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

LITERATURE CITED

5. F. Harary, Graph Theory, Addison-Wesley (1969).

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

D. Yu. Grigor'ev

This note consists of two independent parts. In the first part the concept of an \((m, \xi)\)-system for a set of linear forms is introduced, and a lower bound is obtained for the algebraic complexity of the computation of \((m, \xi)\)-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 for multiplying multiple-digit numbers and multiplying matrices modulo 2 are optimal in a certain sense.

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

1. In this section we will consider the question of the complexity of algebraic circuits for the simultaneous computation of a set of linear forms with complex coefficients in the variables \(x_1, \ldots, x_n\). 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 \(x_1, \ldots, x_n\).

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

\[ y_i = \alpha y_j + \beta y_k, \]

where \( \alpha, \beta \) are complex coefficients satisfying the bounds

\[ |\alpha| \leq 1, |\beta| \leq 1, \]

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 \( \left\lfloor \log \left| \det A \right| \right\rfloor \) (\( \left\lfloor x \right\rfloor \) denotes the integer part of \( x \), \( \left\lfloor x \right\rfloor = -\lfloor -x \rfloor \)).

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 \( x_i \)) corresponds a vertex \( Y_i \) (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 \( 1 \leq \ell \leq m \) we let \( G_\ell \) 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 \( 1 \leq \ell \leq m \) the graph \( G_\ell \) 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 \( \ell_1^c \) ) between \( \text{Conv} \{A_i\}_{i \in J} \) and \( \text{Conv} \{A_j\}_{j \notin J} \) exceeds \( c \), where \( A_j \) is a vector whose components are the coefficients of the linear forms being calculated (the vectors belong to \( n \)-dimensional real linear space) and \( \text{Conv} \) 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

\[ \ln c + \frac{\left| \log c - m - \log m \right|}{4m} = \frac{1}{\log 2} \ln M, \]

(\( \ell_q \) 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

\[ \frac{m^2 \log c}{8 \ell_q A_\log c} \quad (m, c \gg 1). \]