# DETERMINING THE REGULARITY OF AN AUTOMATON FROM ITS CANONICAL EQUATIONS

B. M. KLOSS, V. A. MALYSHEV

1967

SovietRxiv

**Abstract**

**Full Text**

UDC 519.95

## CYBERNETICS AND CONTROL THEORY

**B. M. KLOSS, V. A. MALYSHEV**

# DETERMINING THE REGULARITY OF AN AUTOMATON FROM ITS CANONICAL EQUATIONS

*(Presented by Academician A. N. Kolmogorov, 19 III 1966)*

We shall consider autonomous automata with a finite set of states $\Omega$, containing $N$ elements. Each such automaton $\mathfrak{A}$ may be regarded as a certain transformation of the set $\Omega$ into itself. We agree to call an automaton **regular** if it carries out a one-to-one transformation of $\Omega$. We shall be interested in the problem of determining, from the equations of an automaton, whether the given automaton is regular or not. We shall solve this problem, and also estimate its complexity, within a certain class of methods. The following idea underlies them. It is clear that, in order to check the regularity of an automaton $\mathfrak{A}$, it is sufficient, for the corresponding transformation, to count the cardinality of the preimage of each element of $\Omega$. We shall say that an automaton $\mathfrak{A}$ **preserves the weight** of a set $A \subset \Omega$ if the number of elements in $A$ is equal to the number of elements in the preimage of this set under the mapping $\mathfrak{A}$. Generalizing the rule indicated above, we arrive at the consideration of systems of subsets of $\Omega$ possessing the property that, if the automaton $\mathfrak{A}$ preserves the weight of any set of the given system, then the automaton $\mathfrak{A}$ must be regular. Such systems of sets we shall call **determining**.

Let the sets $A_1, \dots, A_s$ form a determining system in the space $\Omega$. Denote by $x_i$ the number of elements in the preimage of the $i$-th point for the automaton $\mathfrak{A}$. Under the assumption that the automaton $\mathfrak{A}$ preserves the weight of the given sets, we have

$$\sum_{j=1}^{N} a_{ij} x_j = \sum_{j=1}^{N} a_{ij}, \qquad i = 1, \dots, s; \qquad \sum_{j=1}^{N} x_j = N, \tag{1}$$

where $a_{ij} = 1$ if the $j$-th point belongs to $A_i$, and $a_{ij} = 0$ in the opposite case.

**Lemma 1.** *The sets $\{A_1, \dots, A_s\}$ form a determining system if and only if equations (1) have a unique integral solution in the domain $\{x_i \geq 0,\ i = 1, \dots, N\}$.*

We shall deal with the problem of choosing determining systems of sets and estimating the minimal number of sets in such systems.

In parallel, our considerations will also proceed in the following aspect. We shall say that an automaton $\mathfrak{A}$ **preserves the parity** of a set $A$ if the number of elements in $A$ is congruent in parity to the number of elements in the preimage of this set. We shall call a system of sets **parity-determining** if the preservation by the automaton $\mathfrak{A}$ of the parity of every set of the given system implies its regularity.

**Lemma 2.** *For the sets $\{A_1, \dots, A_s\}$ to form a parity-determining system, it is necessary and sufficient that equations (1), in the field of addition of integers modulo 2, have a unique solution.*

From Lemmas 1 and 2 it follows that

**Lemma 3.** *The property of determinacy (parity determinacy) of a system of sets will not change if some of these sets are replaced by their complements.*

It also follows from Lemma 2 that

**Theorem 1.** *The number of sets in a minimal parity defining system is equal to $N-1$. Moreover, the sets $A_1, \dots, A_{N-1}$ form a parity defining system if and only if the determinant of system (1) (over the field of addition of integers modulo 2) is equal to one.*

**Remark.** A parity defining system is at the same time also a defining system.

Denote by $T(N)$ the number of sets in a minimal defining system (the space $\Omega$ consists of $N$ elements).

**Corollary.** $T(N) \leq N - 1$.

On the other hand, from the fact that for every pair of points of $\Omega$ there must be, in the defining system, a set that "separates" them, it follows that $T(N) \geq \log N$.

**Lemma 4.** $T(N-1) \leq T(N) \leq T(N-1) + 1$.

Let us define the set of vectors on which a Boolean function $f$ takes the value 1 as the **support** of the function $f$. The number of elements in the support is called the **weight** of the function and is denoted by $\|f\|$. We shall now give some examples of parity defining systems in the case when $N = 2^n$.

**Theorem 2.** *The supports of all possible elementary conjunctions $x_{i_1} \dots x_{i_k}$, $1 \leq k \leq n$, form a parity defining (and hence also defining) system of sets in the space of $n$-dimensional Boolean vectors.*

**Corollary 1.** *The supports of all possible elementary disjunctions $x_{i_1} \vee \dots \vee x_{i_k}$, $1 \leq k \leq n$, form a parity defining (defining) system of sets in the space of $n$-dimensional Boolean vectors.*

**Corollary 2.** *The system of Boolean equations*

$$y_i = f_i(x_1, \dots, x_n), \qquad i = 1, \dots, n, \tag{2}$$

*is solvable for arbitrary values of the left-hand sides if and only if*

$$\|f_{i_1} \dots f_{i_k}\| = 2^{n-k}, \qquad 1 \le k \le n.$$

**Corollary 3.** *The system of Boolean equations (2) is solvable for arbitrary values of the left-hand sides if and only if*

$$\|f_{i_1} \vee \dots \vee f_{i_k}\| = 2^n - 2^{n-k}, \qquad 1 \le k \le n.$$

**Corollary 4 (D. Huffman [1]).** *In order that the system of equations (2) be solvable for arbitrary values of the left-hand sides, it is necessary and sufficient that the functions $f_{i_1} \dots f_{i_k}$, $1 \le k \le n-1$, written in the form of Zhegalkin polynomials, not contain the product $x_1 x_2 \dots x_n$, while the function $f_1 \dots f_n$ contain it.*

**Theorem 3.** *The supports of all possible linear functions $x_{i_1} \oplus \dots \oplus x_{i_k}$, $1 \le k \le n$ ($\oplus$ denotes addition modulo 2), form, in the space of $n$-dimensional Boolean vectors, a defining system that is not a parity defining system.*

**Proof.** Consider the matrix of the corresponding system (1). One column in it consists of all zeros and one one (the corresponding row consists of ones only); therefore, removing this column and the last row, we arrive at a certain matrix $C$ of order $2^n - 1$. Note that the support of each linear function contains $2^{n-1}$ elements, while the support of the product of two distinct functions contains $2^{n-2}$ elements. Therefore the product of the matrix $C$ by its transpose gives the matrix

$$2^{n-2} \begin{pmatrix} 2 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 1 \\ \cdot & \cdot & \cdots & \cdot \\ 1 & 1 & \cdots & 2 \end{pmatrix},$$

which is nonsingular. The definiteness of the system then follows from Lemma 1. At the same time, over the field of addition of integers modulo 2 the matrix $C$ is singular (since each row of this matrix contains an even number of ones); consequently, by Theorem 1, the given system is not parity defining.

**Corollary.** The system of Boolean equations (2) is solvable for arbitrary values of the left-hand sides if and only if

$$\left\|f_{i_1} \oplus \dots \oplus f_{i_k}\right\| = 2^{n-1}, \qquad 1 \le k \le n.$$

**Theorem 4.** Let $\Omega$ be the set of $n$-dimensional Boolean vectors. If the defining system consists of the supports of linear functions, then the number of sets in such a system is equal to $2^n - 1$.

**Proof.** Suppose that the given system includes the supports of not all linear functions; for example, let the indicator row $a_1, \dots, a_N$, corresponding to the support of some linear function, not be included in the matrix of the system (1) (we take only linearly independent rows). Then, taking into account the remarks made in the proof of the preceding theorem, we arrive at the fact that system (1) has an additional solution equal to $x_1 = 2a_1, \dots, x_N = 2a_N$.

**Theorem 5.** Let $\Omega$ be the set of $n$-dimensional Boolean vectors. If the defining system consists of the supports of conjunctions $x_{i_1} \dots x_{i_k}$, $k \le n$, then the number of sets in such a system is equal to $2^n - 1$.

**Theorem 6.** If the defining system consists of the supports of conjunctions of rank $n$, then the number of sets in such a system is equal to $2^n - 1$.

On the other hand, as the following example shows, the estimates indicated above do not always hold.

**Theorem 7.** In the set of $n$-dimensional Boolean vectors ($n \ge 3$) there exists a defining system in which the number of sets is equal to $2^n - 2$.

**Proof.** As the sets $A_1, \dots, A_{2^n-3}$ we choose the supports of certain $2^n - 3$ linear functions. After an obvious change of variables, the corresponding system (1) is reduced to a homogeneous system, and we shall seek solutions in the domain $\{x_i \ge -1\}$. Let the two rows corresponding to the two missing linear functions have the form:

$$a_1 = \dots = a_{2^{n-1}} = 1, \quad a_{2^{n-1}+1} = \dots = a_{2^n} = 0; \quad b_1 = \dots = b_{2^{n-2}} = 0,$$

$$b_{2^{n-2}+1} = \dots = b_{3\cdot 2^{n-2}} = 1, \quad b_{3\cdot 2^{n-2}+1} = \dots = b_{2^n} = 0.$$

The homogeneous system is satisfied by two linearly independent solutions:

$$x^1_1 = \dots = x^1_{2^{n-1}} = 1, \quad x^1_{2^{n-1}+1} = \dots = x^1_{2^n} = -1;$$

$$x^2_1 = \dots = x^2_{2^{n-2}} = -1, \quad x^2_{2^{n-2}+1} = \dots = x^2_{3\cdot 2^{n-2}} = 1,$$
$$x^2_{3\cdot 2^{n-2}+1} = \dots = x^2_{2^n} = -1,$$

and by two solutions that are their linear combinations:

$$x^3_1 = \dots = x^3_{2^{n-2}} = 0, \quad x^3_{2^{n-2}+1} = \dots = x^3_{2^{n-1}} = 1,$$

$$x^3_{2^{n-1}+1} = \dots = x^3_{3\cdot 2^{n-2}} = 0, \quad x^3_{3\cdot 2^{n-2}+1} = \dots = x^3_{2^n} = -1;$$
$$x^4_1 = \dots = x^4_{2^{n-2}} = 1, \quad x^4_{2^{n-2}+1} = \dots = x^4_{2^{n-1}} = 0,$$
$$x^4_{2^{n-1}+1} = \dots = x^4_{3\cdot 2^{n-2}} = -1, \quad x^4_{3\cdot 2^{n-2}} = \dots = x^4_{2^n} = 0.$$

There are no other solutions, except the zero solution. If now $2^{n-2} \geq 2$, then we choose the set $A_{2^{n-2}}$, to which corresponds the row $c_1, \ldots, c_{2^n}$, in which

$$c_1 = c_2 = c_{2^{n-1}} = 1,$$

and the remaining $c_i = 0$. The four solutions indicated above do not satisfy the equation $c_1 x_1 + \cdots + c_{2^n} x_{2^n} = 0$; therefore, if it is adjoined to the original homogeneous system, then the new system will have, in the domain $\{x_i \geq -1\}$, a unique solution.

**Remark.** Moreover, whatever integer $C_0 > 0$ is given, there will be such an $N_0 = N_0(C_0)$ that for all $N > N_0$ one has $T(N) \leq N - C_0$.

As an example of the application of the criteria obtained above, let us consider various register circuits, whose equations, after simple transformations, are reduced to triangular form:

$$y_i = f_i(x_1, x_2, \ldots, x_i), \qquad i = 1, 2, \ldots, n. \tag{3}$$

A system of type (3) defines a regular automaton, as follows easily from what was said above, if and only if the functions $f_i$ have the form

$$f_i(x_1, \ldots, x_{i-1}, x_i) = f_i'(x_1, \ldots, x_{i-1}) \oplus x_i.$$

In different concrete cases it is convenient to apply one or another criterion—

with different checking functions. These checking functions, naturally, are subject to requirements of simplicity. The criteria given above (parity check, checking of weights by checking linear functions and conjunctions) have, in essence, quadratic complexity (complexity is understood in the sense of ($^2$)). Moreover, Theorems 1, 4, 5, and 6 give a lower estimate for this complexity. It is of interest to estimate from below the complexity of the problem of determining the regularity of an automaton for arbitrary methods of solving it (in the class of circuits of functional elements realizing arbitrary functions of two variables).

Consider an arbitrary numbering $R$ of Boolean functions of $n$ variables by binary strings of length $2^n$ (for example, the coefficients of the Zhegalkin polynomial, the tabular specification of the function, etc.). The numbering $R$ naturally generates a certain numbering of systems of Boolean functions (2) by strings of length $n \cdot 2^n$. Now consider the function $\Phi$ of $n \cdot 2^n$ variables, equal to 1 if and only if the system (2) corresponding to the argument string is solvable for arbitrary values of the right-hand sides. We shall prove that the complexity of the function $\Phi$ is bounded below by $n(2^n - 1) - 1$, which (taking ($^2$) into account) will follow from Theorem 8.

**Theorem 8.** The function $\Phi$ essentially depends on at least $n(2^n - 1)$ variables.

**Proof.** Partition the variables into $n$ groups of $2^n$ in each group—corresponding to the functions from (2). Suppose that $\Phi$ depends inessentially on the variable

$z_1$ of the first group. Then, for a fixed string $(\sigma_2, \dots, \sigma_{2^n})$ of values of the remaining variables of this group, the functions $f_1^0$ and $f_1^1$, corresponding in the given numbering to the strings $(0, \sigma_2, \dots, \sigma_{2^n})$ and $(1, \sigma_2, \dots, \sigma_{2^n})$, as is easy to see, either both have weight $2^{n-1}$, or both do not have this property. Let us examine the first possibility. Here two cases may arise: either there exist two strings $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n)$ at Hamming distance 1 from one another and such that for one function, for example, $f_1^0(\alpha) = f_1^0(\beta)$, while for the other $f_1^1(\alpha) \neq f_1^1(\beta)$, or no such strings exist. In this latter case either $f_1^0 \equiv f_1^1$, or $f_1^0 = \bar{f}_1^1$. Indeed, consider an arbitrary string $x = (x_1, \dots, x_n)$ and a chain of strings $\alpha = \alpha^0, \alpha^1, \dots, \alpha^{k-1}, \alpha^k = x$ such that $\alpha^i \alpha^{i+1}$ for all $i = 0, \dots, k-1$ are at distance 1 from one another. Then, obviously, the equality or inequality of the functions $f_1^0$ and $f_1^1$ on one string $\alpha$ will extend to any string $x$. Since the functions $f_1^0$ and $f_1^1$ must nevertheless, by definition, be different, we arrive at the conclusion that in this case $f_1^0 \equiv \bar{f}_1^1$.

Now consider the other case—when such two strings $\alpha$ and $\beta$ exist (we may restrict ourselves to the case when they differ only in the first coordinate). Then define the remaining functions of the system (2) so that they map the strings $\alpha$ and $\beta$ into one string $(\alpha_2, \dots, \alpha_n)$, and, together with the function $f_1^1$, form a solvable system. This, as is not difficult to see, can always be done, but, on the other hand, it leads to the essentiality of the variable $z_1$, which contradicts the initial assumption. Consequently, this case cannot occur.

On the basis of what has been set forth, one may conclude that two opposite functions (one is the negation of the other) of weight $2^{n-1}$ can differ only in the first coordinate of the numbering string, and any other variable from this same group must be essential (since for it the same arguments can be carried out).

Received
5 III 1966

## REFERENCES

[1] D. Huffman, *Trans. IRE*, CT-6, Spec. Suppl., 41 (1959). [2] B. M. Kloss, V. A. Malyshev, *Vestn. Mosk. Univ.*, No. 4 (1965).

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