ESTIMATES OF THE COMPLEXITY OF SOLVING SYSTEMS OF LINEAR EQUATIONS

MATHEMATICS

1966

SovietRxiv

Abstract

Full Text

UDC 51.16

MATHEMATICS

B. M. KLOSS

ESTIMATES OF THE COMPLEXITY OF SOLVING SYSTEMS OF LINEAR EQUATIONS

(Presented by Academician A. N. Kolmogorov on 10 IX 1966)

The subject of this note is a lower estimate of the complexity of problems connected with the solution of systems of linear equations

$$\begin{gathered}a_{11}y_1 + a_{12}y_2 + \ldots + a_{1n}y_n = b_1,\\ a_{21}y_1 + a_{22}y_2 + \ldots + a_{2n}y_n = b_2,\\ \ldots\\ a_{n1}y_1 + a_{n2}y_2 + \ldots + a_{nn}y_n = b_n\end{gathered} \tag{1}$$

in the field of addition of integers modulo 2. Thus the variables and coefficients take the values 0 and 1, and the operation + is understood in the sense of addition modulo 2. We shall estimate complexity in the class of contact circuits and in the class of superpositions of functions over an arbitrary finite basis. As is known, in the latter case a constant depending on the basis enters into the expression for the Shannon function. For simplicity we shall assume that the basis contains a function of two variables—in order to make the constant equal to 1.

Two problems will be considered by us: 1) the question of the unique solvability of a system of linear equations, 2) finding a solution of a system of linear equations under the condition of its uniqueness. Lower estimates of the complexity of these two problems will be obtained. It should be noted that the basic construction used by us in solving these problems goes back to one method for constructing a sequence of functions of "nonlinear" complexity, proposed by E. I. Nechiporuk (^{1}).

Thus, the first problem is the following: to determine what the determinant of the system (1) is equal to—zero or one. Denote by $\bar{a}$ the set of coefficients located above the main diagonal of the matrix of the system (1). Consider the functions

$$\varphi_{\bar a}(x_1, \dots, x_n) = \begin{vmatrix} x_1 & a_{12} & a_{13} & \dots & a_{1n} & \\ 1 & x_2 & a_{23} & \dots & a_{2n} & \\ 0 & 1 & x_3 & \dots & a_{3n} & \\ . & . & . & . & . & . \\ 0 & 0 & \dots & 1 & x_n & \end{vmatrix}.$$

Lemma. The functions $\varphi_{\bar a}(x_1, \dots, x_n)$ are all distinct for distinct $\bar a$.

Proof. We apply induction. For the case $n = 2, 3$ the assertion of the lemma is verified directly. Assuming now the assertion proved for $n - 1$, consider a determinant of order n. Take two distinct sets $\bar a'$ and $\bar a''$ of values of the variables above the main diagonal and transform our determinant to the form

$$\varphi_{\bar a}(x_1, \dots, x_n) = \begin{vmatrix} 0 & x_1x_2 + a_{12} & a_{23}x_1 + a_{13} & \dots & a_{2n}x_1 + a_{1n} \\ 1 & x_2 & a_{23} & \dots & a_{2n} \\ 0 & 1 & x_3 & \dots & a_{3n} \\ . & . & . & . & . \\ 0 & 0 & \dots & 1 & x_n \end{vmatrix} = \left| \begin{matrix} x_1x_2 + a_{12} & a_{23}x_1 + a_{13} & \dots & a_{2n}x_1 + \\ 1 & x_3 & \dots & a_{3n} \\ 0 & 1 & x_4 & \dots \\ . & . & . & . \\ 0 & 0 & \dots & 1 \end{matrix} \right. \qquad (2)$$

It follows from this that if the tuples $\bar a'$ and $\bar a''$ have distinct values lying below the first two rows, then the functions $\varphi_{\bar a'}(1, x_2, \dots, x_n)$ and $\varphi_{\bar a''}(1, x_2, \dots, x_n)$ are distinct. Analogous arguments (but now with respect to columns) apply if the tuples $\bar a'$ and $\bar a''$ have distinct values lying to the left of the last two columns.

It remains to examine the case when the tuples $\bar a'$ and $\bar a''$ differ by values lying in the upper right square of order 2. Here several possibilities arise.

a) One of the numbers $a_{1,n-1}, a_{2,n-1}$ (a_{1n}, a_{2n}) is changed, and the other is not. In this case the determinant in the form (2), for $x_1 = 1$, reduces to a determinant of order $n - 1$.

b) The whole pair $(a_{1,n-1}, a_{2,n-1})$, or the pair (a_{1n}, a_{2n}), or both of these pairs, is changed. Then the sum $\varphi_{\bar a'}(0, x_2, \dots, x_n) + \varphi_{\bar a''}(0, x_2, \dots, x_n)$ in the first case is equal to x_n, in the second to 1, and in the third to $x_n + 1$. Obviously, in the first and third cases one can choose the corresponding value of the variable x_n so that the above sum is equal to 1.

Theorem 1. *The complexity of computing a determinant of order* n *is bounded from below asymptotically: for superpositions, by* $n^3/2\log n$*; for contact circuits, by* $n^3/6\log n$*; for parallel-sequential contact circuits, by* $n^3/2$.

Proof. Partition the n^2 variables of the determinant into n sets $B_1, \dots, B_n$: take the main diagonal as B_1; the diagonal lying below the main diagonal, together with the element x_{1n}, as B_2; the diagonal lying below the preceding one, together with the elements $x_{1,n-1}$ and x_{2n}, as B_3, and so on. It is easy to see that if, for the set B_i, we substitute different constants for the remaining variables, then the number of functions depending on the variables of the set B_i will be the same for each $i = 1, \dots, n$. On the other hand, as follows from the lemma proved, the number of such functions for each set B_i will be greater than $2^{(n^2-n)/2}$. We now use the method of E. I. Nechiporuk (^{1}). Choose, from the functions obtained, one for which the number of occurrences of variables from the set B_i is maximal. This number is clearly greater than $(1-\varepsilon)(n^2-n)/2\log n$ [2]. Then the total number of occurrences of all variables will be asymptotically greater than $n^3/2\log n$. The complexity of the contact circuit for the chosen function of the variables from B_i will, as is easy to see from (3), be greater than $(1-\varepsilon)(n^2-n)/6\log n$. Hence it follows that the complexity of a contact circuit realizing a determinant of order n will be asymptotically greater than $n^3/6\log n$.

To obtain a lower bound in the class of parallel-sequential contact circuits one can use the method of B. A. Subbotovskaya (^{4}). In the function $\varphi_{\bar{a}}(x_1, \dots, x_n)$ introduced above (the coefficients $a_{ij}, i < j$, are also regarded as variables), we shall estimate the number of occurrences of the variables a_{ij}. Combining the proved lemma with the result of B. A. Subbotovskaya, we obtain the required estimate.

Now let us estimate the complexity of solving the system of linear equations (1) with a determinant different from zero.

Theorem 2. *The complexity of solving a system of linear equations of order n with determinant different from zero is estimated from below asymptotically: for superpositions—by the quantity $n^3/4\log n$, for contact schemes—by the quantity $n^3/4\log n$, and for parallel-sequential contact schemes—by the quantity $n^3/2$.*

Proof. We shall apply the reasoning used by us in the preceding theorem. Consider the sets of variables

$$B = \{b_1, \dots, b_n\}, \quad A_1 = \{a_{11}, \dots, a_{n-1,1}\}, \quad A_2 = \{a_{12}, \dots, a_{n-1,2}\}, \dots, \quad A_n = \{a_{1n}, \dots, a_{n-1,n}\},$$

and estimate the number of occurrences of variables from these sets. Let us first take the set B. It is clear that for any two distinct nonsingular matrices (a'_{ij}) and (a''_{ij}) of order n there will be values of the variables $b_1, \dots, b_n$ such that the corresponding systems of equations will have different solutions. Since the total number of nonsingular matrices of order n is $\approx 0.3 \cdot 2^{n^2}$, the number of occurrences of variables from the set B is estimated from below asymptotically by the quantity $n^2/\log n$.

The estimates for each of the sets A_i are obtained in the same way; therefore we shall demonstrate their derivation using the set A_n as an example. Put all $a_{ii} = 1$, $b_i = 1$, and $a_{ij} = 0$ for $i > j$ (then the determinant is nonzero). Denote $a_{1n} = x_1, \dots, a_{n-1,n} = x_{n-1}$. We shall show that any two different sets of values of the remaining elements a_{ij} are separated by (5). Let $\{a'_{ij}\}$ and $\{a''_{ij}\}$ be two such sets, and let i be the first index from below for which the rows

$$a'_{i,i+1}, \dots, a'_{i,n-1},$$

$$a''_{i,i+1}, \dots, a''_{i,n-1}$$

are different. If the number of nonzero terms in these rows is even in one case and odd in the other, then, choosing the values of the variables $x_{i+1}, \dots, x_{n-1}$ so that $y_{i+1} = 1, \dots, y_n = 1$, we arrive at a situation in which in one case $y_i = 0$, and in the other $y_i = 1$. It remains to consider the case when the number of nonzero terms in both rows has the same parity. Without loss of generality, we may assume that these sets do not intersect. Let in the first row these be the terms $a_{ik_1}, \dots, a_{ik_s}$, and in the second $a_{il_1}, \dots, a_{il_t}$. We then choose the values of the variables $x_{i+1}, \dots, x_{n-1}$ in such a way that all $y_{k_1}, \dots, y_{k_s}$ are equal to zero, and an odd number of the terms among $y_{l_1}, \dots, y_{l_t}$ are equal to one (and the rest to zero). Then, as is easy to see, it again turns out that in one case y_i will be equal to zero, and in the other to one.

The number of occurrences of variables from the set A_n is then estimated from below asymptotically by the quantity $(n^2 - 3n + 2)/4 \log n$ (6). Consequently, the complexity of the whole problem is estimated from below asymptotically by the quantity $n^3/4 \log n$.

Considering a realization in the form of a contact scheme (see (7)), we obtain an asymptotic lower estimate equal to $n^3/4 \log n$, and from the work of G. A. Subbotovskaya (4) for parallel-sequential schemes there follows the estimate $n^3/2$.

In conclusion, we note that the question of estimating complexity in the class of circuits of functional elements remains open (only a linear estimate is known —see (5)); so far no example of a function having nonlinear complexity in this class has been constructed.

Received
9 IX 1966

REFERENCES CITED

1. E. I. Nechiporuk, DAN, **169**, No. 4 (1966).
2. R. E. Krichevsky, *Collection: Problems of Cybernetics*, vol. 2, Moscow, 1959, p. 123.
3. O. B. Lupanov, *Collection: Problems of Cybernetics*, vol. 10, Moscow, 1963, p. 63.
4. G. A. Subbotovskaya, DAN, **136**, No. 3, 553 (1961).
5. B. M. Klos, V. A. Malyshchev, *Vestn. Mosk. Univ.*, Ser. Mat., No. 4, 44 (1965).

6. O. B. Lupanov, *Collection: Problems of Cybernetics*, vol. 14, "Nauka," 1965, p. 31.

7. G. N. Povarov, *Collection: Logical Investigations*, Publishing House of the Academy of Sciences of the USSR, 1959, p. 379.

Note: Figure translations are in progress. See original paper for figures.

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.