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 $\ell$ -independent set of boolean functions is introduced and a lower bound is obtained for a certain complexity measure for circuits of boolean functions computing $\ell$ -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 $x_1,...,x_n$ . 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 $x_1,...,x_n$.

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

$$y_i = \alpha y_j + \beta y_\kappa,$$

(1)

where $\alpha$, $\beta$ are complex coefficients satisfying the bounds

$$|\alpha| \leq 1, \quad |\beta| \leq 1,$$

(*)

and the variables $y_j$, $y_\kappa$ 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 $\lceil \log_2 |\det A| \rceil$ ($\lfloor \alpha \rfloor$ denotes the integer part of $\alpha$, $\lceil \alpha \rceil = -\lfloor -\alpha \rfloor$).

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 $Y_\kappa$ 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 $\ell$ ($1 \leq \ell \leq m$) we let $D_\ell$ denote the subgraph of $G$ generated by the vertices from which there is a directed path to $G$ in $a_\ell$.

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

for each $\ell$ ($1 \leq \ell \leq m$) the graph $D_\ell$ is a tree with $a_\ell$ 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 $\ell_1^n$) between $\text{Conv}\{A_i\}_{i \in J}$ and $\text{Conv}\{A_j\}_{j \in J}$ exceeds $c$, where $A_i$ ($1 \leq i \leq m$) 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

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

($\log$ 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

$$\frac{m \log c}{8 \log \frac{m \log c}{c}} \qquad (m, c \geq 4).$$

If we use in place of the norm $\ell_1^n$ the $\ell_2^n$ -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 $A_1,\ldots,A_\kappa$ are points in $n$ -dimensional real linear space $\mathbb{R}^n$, with $\kappa \geqslant n+2$ . 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 $\rho_1$ be the metric induced by the $\ell_1^n$ norm. We say that the points $A_1,\ldots,A_m$ form an $(m,c)$ -system if

$$\forall I \ (I \subseteq \{1,\ldots,m\} \Longrightarrow \rho_1(\text{Conv}\{A_i\}_{i \in I}, \text{Conv}\{A_j\}_{j \notin I}) \geqslant c).$$

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 $A_1,\ldots,A_\ell$ ( $\ell \geqslant [m/2]$ . Let the points on $P$ closest to these points be $B_1,\ldots,B_\ell$ . Apply Lemma 1 to the points $B_1,\ldots,B_\ell$ . 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 $\sum_{i \in I} \alpha_i = \sum_{j \notin I} \beta_j = 1$, $\alpha_i \geqslant 0$, $\beta_j \geqslant 0$ (the index set $I$ exists by Lemma 1). Then

$$\rho_1\left(\sum_{i \in I} \alpha_i B_i, \sum_{i \in I} A_i \alpha_i\right) \leqslant \sum_{i \in I} \alpha_i \rho_1(A_i, B_i) \leqslant \frac{c}{2} \sum_{i \in I} \alpha_i = \frac{c}{2}.$$

From this it easily follows by the triangle inequality that the distance between the points $\sum_{i \in I} \alpha_i A_i$ and $\sum_{j \in I} \beta_j A_j$ 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 $\ell_1^n$ one may use any norm such that the norm of the vector $(0\ldots\underset{i}{1}\ldots 0)$ for any $i$ is at most 1.

Proof. Consider a circuit computing our set of linear forms. For each linear form $\alpha$ let $\mathcal{D}_i(\alpha)$ ( $1 \leqslant i \leqslant m$ ) denote the subtree of the binary tree $\mathcal{D}_i$ (see Sec. 1) which consists of those forms which are used in the computation of the form $\alpha$ in the tree $\mathcal{D}_i$, if $\alpha$ corresponds to one of the vertices of $\mathcal{D}_i$ , 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 $\alpha$. Let $\alpha_1$ be a form such that $C_1 = \sum_{j=1}^{m} V(\mathcal{D}_j(\alpha_1))$. 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 $\mathcal{D}_j^{(K)}$, are defined, we let $C_{K+1}$ be the greatest value of the sums $\sum_{j=1}^{m} V(\mathcal{D}_j^{(K)}(\alpha))$. Let $\alpha_{K+1}$ be a form such that $C_{K+1} = \sum_{j=1}^{m} V(\mathcal{D}_j^{(K)}(\alpha_{K+1}))$. We now let $\mathcal{D}_j^{(K+1)} = \mathcal{D}_j^{(K)} \setminus \mathcal{D}_j^{(K)}(\alpha_{i_{K+1}})$

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 $A_K = \left( \sum_{i=1}^{\theta} \beta_{K,j} \cdot \alpha_j \right) + B_K$ where $\ell_1^n(B_K)$ is least, deleting from $\mathcal{D}_K$ all vertices $\alpha_j$ $(1 \le j \le \theta)$ and writing in the left summand of the right half of this equation all of these forms $(\beta_{K,j}$ are certain complex numbers).

We now apply Lemma 2, taking as the plane of dimension at most $\theta$ 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 $B_1, \dots, B_\ell$ ( $\ell \ge \frac{m}{2}$ )), 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 $M_K = \sum_{\ell=K+1}^{\theta} C_\ell + \frac{mc}{4}$. Note that

$$M_K \le \sum_{j=1}^{m} V(\mathcal{D}_j^{(K)}) \le 2 \sum_{j=1}^{\ell_K} V(\mathcal{D}_{P_j}^{(K)}),$$

where $P_1, \dots, P_{\ell_K}$ are numbers such that $V(\mathcal{D}_{P_j}^{(K)}) \ge \frac{C}{2}$ (since as proved above $\ell_K \ge \frac{m}{2}$ ).

Consider the following system of inequalities:

$$\begin{cases} C_K \ge \dfrac{M_K \, \ell g_2 \, C/2}{2M} & K = 1, \dots, \theta-1 \\[2mm] C_\theta \ge \dfrac{mc}{4} \, \dfrac{\ell g_2 \, C/2}{2M} \end{cases} \qquad (***)$$

Suppose that for some $K_0 = 1, \dots, \theta$ we have

$$C_{K_0} < \frac{M_{K_0} \, \ell g_2 \, C/2}{2M}. \qquad (2)$$

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 $n \, \ell g_2 \, n$.

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 $\mathcal{D}_1^{(K_0)}, \dots, \mathcal{D}_m^{(K_0)}$. We obtain

$$\sum_{j=1}^{m} \sum_{\alpha} V(\mathcal{D}_j^{(K_0)}(\alpha)) \ge \sum_{j=1}^{\ell_{K_0}} V(\mathcal{D}_{P_j}^{(K_0)}) \, \ell g \, V(\mathcal{D}_{P_j}^{(K_0)}).$$

Obviously

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

for any $\alpha$. We obtain the final chain of inequalities

$$z \cdot C_{\kappa_0} \geqslant \sum_{j=1}^{m} \sum_{\alpha} V(\mathcal{D}_j^{(\kappa_0)}(\alpha)) \geqslant \sum_{j=1}^{\ell_{\kappa_0}} V(\mathcal{D}_{p_j}^{(\kappa_0)}) \ell g_2 V(\mathcal{D}_{p_j}^{(\kappa_0)}) \geqslant \ell g_2 {}^C/_2 \sum_{j=1}^{\ell_{\kappa_0}} V(\mathcal{D}_{p_j}^{(\kappa_0)}) > \ell g {}^C/_2 \cdot M_{\kappa_0}/2 \ ,$$

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 $C_\theta < \dfrac{mc}{4} \cdot \dfrac{\ell g_2 {}^C/_2}{2M}$ (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 $\kappa$.

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

We apply (B) when $a_0 = {}^{mc}/_4$, $a_1 = C_\theta, \dots, a_\theta = C_1, f = \dfrac{\ell g_2 {}^C/_2}{2M}$. The hypothesis of (B) holds according to (***). We have the following chain of inequalities:

$$\sum_{i=1}^{\theta} c_i \geqslant \frac{mc}{4} \frac{\ell g_2 {}^C/_2}{2M} \sum_{\kappa=0}^{\theta-1} \left(1 + \frac{\ell g_2 {}^C/_2}{2M}\right)^\kappa \geqslant \frac{mc}{4} \frac{\ell g_2 {}^C/_2}{2M} \frac{\left(1 + \frac{\ell g_2 {}^C/_2}{2M}\right)^{m/2-3}}{(\ell g_2 {}^C/_2)/2M} \geqslant \frac{mc}{4} e^{(m/2-3)\frac{\ell g {}^C/_2}{2M}} = Mm.$$

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

$$\frac{m \, \ell g_2 m}{\ell g_2 \ell g_2 m} \ ,$$

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 $\ell_1^n$) and proves for the set of functions being computed (for example, bilinear forms) an analogue of Lemma 2, then one 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 $\kappa_j$ denote the arity (the number of arguments) of the function $h_j$.

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

$$y_p \longleftarrow h_s(z_{j_1}, \ldots, z_{j\kappa_s}), \tag{1}$$

where $h_s$ is a function in the basis, $z_{jf}$ is either one of the variables $x_1, \ldots, x_n$ 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 $\ell$ by induction on $\ell$. The value is a boolean function of the variables $x_1, \ldots, x_n$, which is denoted $val[y_i, \ell]$.

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

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

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

$$R_p \longleftarrow h_s(R_{j_1}, \ldots, R_{j\kappa_s})$$

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 $Y_1, \ldots, Y_m$ of the variables $x_1, \ldots, x_n$. Below we will consider the finite set of all boolean vectors of length $n$ (denoted $B^n$). We introduce the following notation: If $A_1, \ldots, A_\kappa$ are subsets of $B^n$ , then $\mathcal{D}(A_1, \ldots, A_\kappa)$ denotes the $2^\kappa$ subsets of $B^n$ (forming a partition) of the form $\varepsilon_1 A_1 \cap \ldots \cap \varepsilon_\kappa A_\kappa$ where $\varepsilon_i$ 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 $\ell$-independent with respect to the set of variables $x_1, \ldots, x_n$ if for all $\kappa$ not exceeding $\ell$ and for all subsets $X_{i_1}, \ldots, X_{i_\kappa}$ and $Y_{j_1}, \ldots, Y_{j_{\ell-\kappa}}$ there is an $\chi$ in $\mathcal{D}(\hat{X}_{i_1}, \ldots, \hat{X}_{i_\kappa})$ such that $\mathcal{D}(\hat{Y}_{j_1}, \ldots \hat{Y}_{j_{\ell-\kappa}})/\chi$ 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 $\ell$-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.

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

<u>Proof.</u> Let $\alpha(1), \ldots, \alpha(m)$ 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 $\alpha(i)$ to $\alpha(i+L)$. 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 $\ell$-independence, for the given sets $X_{j_1}, \ldots, X_{j_p}$ and $Y_i, \ldots, Y_{i+L}$ there is an $\chi$ in $\mathcal{D}(\hat{X}_{j_1}, \ldots, \hat{X}_{j_p})$ 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 val $[y_1, \alpha(i)], \ldots$ val $[y_L, \alpha(i)]$. 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 $\mathcal{D}(\hat{Y}_i, \ldots, \hat{Y}_{i+L}) \leqslant \mathcal{D}(\hat{X}_{j_1}, \ldots, \hat{X}_{j_p}, \hat{A}_1, \ldots, \hat{A}_L)$.

From this fact it follows that

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

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

but this last partition consists of at most $2^L$ sets, which contradicts $\ell$-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 $\alpha(i+L) - \alpha(i) \geqslant {}^{\ell}/_{2\kappa_0}$, since between the lines numbered $\alpha(i)$ and $\alpha(i+L)$ the inputs are transformed at least ${}^{\ell}/_2$ times and the greatest arity of the basis functions is $\kappa_0$. Thus,

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

$$+ (\alpha([{}^m/_L]L+1) - \alpha(([{}^m/_L]-1)L+1)) \geqslant [{}^m/_L]\,{}^{\ell}/_{2\kappa_0} \geqslant \frac{m}{2L}\,\frac{\ell}{2\kappa_0}$$

(supposing $L \leqslant m$; if $L \geqslant m$, we have the bound $TL \geqslant m\ell$, since $m$ is not less than $\ell$, 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 $\ell$ -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 $\kappa (1 \leq \kappa \leq \ell)$ and for any sets $i_1, \ldots, i_\kappa$ and $j_1, \ldots, j_{\ell-\kappa}$ the inequality

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

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 $(A, \Omega)$, where $A$ is a fundamental sequence in some constructive metric space and $\Omega$ 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

---