ON COMPARING THE COMPLEXITY OF REALIZATIONS OF BOOLEAN FUNCTIONS BY AUTOMATA AND TURING MACHINES

CYBERNETICS AND CONTROL THEORY

1968

SovietRxiv

Abstract

Full Text

UDC 519.95

CYBERNETICS AND CONTROL THEORY

Yu. Ya. Breitbart

ON COMPARING THE COMPLEXITY OF REALIZATIONS OF BOOLEAN FUNCTIONS BY AUTOMATA AND TURING MACHINES

(Presented by Academician P. S. Novikov on 1 IX 1967)

1. In the present note the role of the external memory of Turing machines in computing Boolean functions on them is clarified. Namely, the question of comparing the complexities of realizations of Boolean functions by Turing machines (T.M.) and by Turing machines without external memory (automata) is considered. Here, by the complexity of a realization of a function $f(x_1, \dots, x_n)$ by an automaton (respectively, a T.M.) is meant the product of the minimally necessary number of internal states of the automaton (respectively, T.M.) realizing the function obtained from f by some permutation of the variables, by the maximum time for computing $f(\alpha_1, \dots, \alpha_n)$, where the maximum is taken over all possible tuples $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$ of 0 and 1 of length n.

In particular, it is established that the ratio of the complexities of realizations is not less than $2^{cn-\varphi(n)}$, where c and $\varphi(n)$ depend only on the set of possible permutations of the variables of the original function, and moreover $\lim_{n\to\infty} \varphi(n)/n = 0$; $1/8 \le c \le 1$.

For a precise statement of the problem and formulation of the results, we introduce the necessary definitions and notation.

P_a is some permutation of the numbers $(1, 2, \dots, n)$. We shall henceforth call any such permutation a direction.

Definition. We shall say that an automaton $\mathfrak{A} = \langle Q, \varphi, q_0, T\rangle$ ([2]) with input alphabet $(0, 1)$ realizes the Boolean function $f(x_1, \dots, x_n)$ in the direction $P_n = (i_1, \dots, i_n)$, if

$$\varphi(q_0; \alpha_{i_1}, \dots, \alpha_{i_n}) \in T \Longleftrightarrow f(\alpha_1, \dots, \alpha_n) = 1,$$

where $n \ge 1$; $\alpha_i = 0, 1$. $L_{\mathfrak{A}}^{P_n}(f)$ is the number of internal states of the automaton $\mathfrak{A}$ realizing f in the direction P_n.

$L_A'^{P_n}(f)$ is the minimal number of states of an automaton sufficient for realizing

f in the direction P_n. We shall further call

$$L_A^{P_n}(f) = nL_A'^{P_n}(f)$$

the complexity of the realization of f by automata in the direction P_n. Let Π_n be some set of directions. Put

$$L_A^{\Pi_n}(f) = \min_{P_n \in \Pi_n} L_A^{P_n}(f).$$

In what follows we shall be interested in the following sets of directions Π_n^1:

$$\{(1, 2, \dots, n);\ (n, n-1, \dots, 2, 1)\};$$

Π_n^2: $P_n \in \Pi_n^2 \iff P_n$ is some cyclic permutation of $(1, 2, \dots, n)$ or $(n, n-1, \dots, 1)$; Π_n^3 is the set of all possible directions.

Let $\mathfrak{M}$ be a T.M. realizing $f(x_1, \dots, x_n)$ (see (1)). Let $t_{f,\mathfrak{M}}(\tilde{\alpha})$ be the number of steps which $\mathfrak{M}$ expends to compute $f(\alpha_1, \dots, \alpha_n)$, $(\tilde{\alpha} = (\alpha_1, \dots, \alpha_n);\ \alpha_i = 0, 1;\ n \geq 1)$, and let $L'_{\mathfrak{M}}(f)$ be the number of internal states of the T.M. $\mathfrak{M}$ realizing f. We shall call

$$L'_{\mathfrak{M}}(f) \max_{\tilde{\alpha}} t_{f,\mathfrak{M}}(\tilde{\alpha})$$

the complexity of the realization of the function f on the T.M. $\mathfrak{M}$, and denote it by $L_{\mathfrak{M}}(f)$. We shall further call

$$L_{\text{T.M.}}(f) = \min_{\mathfrak{M} \text{ realizes } f} L_{\mathfrak{M}}(f)$$

the complexity of the realization of f on a T.M. Further, everywhere f is a Boolean function of n variables, and $\mathcal{F}_2$ is the set of all such functions.

Let

$$L(n) = \max_{f \in \mathfrak{P}_2} \frac{L_A^{\Pi_n^1}(f)}{L_{\text{M.T}}(f)}, \qquad K(n) = \max_{f \in \mathfrak{P}_2} \frac{L_A^{\Pi_n^2}(f)}{L_{\text{M.T}}(f)}, \qquad M(n) = \max_{f \in \mathfrak{P}_2} \frac{L_A^{\Pi_n^i}(f)}{L_{\text{M.T}}(f)}.$$

The problem consisted in estimating the functions $L(n), K(n), M(n)$. In the paper it is proved that $L(n) \geq 2^n/n \log n^*$. It is further proved that $\log K(n) \sim n$ and $\log M(n) \asymp n$.

2. Let $f(x_1, \dots, x_n)$ be a Boolean function and let $P_n = (i_1, \dots, i_n)$ be some direction. Denote by $\mu(f, s, P_n)$ the number of distinct Boolean functions that can be obtained from $f(x_{i_1}, \dots, x_{i_n})$ by all possible substitutions of constants in place of the first s arguments of $f(x_{i_1}, \dots, x_{i_n})$, where $1 \leq s \leq n$.

Lemma 1. *Let $f(x_1, \dots, x_n)$ be a Boolean function and let $\mathfrak{A}$ be an automaton realizing f in the direction P_n. Then*

$$L'^{P_n}_{\mathfrak{A}}(f) \geq \max_{1\leq s\leq n} \mu(f, s, P_n).$$

The proof is essentially contained in (1).

Following (3), call a set G of square matrices of order n, $n > 1$, whose entries are 0 and 1, complete if any two matrices from this set have no common rows, every vector of length n occurs as a row in at least one matrix of the set G, and no matrix contains identical rows.

Lemma 2. *Whatever $n = 2^{m+1}$, $m \geq 1$, there exists a complete set of symmetric matrices of order n.*

Let G_{m+1} be a complete set of symmetric matrices of order $n = 2^{m+1}$, existing by Lemma 1. Obviously, the number of matrices in G_{m+1} is equal to $2^{2^{m+1}-m-1}$. We next number the matrices in G_{m+1} by the numbers from 0 to $2^{2^{m+1}-m-1}$ and denote by a_{ijk} $(1 \leq i, j \leq 2^{m+1},\ 0 \leq k \leq 2^{2^{m+1}-m-1})$ the element of the matrix with number k lying at the intersection of the i-th row and the j-th column.

Let $2^m + m < n \leq 2^{m+1} + m + 1$; then $n = 2^m + m + r$, where $1 \leq r \leq 2^m + 1$.

Define

$$F_n(\alpha_0, \dots, \alpha_m, \beta_0, \dots, \beta_{2^m-m+r-3}, \gamma_0, \dots, \gamma_m) = a_{ijk},$$

where

$$i - 1 = |\tilde{\alpha}|, \qquad j - 1 = |\tilde{\gamma}|, \qquad k - 1 = |\tilde{\beta}|^{**},$$
$$\tilde{\alpha} = (\alpha_1, \dots, \alpha_m), \qquad \tilde{\gamma} = (\gamma_0, \dots, \gamma_m),$$
$$\tilde{\beta} = (\underbrace{0, \dots, 0}_{2^m-3}, \beta_0, \dots, \beta_{2^m-m+r-3}).$$

Lemma 3. $L^{\Pi^1_n}_A(F_n) \geq 2^n$.

Lemma 4.

$$L_{\text{M.T}}(F_n) \leq n \log n.$$

Remark 1. If one assumes that an M.T. realizing F_{n_1} for some $n_1 > 1$ realizes F_n, whatever n may be, then from (6) it follows that

$$L_{\text{M.T}}(F_n) \leq n \log n.$$

From Lemmas 2-3 it follows that

Theorem 1. $L(n) \geq 2^n/n \log n$.

3. In obtaining the results of this section, E. I. Nechiporuk' s method (see (5)) for obtaining a "complex" function is generalized.

* Here and below logarithms are considered to base 2.

** $|\tilde{\alpha}|$ is the natural number whose binary representation is the tuple $\tilde{\alpha} = (a_0, \dots, a_m)$.

Let

$$\Phi^1(x_1, \dots, x_n) = \bar{x}_k \bigvee_{|\tilde{\gamma}|=0}^{k-1} x_{|\tilde{\gamma}|+1} \cdot x_{k+1}^{\gamma_1} \cdots x_n^{\gamma_{n-k}}, \quad \text{where} \quad n-k = \lfloor \log(k-1) \rfloor,$$

$$\tilde{\gamma} = (\gamma_1, \dots, \gamma_{n-k}); \quad \gamma_i = 0, 1, \quad 1 \le i \le n-k; \quad n > 1, \quad k > 1.$$

Next let

$$\Phi^i(x_1, \dots, x_n) = \Phi^1(x_i, x_{i+1}, \dots, x_n, x_1, \dots, x_{i-1}), \quad \text{where } 2 \le i \le n.$$

Put

$$\Phi_n(x_1, \dots, x_n) = \sum_{i=1}^{n} \Phi^i(x_1, \dots, x_n) *.$$

Lemma 5. If, instead of all variables of Φ_n except the variables $x_i, x_{i+1}^{**}, \dots, x_{i+(n-k)}^{**}$, $1 \le i \le n$, distinct sets of constants are substituted, then the number of distinct functions thereby obtained is $\ge 2^{k-2}$.

Hence, using Lemma 1, we obtain that $L_A^{\Pi_n^2}(\Phi_n) \gtrsim 2^n$.

Remark 2. Let $l(\Phi_n)$ be the number of contacts minimally necessary for realizing Φ_n by a contact circuit. Then, by Lemma 5 and Theorem 2 from ([5]), we have $l(\Phi_n) \gtrsim n^2/\log^2 n$. Next let $m(\Phi_n)$ be the minimally necessary number of input variables for realizing Φ_n in some basis. Then $m(\Phi_n) \gtrsim n^2/\log n$ by Lemma 4 and Theorem 1 from ([5]).

Lemma 6. $L_{\text{M.T}}(\Phi_n) \lesssim n^2 \log n$.

From Lemmas 5 and 6 we obtain that $K(n) \gtrsim 2^n/n^2 \log n$, whence it easily follows

Theorem 2. $\log K(n) \sim n$.

4. Let $S_i^k(\tilde{S}_i^k)$ be an elementary symmetric function of the variables $x_1, \dots, x_k$, $(x_{k+1}, \dots, x_{2k})$ $(k > 1)$ with working number $1 \le i \le k$ (see ([4])). Let $n = 2k$, $k > 1$.

Put

$$\psi_n(x_1, \dots, x_k, x_{k+1}, \dots, x_{2k}) = \sum_{i=1}^{k} x_i \tilde{S}_i^k \oplus \sum_{i=1}^{k} x_{k+i} S_i^k.$$

Let $n = 2k + 1$. Put

$$\psi_n(x_1, \dots, x_{2k}, x_{2k+1}) = \psi_{n-1}(x_1, \dots, x_{2k}) \,\&\, (x_{2k+1} \vee \bar{x}_{2k+1}).$$

Lemma 7. $L_A^{\Pi_n^3}(\psi_n) \gtrsim 2^{[n/8]}$.

Lemma 8. $L_{\text{M.T}}(\psi_n) \lesssim n^2$.

Hence it follows

Theorem 3. $\log M(n) \asymp n$.

The author considers it his pleasant duty to express profound gratitude to P. S. Novikov for posing the problem and supervising the present work, and to A. A. Muchnik for discussion of the results of the work and valuable advice.

Moscow State Pedagogical Institute
named after V. I. Lenin

Received
30 VIII 1967

REFERENCES

[1] V. A. Kuzmin, *Problems of Cybernetics*, 13, "Nauka," 1965, p. 75.
[2] M. O. Rabin, D. Scott, *Cybernetics. Collection*, 4, IL, 1962, p. 58.
[3] O. B. Lupanov, *Problems of Cybernetics*, 3, Moscow, 1960, p. 61.
[4] O. B. Lupanov, *Problems of Cybernetics*, 15, "Nauka," 1965, p. 85.
[5] E. I. Nechiporuk, DAN, 169, No. 4 (1966).
[6] B. A. Trakhtenbrot, *Algebra, Logic, Seminar*, 4, 5 (1964).

* $\sum$ is the sign of summation mod 2.
** $+$ is the sign of addition mod $(n - k + 1)$.

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