On Submodular Complexity Measures

A. A. Razborov [*]

1. Introduction

In recent years several methods have been developed for obtaining superpolynomial lower bounds on the monotone formula and circuit size of explicitly given Boolean functions. Among these are the method of approximations [3, 4, 1, 7, 15, 2], the combinatorial analysis of a communication problem related to monotone depth [9, 12] and the use of matrices with very particular rank properties [13]. Now it can be said almost surely that each of these methods would need considerable strengthening to yield nontrivial lower bounds for the size of circuits or formulae over a complete basis. So, it seems interesting to try to understand from the formal point of view what kind of machinery we lack.

The first step in that direction was undertaken by the author in [14]. In that paper two possible formalizations of the method of approximations were considered. The restrictive version forbids the method to use extra variables. This version was proven to be practically useless for circuits over a complete basis. If extra variables are allowed (the second formalization) then the method becomes universal, i.e. for *any* Boolean function f there exists an approximating model giving a lower bound for the circuit size of f which is tight up to a polynomial. Then the burden of proving lower bounds for the circuit size shifts to estimating from below the minimal number of covering sets in a particular instance of *"MINIMUM COVER"*. One application of an analogous model appears in [5] where the first nonlinear lower bound was proven for the complexity of *MAJORITY* with respect to switching-and-rectifiers networks.

R. Raz and A. Wigderson in [11, 12] gave an indication that the communication problem of Karchmer and Wigderson [9] over the standard basis with negations also behaves very differently from its monotone analogue. Namely,

[*] Steklov Mathematical Institute, 117966, GSP-1, Vavilova, 42, Moscow, USSR

they showed that the probabilistic complexity of this problem for *any* specific Boolean function is $O(\log n)$ whereas the probabilistic complexity of the problem related to the *monotone* depth of *"PERFECT MATCHING"* is $\Omega(n)$.

In the present paper we study in this fashion the third method among those listed in the first paragraph, i.e. the method which relies upon constructing a matrix whose rank is much bigger than the ranks of certain submatrices of this matrix. We show that this method cannot even give nonlinear lower bounds over the standard basis with negations. This answers an open question from [13]. On the other hand we observe that if the matrix is allowed to be partial, then the method becomes very powerful.

Actually, we can treat a natural class of methods which contains the one from [13]. To say exactly what this class is, we recall (see e.g. [16, §8.8]) the notion of a formal complexity measure. Namely, a nonnegative real-valued function μ defined on the set of all Boolean functions in n variables is a *formal complexity measure*[1] if

$$\mu(x_i) \leq 1, \quad \mu(\neg x_i) \leq 1 \quad (1 \leq i \leq n); \tag{1}$$

$$\mu(f \vee g) \leq \mu(f) + \mu(g) \quad \text{for each } f, g; \tag{2}$$

and

$$\mu(f \wedge g) \leq \mu(f) + \mu(g) \quad \text{for each } f, g. \tag{3}$$

Restricting the domain of μ and arguments in (1-3) to the set of monotone functions, we obtain the definition of a *formal complexity measure on monotone functions.* Obvious induction shows that for any formal complexity measure μ we have $\mu(f) \leq L(f)$ ($L(f)$ is the formula size of f) and similarly for the monotone case. Actually, proofs of many known lower bounds on $L(f)$ can be viewed as inventing clever formal complexity measures which can be nontrivially bounded from below at some explicitly given Boolean functions (see e.g. the re-formulation of the Khrapchenko bound [6] given by M. Paterson [16, §8.8]).

We will see that the matrix method from [13] can also be easily reformulated in terms of formal complexity measures. Moreover, it turns out (Theorem 1 below) that the resulting measures μ satisfy the *submodularity condition*

$$\mu(f \wedge g) + \mu(f \vee g) \leq \mu(f) + \mu(g) \quad \text{for each } f, g \tag{4}$$

which is stronger than both (2) and (3). We call a formal complexity measure μ *submodular* if (4) holds and similarly for the monotone case. The results

[1] In this definition we have removed several unnecessary conditions from [16].

from [13] imply the existence of submodular formal complexity measures on monotone functions which take on values of size $n^{\Omega(\log n)}$.

The main result of this paper (Theorem 2) says that *all values of any submodular formal complexity measure* (on the set of *all* Boolean functions in n variables) *are bounded from above by* $O(n)$.

It is worth noting that the proof of Theorem 2 makes use of the same random circuit C which was previously used in the proof of Lemma 3.1 from [14] for breaking down the restrictive version of the method of approximations. It seems that this circuit can act as a hard test for different ideas aimed at proving lower bounds on the size of circuits or formulas over a complete basis.

2. Definitions and example of submodular complexity measures

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 $u \in B^n$, $1 \leq i \leq n$, u^i means the i^{th} bit in u. Let $X_i^\epsilon \rightleftharpoons \{u \in B^n | u^i = \epsilon\}$ for $1 \leq i \leq n$, $\epsilon \in \{0,1\}$. Given a variable x_i, set $x_i^1 \rightleftharpoons x_i$; $x_i^0 \rightleftharpoons (\neg x_i)$. Given $f \in F_n$, $U \subseteq B^n$, $\epsilon \in \{0,1\}$, the statement $\forall u \in U\ (f(u) = \epsilon)$ will be written in the simplified form $f(U) = \epsilon$. By a *formula* (over the standard basis) we mean an expression of the propositional calculus constructed (following the usual rules and conventions) from variables $x_1, x_2, ..., x_n$ with connectives $\vee$, $\wedge$, $\neg$; every formula $\phi(x_1, x_2, ..., x_n)$ 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., a formula in which negations occur only in the form $(\neg x_i)$) without increasing its size. Given $f \in F_n$, the *formula size* $L(f)$ is $\min\{s(\phi) | \phi$ computes $f\}$. A formula is *monotone* if it contains no negations at all; the *monotone formula size* $L_{\mathrm{mon}}(f)$ of an $f \in F_n^{\mathrm{mon}}$ is defined by analogy with $L(f)$.

We say that a function $\mu : F_n \longrightarrow \mathbf{R}^+$ is a *submodular formal complexity measure* (or *submodular complexity measure* for short) if it satisfies (1) and (4) (and hence also satisfies (2) and (3)). A function $\mu : F_n^{\mathrm{mon}} \longrightarrow \mathbf{R}^+$ is a *submodular complexity measure on* F_n^{mon} if it satisfies the first condition in (1) and satisfies (4) whenever $f, g \in F_n^{\mathrm{mon}}$. In the rest of the section we consider an example of submodular complexity measures.

Let $U, V \subseteq B^n$, $U \cap V = \varnothing$. 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 $\mathcal{R}$ of rectangles such that $\cup\mathcal{R} = U \times V$ will be called a *covering* (over U, V). The *canonical* covering $\mathcal{R}_{\mathrm{can}}(U, V)$ is defined as follows:

$$\mathcal{R}_{\mathrm{can}}(U, V) \rightleftharpoons \{R_{01}, R_{02}, \ldots, R_{0n}, R_{11}, R_{12}, \ldots, R_{1n}\}$$

$$\text{where } R_{\epsilon i} \rightleftharpoons (U \cap X_i^\epsilon) \times \left(V \cap X_i^{1-\epsilon}\right) \quad (1 \leq i \leq n, \epsilon \in \{0, 1\}).$$

By a *matrix over* U, V we mean a matrix over a field 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. The following result was proved in [13].

Proposition 1 [13] *For any $U, V \subseteq B^n$ and $f \in F_n$ such that $f(U) = 0$, $f(V) = 1$ and any non-zero matrix A over U, V (over an arbitrary field k), the inequality*

$$L(f) \geq \frac{\mathrm{rk}(A)}{\max\limits_{R \in \mathcal{R}_{\mathrm{can}}(U,V)} \mathrm{rk}(A_R)} \tag{5}$$

holds.

Let us understand that this lower bound is essentially the bound provided by a submodular complexity measure μ. For arbitrary $f \in F_n$, define the rectangle R_f over U, V by

$$R_f \rightleftharpoons \left(U \cap f^{-1}(0)\right) \times \left(V \cap f^{-1}(1)\right).$$

Let

$$\mu(f) \rightleftharpoons \frac{\mathrm{rk}(A_{R_f})}{\max\limits_{R \in \mathcal{R}_{\mathrm{can}}(U,V)} \mathrm{rk}(A_R)}.$$

Theorem 1 *a) μ is a submodular complexity measure;*
b) if $f(U) = 0$, $f(V) = 1$ then $\mu(f)$ equals the right-hand side of (5).

Proof : a) We have to check (1) and (4). (1) trivially follows from the definitions because if $f = x_i^\epsilon$ then $R_f = R_{i,1-\epsilon} \in \mathcal{R}_{\mathrm{can}}(U, V)$. For proving (4) consider the linear space k^U with the set U embedded into it as the basis. Using the matrix A we can also map V to k^U ($v \in V$ goes to the corresponding column of A). For $W \subseteq U \cup V$, denote by $\rho(W)$ the dimension of the subspace generated in k^U by the image of W via the mapping described. Then ρ is the rank function of a (linear) matroid on $U \cup V$ and hence is submodular. Now, $\mathrm{rk}(A_{R_f})$ can be expressed in the form

$$\mathrm{rk}(A_{R_f}) = \rho\left((U \cup V) \cap f^{-1}(1)\right) - |U \cap f^{-1}(1)|.$$

The submodularity of $\mathrm{rk}(A_{R_f})$ (and hence $\mu(f)$) follows from the submodularity of ρ.

b) is trivial. □

Similar results hold for the monotone case if we place on $U, V \subseteq B^n$ the restriction

$$\forall u \in U \, \forall v \in V \, \exists i \, (u^i = 0 \,\&\, v^i = 1)$$

(which is stronger than just $U \cap V = \varnothing$) and replace $\mathcal{R}_{\mathrm{can}}(U,V)$ by

$$\mathcal{R}_{\mathrm{mon}}(U,V) \rightleftharpoons \{R_{01}, R_{02}, \dots, R_{0n}\}.$$

It was shown in [13] that any 0-1 matrix A for which the rank lower bound of Mehlhorn and Schmidt [10] gives a *superlinear* gap between $\mathrm{DCC}(A)$ and $\max\,(\mathrm{NCC}(A), \mathrm{NCC}(\neg A))$ ($\mathrm{DCC}(A)$ and $\mathrm{NCC}(A)$ are deterministic and nondeterministic communication complexities of A respectively), can be used to construct a monotone Boolean function for which the monotone analogue of Proposition 1 gives a *superpolynomial* lower bound on its monotone formula size. In particular, the matrices presented in [10] lead to the bound $n^{\Omega(\log n / \log\log n)}$ and the matrices from [8] and [13] lead to the bound $n^{\Omega(\log n)}$. Applying the monotone analogue of Theorem 1, we obtain

Corollary 1 *There exist submodular complexity measures on F_n^{mon} which take on values of size at least $n^{\Omega(\log n)}$.*

3. Main result

The reader is invited to compare the following theorem (which is the main result of this paper) with Corollary 1 above and the proof of this theorem with the proof of Lemma 3.1 in [14].

Theorem 2 *For each submodular complexity measure μ (on F_n) and each $f_n \in F_n$ we have $\mu(f_n) \leq O(n)$.*

Proof : Let $\mathbf{g}_d$ be a random Boolean function in variables $x_1, \dots, x_d$. We are going to prove by induction on d that

$$\mathsf{E}\,[\mu(\mathbf{g}_d)] \leq d+1 \tag{6}$$

Base. $d = 1$. Here we have $\mu(g(x_1)) \leq 2$ for *any* $g(x_1)$. This follows from (1) if $g = x_1^\epsilon$. By (4) and (1) we have $\mu(0) + \mu(1) \leq \mu(x_1) + \mu(\neg x_1) \leq 2$ which proves $\mu(g(x_1)) \leq 2$ in the remaining case, when g is a constant.

Inductive step. Assume that (6) is already proved for d. Let the symbol $\approx$ mean that two random functions are equally distributed. Note that

$$\mathbf{g}_{d+1} \approx \left(\mathbf{g}_d^0 \wedge x_{d+1}^0\right) \vee \left(\mathbf{g}_d^1 \wedge x_{d+1}^1\right) \tag{7}$$

where $\mathbf{g}_d^0$ and $\mathbf{g}_d^1$ are two independent copies of $\mathbf{g}_d$. By duality,

$$\mathbf{g}_{d+1} \approx \left(\mathbf{g}_d^0 \vee x_{d+1}^0\right) \wedge \left(\mathbf{g}_d^1 \vee x_{d+1}^1\right) \tag{8}$$

From (7) and (2) (remember that the latter is a consequence of (4)!) we have

$$\mathsf{E}\left[\mu(\mathbf{g}_{d+1})\right] \leq \mathsf{E}\left[\mu\left(\mathbf{g}_d^0 \wedge x_{d+1}^0\right)\right] + \mathsf{E}\left[\mu\left(\mathbf{g}_d^1 \wedge x_{d+1}^1\right)\right] \tag{9}$$

and similarly from (8) and (3),

$$\mathsf{E}\left[\mu(\mathbf{g}_{d+1})\right] \leq \mathsf{E}\left[\mu\left(\mathbf{g}_d^0 \vee x_{d+1}^0\right)\right] + \mathsf{E}\left[\mu\left(\mathbf{g}_d^1 \vee x_{d+1}^1\right)\right]. \tag{10}$$

Summing (9), (10) and applying consecutively (4), (1) and the inductive assumption (6), we obtain

$$\begin{aligned}
2 \cdot \mathsf{E}\left[\mu(\mathbf{g}_{d+1})\right] &\leq \mathsf{E}\left[\mu\left(\mathbf{g}_d^0 \wedge x_{d+1}^0\right)\right] + \mathsf{E}\left[\mu\left(\mathbf{g}_d^0 \vee x_{d+1}^0\right)\right] + \\
&\quad\ \mathsf{E}\left[\mu\left(\mathbf{g}_d^1 \wedge x_{d+1}^1\right)\right] + \mathsf{E}\left[\mu\left(\mathbf{g}_d^1 \vee x_{d+1}^1\right)\right] \\
&\leq \mathsf{E}\left[\mu(\mathbf{g}_d^0)\right] + \mu(x_{d+1}^0) + \mathsf{E}\left[\mu(\mathbf{g}_d^1)\right] + \mu(x_{d+1}^1) \\
&\leq 2 \cdot \mathsf{E}\left[\mu(\mathbf{g}_d)\right] + 2 \\
&\leq 2d + 4.
\end{aligned}$$

The inductive step is completed and (6) is proved.

Now the given function $f_n \in F_n$ can be expressed in the form

$$f_n = (\mathbf{g}_n \wedge (\mathbf{g}_n \oplus f_n \oplus 1)) \vee ((\mathbf{g}_n \oplus 1) \wedge (\mathbf{g}_n \oplus f_n)). \tag{11}$$

But $\mathbf{g}_n \approx \mathbf{g}_n \oplus f_n \oplus 1 \approx \mathbf{g}_n \oplus 1 \approx \mathbf{g}_n \oplus f_n$. So, applying to (11) the inequalities (2) and (3), averaging the result over $\mathbf{g}_n$ and applying (6) with $d = n$, we prove the desired bound $\mu(f_n) \leq O(n)$. □

Theorems 1, 2 lead to the following result which shows the uselessness of Proposition 1 (unlike its monotone analogue!) for obtaining even superlinear lower bounds for the formula size over the standard basis with negations and resolves in the negative an open question from [13]:

Corollary 2 *For any $U, V \subseteq B^n$ such that $U \cap V = \emptyset$ and any non-zero matrix A over U, V (over an arbitrary field), the inequality*

$$\frac{\mathrm{rk}(A)}{\max_{R \in \mathcal{R}_{\mathrm{can}}(U,V)} \mathrm{rk}(A_R)} \leq O(n)$$

holds.

We conclude this paper with the following remark which is in a sense opposite to Corollary 2. Define a *partial matrix* over U, V to be an ordinary matrix over U, V with the exception that some entries can be left empty. The *rank* of a partial matrix A is the minimal rank of all possible full extensions of the partial matrix A. Proposition 1 can be strengthened by letting the matrix A be partial. Results contained in section 3 of the paper [13] imply that in this case the situation changes dramatically. Namely, the bound provided by the new version of Proposition 1 becomes almost universal in the context of graph complexity. If we prefer to stay in the Boolean framework, then we can claim (at least when the underlying field k is finite) that Proposition 1, applied to partial matrices A defined in the statement of Theorem 3.1 from [13], must provide exponential lower bounds for the formula size of almost all Boolean functions. Surely, the problem of getting actual lower bounds for $\mathrm{rk}(A)$ becomes extremely difficult in this context.

References

[1] **Андреев А. Е.** (1985) **Об одном методе получения нижних оценок сложности индивидуальных монотонных функций, ДАН СССР, т.** 282, **№** 5, **с.** 1033-1037. (Engl. transl. in: *Sov. Math. Dokl. 31, 530-534.*)

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

[3] **Разборов А. А.** (1985) **Нижние оценки монотонной сложности некоторых булевых функций, ДАН СССР, т.** 281, **№** 4, **с.** 798-801. (Engl. transl. in: *Sov. Math. Dokl. 31, 354-357.*)

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

[5] **Разборов А. А.** (1990) **Нижние оценки сложности реализации симметрических булевых функций контактно-вентильными шемами, Матем. зам. т.**48, **вып.** 6, **с.** 79-91.

[6] **Храпченко В. М.** (1971) **О сложности реализации линейной функции в классе П-схем, Матем. зам., т.** 9, **вып.** 1, **с.** 35-40. (Engl. transl. in: *Mathem. Notes of the Academy of Sci. of the USSR 11 (1972), 474-479.*)

[7] Alon N., Boppana R. B. (1987) The monotone circuit complexity of Boolean functions, Combinatorica, v. 7, 1, p. 1-22.

[8] Halsenberg B., Reischuk R. (1988) On Different Modes of Communication, Proc. 20th ACM STOC, p. 162-172.

[9] Karchmer M., Wigderson A. (1988) Monotone Circuits for Connectivity Require Super-logarithmic Depth, Proc. 20th ACM STOC, p. 539-550.

[10] Mehlhorn K., Schmidt E. M. (1982) Las Vegas is better than determinism in VLSI and distributive computing, Proc. 14th ACM STOC, p. 330-337.

[11] Raz R., Wigderson A. (1989) Probabilistic Communication Complexity of Boolean Relations, Proc. 30th IEEE FOCS, p. 562-567.

[12] Raz R., Wigderson A. (1990) Monotone Circuits for Matching Require Linear Depth, Proc. 22nd ACM STOC, p. 287-292.

[13] Razborov A. A. (1990) Applications of Matrix Methods to the Theory of Lower Bounds in Computational Complexity, Combinatorica v. 10, 1, p. 81-93.

[14] Razborov A. A. (1989) On the method of approximations, Proc. 21st ACM STOC, p. 167-176.

[15] Tárdos E. (1988) The gap between monotone and non-monotone circuit complexity is exponential, Combinatorica, v. 8, 1, p. 141-142.

[16] Wegener I. (1987) The Complexity of Boolean Functions, Wiley-Teubner.