. Let J be the matrix over U, V with all entries equal to 1. Then the matrix $a_1\sum_{R\in\mathscr{R}'_2}\hat{J}_R+a_2\sum_{R\in\mathscr{R}'_1}\hat{J}_R$ has rank at most $|\mathscr{R}'|$ and extends A; hence $\alpha(\mathscr{R})\geqq$ $\geqq\mathrm{rk}(A)$. ∎

So, dividing somehow variables of a boolean function f into two groups we obtain, by Theorems 1.3 and 3.1, a partial matrix A such that $L(f)\geqq\mathrm{rk}(A)$. It turns out however that the rank of the same matrix also estimates the formula size of the bipartite graph corresponding to f and the division under consideration.

To be more precise, fix two finite sets P, Q. A bipartite graph of the form (P, Q, E) will be identified with the characteristic function of the set $E\subseteq P\times Q$. Assign a boolean variable x_{P_0} to any $P_0\subseteq P$ and a variable y_{Q_0} to any $Q_0\subseteq Q$. Set $X_{P_0}=P_0\times Q$ and $Y_{Q_0}=P\times Q_0$. We think of x_{P_0} as the graph (P, Q, X_{P_0}) and of y_{Q_0} as the graph (P, Q, Y_{Q_0}). Then any boolean formula in variables $\{x_{P_0}\}$, $\{y_{Q_0}\}$ computes in the natural way a graph. So, we can define the corresponding *formula size of a bipartite graph* E denoted by $L_{gr}(E)$ and its *depth* denoted by $D_{rg}(E)$. Because of $\neg x_{P_0}=x_{P-P_0}$, $\neg y_{Q_0}=y_{Q-Q_0}$ we can consider only monotone formulas; negations have no power in this computational model. Finally, note that it is possible to associate the bipartite graph $H(f)=(\{0,1\}^n, \{0,1\}^n, E(f))$ with any Boolean function $f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n)$ (here $E(f)=\{\langle\varepsilon,\delta\rangle | f(\varepsilon,\delta)=1\}$). After this we obtain $L(f)\geqq L_{gr}(E(f))$ therefore the problem of proving lower bounds for complexity of boolean functions is reduced to the same problem for bipartite graphs. More information about graph complexity can be found in [19, 6, 11].

Assume now that $U, V\subseteq P\times Q$, $U\cap V=\emptyset$. Define $\mathscr{R}_{gr}(U, V)$ to be the covering over U, V consisting of the following two collections of rectangles:

$$\{(U\setminus X_{P_0})\times(V\cap X_{P_0}) | P_0\subseteq P\}, \tag{11}$$

$$\{(U\setminus Y_{Q_0})\times(V\cap Y_{Q_0}) | Q_0\subseteq Q\}. \tag{12}$$

For $E\subseteq P\times Q$ set $\mathscr{R}_{gr}(E)=\mathscr{R}_{gr}(E, P\times Q\setminus E)$. Repeating word by word the arguments of Section 1 we obtain

Theorem 3.2. *Let $U, V\subseteq P\times Q$, $U\cap V=\emptyset$. Then for any graph $E\subseteq P\times Q$ such that $U\cap E=\emptyset$, $V\subseteq E$ we have $L_{gr}(E)\geqq\alpha(\mathscr{R}_{gr}(U, V))$.* ∎

The statement analogous to the Theorem 1.6 is:

Theorem 3.3. *Let* $U, V \subseteq P \times Q$, $U \cap V = \emptyset$. *Then there exists a graph* $E \subseteq P \times Q$ *such that* $U \cap E = \emptyset$, $V \subseteq E$ *and* $D_{gr}(E) \leqq O((\log \alpha(\mathscr{R}_{gr}(U, V))^2)$.

This theorem can be proved just as Theorem 1.6. Below we will see another proof of it grounded on entirely new ideas. ∎

Given U, V such that $U, V \subseteq P \times Q$, $U \cap V = \emptyset$, and two elements a_1, a_2 from a field $\mathscr{k}$, define the partial matrix $A(U, V, a_1, a_2)$ by

$$a_{uv} = \begin{cases} a & \text{if edges } u \text{ and } v \text{ have a common vertex in the set } P \\ a_2 & \text{if edges } u \text{ and } v \text{ have a common vertex in the set } Q \\ \text{left empty} & \text{otherwise.} \end{cases}$$

For $E \subseteq P \times Q$ set $A(E, a_1, a_2) = A((P \times Q \setminus E), E, a_1, a_2)$.

Applying Theorem 3.1 to the covering $\mathscr{R} = \mathscr{R}_{gr}(U, V)$ and the division (11), (12) of this covering into two parts we obtain

Theorem 3.4. *Let* $U, V \subseteq P \times Q$, $U \cap V = \emptyset$, $\mathscr{k}$ *be an arbitrary field and* $a_1, a_2 \in \mathscr{k}$. *Then* $\alpha(\mathscr{R}_{gr}(U, V)) \cong rk(A(U, V, a_1, a_2))$. *In particular,*

$$\alpha(\mathscr{R}_{gr}(E)) \cong \mathrm{rk}(A(E, a_1, a_2)). \quad ∎$$

From now on we consider only the case $U = E$, $V = P \times Q \setminus E$ but all the results below can be automatically extended for the general case.

Denote by $I(\mathscr{k}, d)$ the intersection graph of the family $S(\mathscr{k}, d)$ formed by all affine subspaces (of arbitrary dimension) of a d-dimensional affine space $A^d_{\mathscr{k}}$ over the field $\mathscr{k}$. We say that a bipartite graph (P, Q, E) is *realizable* in $I(\mathscr{k}, d)$ if there exists a mapping i: $P \cup Q \to S(\mathscr{k}, d)$ (not necessarily injective) such that $(p, q) \in E \Leftrightarrow i(p) \cap i(q) \neq \emptyset$. Denote by $\mathrm{adim}_{\mathscr{k}}(E)$ the *affine dimension of* E that is the minimal d for which (P, Q, E) is realizable in $I(\mathscr{k}, d)$.

Theorem 3.5. *Let* $E \subseteq P \times Q$; $\mathscr{k}$ *be an arbitrary field,* $a_1, a_2 \in \mathscr{k}$, $a_1 \neq a_2$. *Then* $\mathrm{rk}(A(E, a_1, a_2)) \cong \mathrm{adim}_{\mathscr{k}}(E)$.

Proof. Let B be a usual matrix of rank $d = \mathrm{rk}(A(E, a_1, a_2))$ extending $A(E, a_1, a_2)$. Let $U = P \times Q \setminus E$, $V = E$. Take the affine subspace in $\mathscr{k}^U$ generated by 0 and all columns of B as $A^d_{\mathscr{k}}$. Given $v \in V$, denote by $j(v)$ the corresponding column. Given $r \in P \cup Q$, let $i(r)$ be the affine subspace in $A^d_{\mathscr{k}}$ generated by vectors $\{j(v) | v$ is incident to $r\}$. We claim that i is the desirable realization.

If $v = (p, q) \in V$ then $j(v)$ belongs to the intersection of $i(p)$ and $i(q)$.

Assume $u = (p, q) \in U$. Define the affine functional π_u: $A^d_{\mathscr{k}} \to \mathscr{k}$ as the composition $A^d_{\mathscr{k}} \to \mathscr{k}^U \xrightarrow{\mu_u} \mathscr{k}$ where μ_u is the projection onto the u's position. Then for any $v \in V$ adjacent to p we have $\pi_u(j(v)) = a_{uv} = a_1$ and, similarly, if v is adjacent to q, $\pi_u(j(v)) = a_2$. Hence $\pi_u(i(p)) = \{a_1\}$, $\pi_u(i(q)) = \{a_2\}$. This implies $i(p) \cap i(q) = \emptyset$. ∎

As an application we obtain the following result.

Corollary 3.6. *For any* $E \subseteq P \times Q$ *and any field* $\mathscr{k}$, $L_{gr}(E) \cong \mathrm{adim}_{\mathscr{k}}(E)$. ∎

For finite fields this result can be partially reversed as follows:

Theorem 3.7. *For any finite field* $\mathcal{k}$, $D_{gr}(E) \leqq O((\log \operatorname{adim}_{\mathcal{k}}(E))^2)$.

Proof. Let $d = \operatorname{adim}_{\mathcal{k}}(E)$ and $i: P \cup Q \to S(\mathcal{k}, d)$ be an affine representation of the graph E. For $r \in P \cup Q$ write down $i(r)$ in the form

$$i(r) = a(r) + \operatorname{Span}(a_1(r), \ldots, a_{d(r)}(r))$$

where $d(r)$ is the affine dimension of $i(r)$ and $\operatorname{Span}(a_1, \ldots, a_m)$ is the linear space generated by $a_1, \ldots, a_m$. Then

$$\begin{aligned} &(p, q) \in E \Leftrightarrow \\ &i(p) \cap i(q) \neq \emptyset \Leftrightarrow \\ &a(p) - a(q) \in \operatorname{Span}(a_1(p), \ldots, a_{d(p)}(p), a_1(q), \ldots, a_{d(q)}(q)) \Leftrightarrow \\ &\quad \dim \operatorname{Span}(a_1(p), \ldots, a_{d(p)}(p), a_1(q), \ldots, a_{d(q)}(q)) = \\ &\quad \dim \operatorname{Span}(a_1(p), \ldots, a_{d(p)}(p), a_1(q), \ldots, a_{d(q)}(q), a(p) - a(q)). \end{aligned} \tag{13}$$

But the rank of a $d \times d$ matrix over a finite field can be computed by a Boolean circuit of depth $O((\log d)^2)$ (see [12]). Therefore, the fact (13) can be tested by a Boolean circuit of depth $O((\log d)^2)$ and this circuit also works in the graph complexity framework. ∎

Theorems 3.4, 3.5 and 3.7 together provide a new proof of the Theorem 3.3.

We conclude this section by discussing connections with the paper [18]. Let $BPP_{gr}(E)$ be the size of a minimal branching program (measured by the number of non-sink nodes) computing the graph E (the node questions to an input pair (p, q) are of the forms "$p \in P_0$?" or "$q \in Q_0$?" where P_0 and Q_0 are *arbitrary* subsets of P and Q). Then, just as in the Boolean case,

$$BPP_{gr}(E) \leqq L_{gr}(E). \tag{14}$$

The *projective dimension* $\operatorname{pdim}_{\mathcal{k}}(E)$ is defined like $\operatorname{adim}_{\mathcal{k}}(E)$ with the difference that $i(p)$ and $i(q)$ this time should be *linear* subspaces and $(p, q) \in E \Leftrightarrow i(p) \cap i(q) \neq \{0\}$.

P. Pudlak and V. Rödl showed that $\operatorname{adim}_{\mathcal{k}}(E) \leqq (\operatorname{pdim}_{\mathcal{k}}(E))^2$ for every field $\mathcal{k}$ and $\operatorname{adim}_{\mathcal{k}}(E) \leqq \operatorname{pdim}_{\mathcal{k}}(E) - 1$ if $\mathcal{k}$ is infinite. By methods entirely different from those of the present paper they proved

$$p \dim_{\mathcal{k}}(E) \leqq BPP_{gv}(E) + 2 \tag{15}$$

(actually P. Pudlak and V. Rödl stated this only for Boolean branching programs but their arguments can be straightforwardly extended for the graph complexity framework). So, the results from [18] imply $L_{gr}(E) \geqq (\operatorname{adim}_{\mathcal{k}}(E))^{1/2}$ for every field and $L_{gr}(E) \geqq \operatorname{adim}_{\mathcal{k}}(E) - 1$ if $\mathcal{k}$ is infinite which is only a little worse than our bound $L_{gr}(E) \geqq \operatorname{adim}_{\mathcal{k}}(E)$. An interesting corollary of Theorem 3.7 and results by P. Pudlak and V. Rödl is the following theorem.

Theorem 3.8. *For any finite field* $\mathcal{k}$,

$$\operatorname{p\,dim}_{\mathcal{k}}(E) \leqq \operatorname{adim}_{\mathcal{k}}(E)^{O(\operatorname{adim}_{\mathcal{k}}(E))}.$$

Proof. From (15), (14), $L_{gr}(E) \leqq \exp(O(D_{gr}(E))$ and Theorem 3.7. ∎

I do not know any purely combinatorial proof of the Theorem 3.8. Note also that, at least in this form, it is not true for infinite fields. Say, if E is the complement of an N to N matching then, as proved by L. Lovasz, $\mathrm{pdim}_{\mathcal{F}}(E) \geq \Omega(\log N)$ (for any field $\mathcal{F}$) but it is easy to see that $\mathrm{adim}_{\mathcal{F}}(E)=2$ if $\mathcal{F}$ is infinite.

4. Open questions

We do not present here obvious questions an answer to which would imply superpolynomial lower bounds for the formula size of explicitly given Boolean functions. Among others are the following two.

Question 4.1. What is the best lower bound for formula size over the standard basis with negation which could be obtained using Theorem 2.2? More precisely, let

$$B(n) = \max_{|\mathcal{R}|=2n} \max_{A} \left(\frac{\mathrm{rk}(A)}{\max\limits_{R \in \mathcal{R}} \mathrm{rk}(A_R)} \right),$$

where $\max\limits_{|\mathcal{R}|=2n}$ ranges over all self-complementary coverings of cardinality $2n$ and $\max\limits_{A}$ ranges over all non-zero matrices of the corresponding size over arbitrary fields. What is the magnitude of growth of the function $B(n)$? In particular, does $B(n)$ grow superpolynomially?[1]

Question 4.2. Can $D_{gr}(E)$ be nontrivially bounded from above in terms of N and $\mathrm{adim}_{\mathcal{F}}(E)$ for an infinite field $\mathcal{F}$? In particular, is it true that $D_{gr}(E)$ is polynomial in $\log\log N$ and $\log \mathrm{adim}_{\mathcal{F}}(E)$?

Acknowledgements. My thanks are due to P. Pudlak and P. Savicky for many helpful discussions. I am also grateful to all of the anonymous referees for many valuable remarks and suggestions.

References

[1] А. Е. Андреев, Об одном методе получения нижних оценок сложности индивидуальных монотонных функций — ДАН СССР, **1985**, т. 282, N5, 1033—1037. (Engl. transl. in: *Sov. Math. Dokl.*, **31**, 530—534.)

[2] А. Е. Андреев, Об одном методе получения эффективных нижних оценок монотонной сложности, Алгебра и логика, **1987**, т. 26, 1, с. 3—26.

[3] А. А. Разборов, Нижние оценки монотонной сложности некоторых булевых функций — ДАН СССР, **1985**, т. 281, N4, с. 798—801. (Engl. transl. in: *Sov. Math. Dokl.* **31**, 354—357.)

[4] А. А. Разборов, Нижние оценки монотонной сложности логического перманента — "Матем. зам.", **1985**, т. 37, вып. 6, с. 887—900. (Engl. transl. in: *Mathem. Notes of the Academy of Sci. of the USSR* **37**, 485—493.)

[5] А. А. Разборов, Нижние оценки размера схем ограниченной глубины в полном базисе, содержащем функцию логического сложения — *Матем. зам.*, **1987**, т. 41, вып. 4, с. 598—607. (Engl. transl. in: *Mathem. Notes of the Academy of Sci. of the USSR*, 41:4, 333—338.)

[6] А. А. Разборов, Формулы ограниченной глубины в базисе $\{\&, \oplus\}$ и некоторые комбинаторные задачи — в сб. «Вопросы кибернетики. Сложность вычислений и прикладная математическая логика», М.: **1988**, с. 149—166.

[1] Added in proof. Quite recently I was able to show that $B(n) \leq O(n)$.

[7] К. Л. Рычков, Модификация метода В. М. Храпченко и применение ее к оценкам сложности П-схем для кодовых функций — в сб. «Методы дискретного анализа в теории графов и схем», вып. 42, Новосибирск, **1985**, с. 91—98.
[8] В. М. Храпченко, О сложности реализации линейной функции в классе П-схем, *Матем. зам.*, **1971**, т. 9, вып. 1, с. 35—40. (Engl. transl. in: *Mathem. Notes of the Academy of Sci. of the USSR* **11** (1972), 474—479.)
[9] A. V. Aho, J. D. Ullman, M. Yannakakis, On Notions of Information Transfer in VLSI Circuits — *Proc. 15th ACM STOC*, **1983**, 133—139.
[10] N. Alon, R. B. Boppana, The monotone circuit complexity of Boolean functions, *Combinatorica*, **1987**, v. 7, N1, 1—22.
[11] L. Babai, P. Frankl, J. Simon, Complexity classes in communication complexity theory, *Proc. 27th IEEE FOCS*, **1986**, 337—347.
[12] A. Borodin, von zur Gathen, J. Hopcroft, Fast parallel matrix and GCD computations, *Information and Control*, **52** (1982), 241—256.
[13] B. Halsenberg, R. Reischuk, On Different Modes of Communication, 1988, 20th *ACM STOC*, 162—172.
[14] M. Karchmer, A. Wigderson, Monotone Circuits for Connectivity Require Super-logarithmic Depth, *Proc. 20th ACM STOC*, **1988**, 539—550.
[15] B. Lindström, H. O. Zetterström, A combinatorial problem in the k-adic number system, *Proc. of the Amer. Math. Soc.*, 1967, **18**, 1, 166—170.
[16] R. J. Lipton, R. Sedgewick, Lower Bounds for VLSI, *Proc. 13th ACM STOC*, **1981**, 300—307.
[17] K. Mehlhorn, E. M. Schmidt, Las Vegas is better than determinism in VLSI and distributive computing, *Proc. 14th ACM STOC*, **1982**, 330—337.
[18] P. Pudlak, V. Rödl, *A combinatorial approach to complexity*—unpublished manuscript, **1989**.
[19] P. Pudlak, V. Rödl, P. Savicky, Graph Complexity, *Acta Informatica*, **25** (1988), 515—535.
[20] P. M. Spira, On time-hardware complexity tradeoffs for Boolean functions, *Proceedings of 4th Hawaii Symposium on System Sciences*, **1971**, Western Periodicals Company, North Hollywood, 525—527.
[21] É. Tardos, The gap between monotone and non-monotone circuit complexity is exponential, *Combinatorica*, **1988**, v. 8, **1**, 141—142.
[22] I. Wegeher, Relating monotone formula size and monotone depth of Boolean functions, *Information Processing Letters*, **16**, (1983), 41—42.
[23] A. C. Yao, Some Complexity Questions Related to Distributed Computing, *Proc. 11th ACM STOC*, **1979**, 209—213.

A. A. Razborov

Steklov Mathematical Institute
Vavilova 42, 117966, GSP—1,
Moscow, USSR