An application of separability and independence notions for proving lower bounds of circuit complexity.

Dima Grigoriev

The author would like to acknowledge the advice of A. O. Slisenko and the valuable comments of S. V. Pakhomova, whichsubstantially improved the presentation.

LITERATURE CITED

1. A. N. Kolmogorov, "Onthe concept of an algorithm," Usp. Mat. Nauk, 8, No. 4(56), 175-176 (1953).
2. S. A. Cook and S. O. Aanderaa, "On the minimum computation time of functions," Trans. Am. Math. Soc., 142, 291-314 (1969).
3. M. S. Paterson, M. J. Fisher, and A. R. Meyer, "An improved overlap argument for on-line multiplication," SIAM-AMS Proc., Soc., 142, 291-314 (1969).
4. A. Schönhage, "Real time simulation of multidimensional Turing machines by storage modification machines," Proj. MAC Tech. Memo., No. 37 (1973).
5. F. Harary, Graph Theory, Addison-Wesley (1969).
6. F. C. Hennie, "On-line Turing machine computation," IEEE Trans. Electrical Comp., EC-15, 1, 35-44 (1966).

APPLICATION OF SEPARABILITY AND INDEPENDENCE NOTIONS FOR PROVING LOWER BOUNDS OF CIRCUIT COMPLEXITY

D. Yu. Grigor'ev

UDC 518.5:519.1

This note consists of two independent parts. In the first part the concept of an (m,c)-system for a set of linear forms is introduced, and a lower bound is obtained for the algebraic complexity of the computation of (m,c)-systems on algebraic circuits of a special form. In the second part, the notion of an l-independent set of boolean functions is introduced and a lower bound is obtained for a certain complexity measure for circuits of boolean functions computing l-independent sets. As a corollary it is shown that the standard algorithm for multiplying matrices or polynomials may be realized by a circuit of boolean functions in a way that is optimal with respect to a selected complexity measure.

In our paper two lower bounds on the complexity of computation of algebraic circuits (defined in [1], [2]) are obtained.

In Sec. 1 a lower bound is found for the computational complexity of a set of linear forms (Theorem 1). The second bound is given in Theorem 2 in Sec. 2. It follows from this theorem that the standard procedures formultiplying multiple-digit numbers and multiplying matrices modulo 2 are optimal in a certain sense.

1. Bounds for (m,c)-Systems of Linear Forms

1. In thissection wewill consider thequestion of the complexity of algebraic circuits for the simultaneous computation of a set of linear forms with complex coefficients in the variables $x_1,\dots,x_n$. A set of linear forms may be represented by the matrix of their coefficients, denoted A below, and the problem reduces to the problem of constructing a circuit for the calculation of the product AX where X is the vector of variables $x_1,\dots,x_n$.

Translated from Zapiski Nauchykh Seminarov Leningradskogo Otdeleniya Mathematicheskogo Instituta im. V. A. Steklova Akad. Nauk SSSR, Vol. 60, pp. 38-48, 1976. Main results presented December 12, 1974 and May 29, 1975.

 0090-4104/80/1405-1450$07.50

Morgenstern (in [3]) considered this problem when the elements of the circuit had the form

$$y_i = \alpha y_j + \beta y_k, \tag{1}$$

where α, β are complex coefficients satisfying the bounds

$$|\alpha| \le 1, \quad |\beta| \le 1, \tag{*}$$

and the variables y_j, y_k are either one of the variables $x_1, \ldots, x_n$ or the left side of one of the equations whose index is less than i. In [3] it is proved that the complexity of the circuits computing linear forms with the matrix of coefficients A, which is assumed to be square, exceeds $\lceil \lg_2 |\det A| \rceil$ ($[a]$ denotes the integer part of a, $\lceil a \rceil = -[-a]$).

The situation we consider is different from that in [3] in that below we consider a more restricted class of circuits and a narrower class of sets of linear forms to compute, but the lower bounds obtained are, generally speaking, stronger.

We represent each circuit by a directed graph G. To each variable y_i (variable x_j) corresponds a vertex Y_j (vertex X_i) of the graph G, i.e., G has $n+p$ vertices where p is the number of lines of the circuit. If y_i is represented in the form (1) then there is an edge from each of the vertices Y_j and Y_k to Y_i; i.e., G has $2p$ edges.

We assume that the calculation is carried out for m linear forms, which correspond to the vertices $a_1, \ldots, a_m$ of G.

For each l ($1 \le l \le m$) we let D_l denote the subgraph of G generated by the vertices from which there is a directed path to G in a_l.

From now on we consider circuits for which the corresponding graph G satisfies the following restriction:

for each l ($1 \le l \le m$) the graph D_l is a tree with a_l as its root. (**)

In distinction to the lower bounds on the complexity of circuits obtained by Morgenstern, the lower bounds found in this paper are for forms satisfying the following condition (the (m,c)-condition): for any subset J of $\{1, \ldots, m\}$ the distance (with respect to the norm l_1^n) between $\mathrm{Conv}\{A_i\}_{i \in J}$ and $\mathrm{Conv}\{A_j\}_{j \notin J}$ exceeds c, where A_i ($1 \le i \le m$) is a vector whose components are the coefficients of the linear forms being calculated (the vectors belong to n-dimensional real linear space) and Conv denotes "convex hull." We will say that in this case $A_1, \ldots, A_m$ form an (m,c)-system.

The main result, the theorem in Sec. 3, asserts that if the vectors, the rows of the matrix of coefficients, form an (m,c)-system, then the complexity of a circuit computing the linear forms with the given matrix of coefficient satisfying and restrictions (*) and (**), exceeds M, where M is the solution of the equation

$$\ln c + \frac{(m-6)(\log c - 1)}{4M} = \ln 4M$$

($\lg$ denotes logarithm to the base 2). This bound on M is interesting when $m^2 > c^2 > m$. In this case, the size of M is greater than

$$\frac{m \lg c}{8 \lg \frac{8 \lg c}{c}} \quad (m, c \ge 4).$$

If we use in placeof the norm l_1^n the l_2^n -Euclidean norm, then we can deduce this result using the method given in [3] (see also the remark following the statement of the theorem).

Note that in the case of complex coefficients the number of elements in the circuit is not increased more than 6 times, if one calculates separately the real and imaginary parts of each intermediate linear form.

2. We begin with two geometric lemmas.

LEMMA 1. Suppose that $A_1,\dots,A_k$ are points in n -dimensional real linear space $\mathbb{R}^n$, with $k \geq n+2$. Then these points may be divided into two disjoint sets such that the convex hulls of the two sets have a common point.

This lemma follows from Radon's theorem (see, e.g., [4], Proposition 3.10).

Let ρ_1 be the metric induced by the l_1^n norm. We say that the points $A_1,\dots,A_m$ form an (m,c) -system if

$$\forall I \ (I \subseteq \{1,\dots,m\} \Rightarrow \rho_1(\mathrm{Conv}\{A_i\}_{i\in I}, \mathrm{Conv}\{A_j\}_{j\notin I}) \geq c).$$

LEMMA 2. For any (m,c)-system and any plane in n -dimensional real linear space with dimension at most $[m/2-2]$, there are at least $\lceil m/2 \rceil$ points in the (m,c)-system such that the distance from each of these points to the plane is at least $c/2$.

Proof. Suppose that at least $[m/2]$ points of the given system have distance less than $c/2$ from the plane P. Denote these points by $A_1,\dots,A_l$ $(l \geq [m/2])$. Let the points on P closest to these points be $B_1,\dots,B_l$. Apply Lemma 1 to the points $B_1,\dots,B_l$. Suppose that B is the point whose existence is guaranteed by Lemma 1 and let $B = \sum_{i\in I}\alpha_i B_i = \sum_{j\notin I}\beta_j B_j$ where $\sum_{i\in I}\alpha_i = \sum_{j\notin I}\beta_j = 1$, $\alpha_i \geq 0$, $\beta_j \geq 0$ (the index set I exists by Lemma 1). Then

$$\rho_1\Big(\sum_{i\in I}\alpha_i B_i, \sum_{i\in I} A_i\alpha_i\Big) \leq \sum_{i\in I}\alpha_i \rho_1(A_i,B_i) < \frac{c}{2}\sum_{i\in I}\alpha_i = \frac{c}{2}.$$

From this it easily follows by the triangle inequality that the distance between the points $\sum_{i\in I}\alpha_i A_i$ and $\sum_{j\notin I}\beta_j A_j$ is less than c, which contradicts the (m,c)-condition. The lemma is proved.

3. We turn to the statement and proof of the theorem.

THEOREM 1. If the vectors whose components are the coefficients of the linear forms being computed form an (m,c) -system, then the number of elements of a circuit computing these forms satisfying the restrictions (*) and (**) is at least M , where M is the solution of the equation

$$\ln c + \frac{(m-6)\lg c/2}{4M} = \ln 4M.$$

Remark. In place of the norm l_1^n one may use any norm such that the norm of the vector $(\underbrace{0\dots1}_{i}\dots0)$ for any i is at most 1.

Proof. Consider a circuit computing our set of linear forms. For each linear form α let $\mathfrak{D}_i(\alpha)$ $(1 \leq i \leq m)$ denote the subtree of the binary tree $\mathfrak{D}_i$ (see Sec. 1) which consists of those forms which are used in the computation of the form α in the tree $\mathfrak{D}_i$, if α corresponds to one of the vertices of $\mathfrak{D}_i$, and which is the empty tree otherwise.

We denote the number of initial vertices (i.e., those vertices with no incoming edge) in a tree $\mathcal{D}$ by $V(\mathcal{D})$. Let C_1 be the greatest value of the sums $\sum_{j=1}^{m} V(\mathcal{D}_j(\alpha))$ for all forms α. Let α_{i_1} be a form such that $C_1 = \sum_{j=1}^{m} V(\mathcal{D}_j(\alpha_{i_1}))$. We define the new trees by: $\mathcal{D}_j^{(1)} = \mathcal{D}_j \setminus \mathcal{D}_j(\alpha_{i_1})$ $(1 \le j \le m)$. If the trees $\mathcal{D}_j^{(\kappa)}$, are defined, we let $C_{\kappa+1}$ be the greatest value of the sums $\sum_{j=1}^{m} V(\mathcal{D}_j^{(\kappa)}(\alpha))$. Let $\alpha_{\kappa+1}$ be a form such that $C_{\kappa+1} = \sum_{j=1}^{m} V(\mathcal{D}_j^{(\kappa)}(\alpha_{\kappa+1}))$. We now let $\mathcal{D}_j^{(\kappa+1)} = \mathcal{D}_j^{(\kappa)} \setminus \mathcal{D}_j^{(\kappa)}(\alpha_{i_{\kappa+1}})$.

It is easy to see that $C_1 \ge C_2 \ge \dots$. Consider $\mathcal{D}_j^{(\theta)}$ $(1 \le j \le m)$, where $\theta = \lceil m/2 \rceil - 2$. We write each of the m forms $A_1, \dots, A_m$ being computed in the form $A_\kappa = \left(\sum_{j=1}^{\theta} \beta_{\kappa j} \cdot \alpha_j\right) + B_\kappa$ where $l(B_\kappa)$ is least, deleting from $\mathcal{D}_\kappa$ all vertices α_j $(1 \le j \le \theta)$ and writing in the left summand of the right half of this equation all of these forms ($\beta_{\kappa j}$ are certain complex numbers).

We now apply Lemma 2, taking as the plane of dimension at most θ the plane spanned by $\alpha_1, \dots, \alpha_\theta$ and as the (m, c)-system the forms $A_1, \dots, A_m$ being computed. Then by Lemma 2 at least half of the vectors $B_1, \dots, B_m$ will have norm at least $c/2$ (suppose these are $B_1, \dots, B_l$ $(l \ge \frac{m}{2})$), and hence by (*) at least $\lceil m/2 \rceil$ of the sets $\mathcal{D}_1^{(\theta)}, \dots, \mathcal{D}_m^{(\theta)}$ will contain at least $c/2$ elements corresponding to the variables $X_1, \dots, X_n$ (the initial vertices).

Let $M_\kappa = \sum_{l=\kappa+1}^{\theta} C_l + \frac{mc}{4}$. Note that

$$M_\kappa \le \sum_{j=1}^{m} V(\mathcal{D}_j^{(\kappa)}) \le 2 \sum_{j=1}^{l_\kappa} V(\mathcal{D}_{p_j}^{(\kappa)}),$$

where $p_1, \dots, p_{l_\kappa}$ are numbers such that $V(\mathcal{D}_{p_j}^{(\kappa)}) \ge \frac{c}{2}$ (since as proved above $l_\kappa \ge \frac{m}{2}$).

Consider the following system of inequalities:

$$\begin{cases} C_\kappa \ge \dfrac{M_\kappa \lg_2 c/2}{2M} & \kappa = 1, \dots, \theta-1 \\ C_\theta \ge \dfrac{mc}{4} \dfrac{\lg_2 c/2}{2M} \end{cases} \qquad (***)$$

Suppose that for some $\kappa_0 = 1, \dots, \theta$ we have

$$C_{\kappa_0} < \frac{M_{\kappa_0} \lg_2 c/2}{2M}. \qquad (2)$$

The following fact is well known from coding theory:

(A) Suppose one associates with each vertex of a binary tree with n initial vertices, directed from the initial vertices to the root, the number of initial vertices above it. Then the sum of all these values is at least $n \lg_2 n$.

Remark. The statement (A) remains true if one assumes that one edge may enter a vertex of the tree.

We summarize now the inequalities obtained by applying the statement (A) (with the accompanying remark) to all of the trees $\mathcal{D}_1^{(\kappa_0)}, \dots, \mathcal{D}_m^{(\kappa_0)}$. We obtain

$$\sum_{j=1}^{m} \sum_{\alpha} V(\mathcal{D}_j^{(\kappa_0)}(\alpha)) \ge \sum_{j=1}^{l_{\kappa_0}} V(\mathcal{D}_{p_j}^{(\kappa_0)}) \lg V(\mathcal{D}_{p_j}^{(\kappa_0)}).$$

Obviously

$$C_{\kappa_0} \geqslant \sum_{j=1}^{m} V\left(\mathcal{D}_j^{(\kappa_0)}(\alpha)\right)$$

for any α. We obtain the final chain of inequalities

$$z \cdot C_{\kappa_0} \geqslant \sum_{j=1}^{m} \sum_{\alpha} V\left(\mathcal{D}_j^{(\kappa_0)}(\alpha)\right) \geqslant \sum_{j=1}^{\ell_{\kappa_0}} V\left(\mathcal{D}_{p_j}^{(\kappa_0)}\right) \lg_2 V\left(\mathcal{D}_{p_j}^{(\kappa_0)}\right) \geqslant \lg_2 c/2 \sum_{j=1}^{\ell_{\kappa_0}} V\left(\mathcal{D}_{p_j}^{(\kappa_0)}\right) > \lg c/2 \cdot M_{\kappa_0}/2 ,$$

where z is the number of elements of the circuit being evaluated. Using the last inequality (2), we have shown finally that $z \geqslant M$.

The same result holds if we add the assumption $C_\theta < \frac{mc}{4} \cdot \frac{\lg_2 c/2}{2M}$ (the proof is practically unchanged).

It remains to consider the case when the inequalities (***) hold.

In order to do this, we need statement (B), which is easily proved by induction on κ.

(B) Suppose $f \geqslant 0$ and $0 < a_0 \leqslant a_1 \leqslant \ldots$ are such that for any ℓ $a_{\ell+1} \geqslant f \cdot \sum_{i=0}^{\ell} a_i$. Then $a_{\kappa+1} \geqslant a_0 (1+f)^\kappa f$ $(\kappa \geqslant 0)$.

We apply (B) when $a_0 = mc/4$, $a_1 = c_\theta, \ldots, a_\theta = c_1 f = \frac{\lg_2 c/2}{2M}$. The hypothesis of (B) holds according to (***). We have the following chain of inequalities:

$$\sum_{i=1}^{\theta} c_i \geqslant \frac{mc}{4} \frac{\lg_2 c/2}{2M} \sum_{\kappa=0}^{\theta-1} \left(1 + \frac{\lg_2 c/2}{2M}\right)^\kappa \geqslant \frac{mc}{4} \frac{\lg_2 c/2}{2M} \frac{\left(1 + \frac{\lg_2 c/2}{2M}\right)^{m/2-3}}{(\lg_2 c/2)/2M} \geqslant \frac{mc}{4} e^{(m/2-3)\frac{\lg c/2}{2M}} = Mm.$$

Note also that $\sum_{j=1}^{m} V(\mathcal{D}_j)$ is greater than $\sum_{i=1}^{\theta} c_i$ and on the other hand it is bounded above by $z \cdot m$. Thus,

$$z \cdot m \geqslant \sum_{j=1}^{m} V(\mathcal{D}_j) \geqslant M \cdot m$$

and finally $z \geqslant M$. The theorem is proved.

4. We make several concluding remarks. In the special case $m = c$, the order of magnitude of M is

$$\frac{m \lg_2 m}{\lg_2 \lg_2 m} ,$$

which represents a nontrivial bound.

One may reduce the construction of a circuit for the calculation of the values of polynomials at a fixed set of points to the calculation of a set of linear forms. One may also reduce to this problem the problem of calculating the product of arbitrary matrices over some constants.

It is easy to see from the proof of the theorem that the form of the functions being computed (in our case, the linear forms) was used only in section 2 in the proof of Lemma 2. If one introduces in an appropriate way some functional (similar to our norm l_1^n) and proves for the set of functions being computed (for example, bilinear forms) an analogue of Lemma 2, thenone may obtain a lower bound for the number of elements in a circuit computing these

functions by using the method described in the proof of the theorem in section 3.

By means of a strengthening of statement (A) above, one may eliminate the restriction (**) in the statement of Theorem 1.

2. Bounds for Sets of Independent Boolean Functions

In this section the problem of calculating a set of boolean functions is considered, actually with the aid of a circuit of functional elements. But since certain special characteristics of the complexity of circuits are of interest to us, another concept will be described: circuits with registers.

We fix a finite set of boolean functions $\{h_j\}$; we let κ_j denote the arity (the number of arguments) of the function h_j.

A circuit with registers $\{y_i\}_{i=1}^{L}$, where each of $y_1,\dots,y_L$ is a variable, on the basis $\{h_j\}$ with variables $x_1,\dots,x_n$ is a sequence of T lines of the form

$$y_p \longleftarrow h_s(z_{j_1},\dots,z_{j_{\kappa_s}}), \tag{1}$$

where h_s is a function in the basis, z_{j_f} is either one of the variables $x_1,\dots,x_n$ or one of the registers y_i, where i is less than p. (The number L is the register size of the circuit.)

We now define the value of the register y_i at line l by induction on l. The values is a boolean function of the variables $x_1,\dots,x_n$, which is denoted val$[y_i,l]$.

Suppose the line with number l has the form (1). Then a) if $l \geq 2$, val $[y_\nu,l]$= val $[y_\nu,l-1]$ $(\nu \neq p)$ and val $[y_p,l]=h_s$ (val $[z_{j_1},l-1],\dots,$ val; $[z_{j_{\kappa_s}},l-1]$); b) if $l=1$, we set val $[y_i,1]=0$ $(i>1)$, val $[y_1,1]=h_s(z_{j_1},\dots,z_{j_{\kappa_s}})$; and also val $[x_i,\kappa]=x_i$ for all i,κ.

A set of boolean functions $Y_1,\dots,Y_m$ is computable by the given circuit if for all i $(1\leq i\leq m)$ there are κ,l such that (val$[y_\kappa,l]=Y_i$).

From a circuit with T lines, one may construct a circuit with functional elements on the basis $\{h_j\}$, having T elements.

We note moreover that the circuits described above are in fact RAM (random access machines) with commands of the form

$$R_p \longleftarrow h_s(R_{j_1},\dots,R_{j_{\kappa_s}})$$

with register size L, the number of registers used; T is the number of lines of the program and clearly also the time of computation of the RAM.

Suppose the circuit computes the boolean functions $Y_1,\dots,Y_m$ of the variables $x_1,\dots,x_n$. Below we will consider the finite set of all boolean vectors of length n (denoted B^n). We introduce the following notation: If $A_1,\dots,A_\kappa$ are subsets of B^n, then $\mathfrak{D}(A_1,\dots,A_\kappa)$ denotes the 2^κ subsets of B^n (forming a partition) of the form $\varepsilon_1 A_1 \cap \dots \cap \varepsilon_\kappa A_\kappa$ where ε_i is either C or the empty word, and CA denotes the complement of A.

The restriction of a partition A to the set X, denoted A/X, is the collection of sets of the form $A_i \cap X$ where A_i are the elements of the partition A.

We associate with each boolean function f the set of boolean vectors on which it has the value 0. We denote this set $\hat{f}$.

We will say that a set of boolean functions $Y_1,\ldots,Y_m$ is ℓ-independent with respect to the set of variables $x_1,\ldots,x_n$ if for all κ not exceeding ℓ and for all subsets $X_{i_1},\ldots,X_{i_\kappa}$ and $Y_{j_1},\ldots,Y_{j_{\ell-\kappa}}$ there is an χ in $\mathfrak{D}(\hat{X}_{i_1},\ldots,\hat{X}_{i_\kappa})$ such that $\mathfrak{D}(\hat{Y}_{j_1},\ldots,\hat{Y}_{j_{\ell-\kappa}})/\chi$ contains at least $2^{\ell-\kappa-1}+1$ nonempty distinct subsets. Further, we will write $A \leqslant B$ if each set of the partition A is the union of some sets of the partition B.

We note that if the set $Y_1,\ldots,Y_m$ is ℓ-independent with respect to $X_1,\ldots,X_n$, then it is also p-independent, where $p \leqslant \ell$. Thus $Y_1,\ldots,Y_m$ are pairwise distinct.

We now state and prove the main theorem of this section.

THEOREM 2. If a circuit with L registers and T lines computes a set $Y_1,\ldots,Y_m$, which is ℓ-independent with respect to the input circuits $X_1,\ldots,X_n$, then $TL \geqslant m\ell/4\kappa_0$, where κ_0 is the greatest arity of the basis functions.

Proof. Let $a(1),\ldots,a(m)$ be the numbers of the lines, in increasing order, in which the inputs of the circuits $Y_1,\ldots,Y_m$ are computed. Consider the lines from $a(i)$ to $a(i+L)$. Suppose $X_{j_1},\ldots,X_{j_p}$ are the inputs which the circuit operates on in this interval. We will prove that $p \geqslant \ell - L$. Suppose that $p < \ell - L$.

According to the definition of ℓ-independence, for the given sets $X_{j_1},\ldots,X_{j_p}$ and $Y_i,\ldots,Y_{i+L}$ there is an X in $\mathfrak{D}(\hat{X}_{j_1},\ldots,\hat{X}_{j_p})$ which divides the sets $\hat{Y}_i,\ldots,\hat{Y}_{i+L}$ into more than 2^L nonempty sets.

Let $A_1,\ldots,A_L$ denote the boolean functions $\operatorname{val}[y_i, a(i)],\ldots,\operatorname{val}[y_i, a(i)]$. Since the set $Y_i,\ldots,Y_{i+L}$ is defined by the sets $X_{j_1},\ldots,X_{j_p}$ and $A_1,\ldots,A_L$, then $\mathfrak{D}(\hat{Y}_i,\ldots,\hat{Y}_{i+L}) \leqslant \mathfrak{D}(\hat{X}_{j_1},\ldots,\hat{X}_{j_p},\hat{A}_1,\ldots,\hat{A}_L)$.

From this fact it follows that

$$\mathfrak{D}(\hat{Y}_i,\ldots,\hat{Y}_{i+L})/\chi \leqslant$$

$$\mathfrak{D}(\hat{X}_{j_1},\ldots,\hat{X}_{j_p},\hat{A}_1,\ldots,\hat{A}_L)/\chi = \mathfrak{D}(\hat{A}_1,\ldots,\hat{A}_L)/\chi,$$

but this last partition consists of at most 2^L sets, which contradicts ℓ-independence. Thus $p \geqslant \ell - L$. If $L \geqslant \ell/2$, then since $T \geqslant m$, we have $TL \geqslant m\ell/2$ and everything is proved. is proved. If however $L \leqslant \ell/2$, then $\ell - L \geqslant \ell/2$. From the above argument it follows that $a(i+L) - a(i) \geqslant \ell/2\kappa_0$, since between the lines numbered $a(i)$ and $a(i+L)$ the inputs are transformed at least $\ell/2$ times and the greatest arity of the basis functions is κ_0. Thus,

$$T \geqslant (a(L+1)-a(1)) + (a(2L+1)-a(L+1)) + \ldots$$

$$+ \left(a([m/L]L+1) - a(([m/L]-1)L+1)\right) \geqslant [m/L]\,\ell/2\kappa_0 \geqslant \frac{m}{2L}\,\frac{\ell}{2\kappa_0}$$

(supposing $L \leqslant m$; if $L \geqslant m$, we have the bound $TL \geqslant m\ell$, since m is not less than ℓ, as is easily seen, and $T \geqslant m$). The theorem is proved.

As corollaries we obtain, for example: the fact that in a circuit for multiplying mod 2 two $n \times n$ matrices (i.e., in the circuit which computes, given the elements of the factor matrices, the elements of their product) the product TL exceeds $n^3/4\kappa_0$; the fact that in a circuit for multiplying mod 2 two polynomials of degree n, or natural numbers whose binary

representation has length n, $TL \geq n^2/4\kappa_0$. We note that these bounds are exact. In order to prove this, it is sufficient to apply the standard procedures (for matrices this may be done with a circuit with the parameters $L=3$, $T=2n^3$, $\kappa_0=2$).

We observe that a condition sufficient for the ℓ-independence of a set of boolean functions $Y_1,\ldots,Y_m$ with respect to a set of variables $X_1,\ldots,X_n$ may be stated using the language of entropy (see [5]):

for any κ $(1\leq\kappa\leq\ell)$ and for any sets $i_1,\ldots,i_\kappa$ and $j_1,\ldots,j_{\ell-\kappa}$ the inequality

$$H(\mathcal{D}(\hat{Y}_{i_1},\ldots,\hat{Y}_{i_\kappa})/\mathcal{D}(\hat{X}_{j_1},\ldots,\hat{X}_{j_{\ell-\kappa}}))>\kappa-1$$

holds, where H is the conditional entropy.

The author would like to express his deep appreciation to A. O. Slisenko for his help.

LITERATURE CITED

1. V. Strassen, "Berechnung und Programm I," Acta Informatica, No. 1, 320-335 (1972).
2. V. Ya. Pan, "Special computations of values of polynomials," Usp.Mat. Nauk, 21, No. 1 (127), 103-134 (1966).
3. J. Morgenstern, "Note on a lower bound of the linear complexity of the fast Fourier transformation," J. Assoc. Comput. Mach., 20, No. 2, 305-306 (1973).
4. L. Danzer, B. Grunbaum, and V. Klee, "Helly's theorem and its relatives" Am.Math. Soc., Providence, Rhode Island (1963).
5. P. Billingsley, Ergodic Theory and Information, Wiley, New York—London—Sydney (1965).

ON AN APPROXIMATIVE VERSION OF THE NOTION OF CONSTRUCTIVE ANALYTIC FUNCTION

E. Ya. Dantsin

UDC 51.01

A constructive analytic function f is defined as a pair of form (A,Ω), where A is a fundamental sequence in some constructive metric space and Ω is a regulator of its convergence into itself. The pointwise-defined function f corresponding to function f^* turns out to be Bishop-differentiable [2], while the domain of f^* is the limit of a growing sequence of compacta. The derivative of a constructive analytic function and the integral along a curve are defined approximatively. It is proved that the fundamental theorems of constructive complex analysis are valid for such functions. Eight items of literature are cited.

INTRODUCTION

In the literature on constructive mathematics there are a number of papers in which various constructive analogs of an analytic function of a complex variable are investigated

Translated from Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova Akad. Nauk SSSR, Vol. 50, pp. 49-58, 1976. Result announced November 1, 1973.

0090-4104/80/1405-1457$07.50