CYBERNETICS AND CONTROL THEORY

N. A. GORBOVITSKAYA

1963

SovietRxiv

Fig. 1

Figure 1: Fig. 1

Abstract

Full Text

CYBERNETICS AND CONTROL THEORY

N. A. GORBOVITSKAYA

EQUIVALENT TRANSFORMATIONS OF AUTOMATA OF CERTAIN TYPES

(Presented by Academician P. S. Novikov on 22 II 1963)

1°. Let us first consider circuits made up of functional elements in an arbitrary complete finite basis ([1]). A circuit B is called a **subcircuit** of a circuit A if all elements and vertices of the circuit B belong to A, and the poles of the circuit B are all the poles of the circuit A belonging to B and all vertices at which the circuit B is connected with the remaining part of the circuit A.

Fig. 1

Let B and C be circuits between whose input poles (inputs), and also between whose output poles (outputs), some one-to-one correspondence has been established. The circuits B and C are called **equivalent** under the given correspondence between their poles if they realize one and the same system of functions. Let B and C be equivalent circuits and let B be a subcircuit of a circuit A. Replacing in A the subcircuit B by C, taking account of the correspondence between their poles, we obtain a circuit A', equivalent to A. We shall say that the pair of equivalent circuits B and C defines the following rule $B \leftrightarrow C$ of **equivalent transformation** of circuits: in any circuit containing the circuit B as a subcircuit, this subcircuit may be replaced by the circuit C, and conversely.

Theorem 1. *For circuits made up of functional elements in an arbitrary complete finite basis, there exists a finite system of rules in this basis such that any two equivalent circuits can be transformed into one another by means of this system of rules.*

Such a system of rules includes three basic subsystems:

Subsystem I is determined by the rules for the corresponding formulas. For example, let the basis consist of elements realizing conjunction, disjunction, and negation. Then subsystem I is determined by a complete system of rules for formulas composed of conjunctions, disjunctions, and negations.

Thus, the rules for formulas

$$1)\quad (x\&y)\vee z=(x\vee z)\&(y\vee z);\qquad 2)\quad \overline{x\&y}=\bar{x}\vee\bar{y}$$

determine the rules for transforming the circuits in Fig. 1a and 1b.

Subsystem II consists of rules that discard "branches" not leading to the output poles of the circuit (see the example in Fig. 1c).

Subsystem III makes it possible to carry out a "splitting" of the circuit so that the circuit contains no vertices (with the exception of the input poles of the circuit) to which several inputs of elements would be connected (see the example in Fig. 1 –for pole 3).

The system may also contain certain rules connected with the necessity of preserving the number of poles.

Fig. 2

2°. Let us now turn to the consideration of certain types of automata. These automata are constructed from generalizations of "flip-flops" and certain logical elements. Introduce the following operators on sequences $X=(x_0^i,x_1^i,\dots,x_t^i,\dots)$:

1. The operator of digitwise addition of two sequences modulo 2 (notation X^1+X^2).
2. The shift operator D: if $X=(x_0,x_1,x_2,\dots)$, then

$$D[X]=(0,x_0,x_1,\dots);$$

the m-fold application of this operator will be denoted $D^m[X]$.

3. The operator Z_K of periodic summation: if $X=(x_0,x_1,x_2,\dots)$, then $Z_K[X]=(z_0,z_1,z_2,\dots)$, where $z_t=x_t+x_{t-K}+x_{t-2K}+\dots+x_\tau$, $\tau\equiv t$ (mod K), $0\le\tau<K$. For example,

$$Z_3[X]=(x_0,x_1,x_2,x_3+x_0,x_4+x_1,x_5+x_2,x_6+x_3+x_0,\dots).$$

For the operators under consideration the following relations hold:

$$
\begin{aligned}
&1.\quad Z_{2K}[X] = Z_K[Z_K][X].\\
&2.\quad Z_K[X^1 + X^2] = Z_K[X^1] + Z_K[X^2].\\
&3.\quad Z_K[D[X]] = D[Z_K[X]].\\
&4.\quad Z_{K_1}[Z_{K_2}[X]] = Z_{K_2}[Z_{K_1}[X]].\\
&5.\quad D^K[Z_K[X]] = X + Z_K[X].\\
&6.\quad Z_K[X] = Z_{mK}[X] + D^K[Z_{mK}[X]] + D^{2K}[Z_{mK}[X]] + \cdots\\
&\qquad\qquad \cdots + D^{(m-1)K}[Z_{mK}[X]], \quad \text{where } m \geq 1.\\
&7.\quad D^{K-1}[Z_K[X]] = Z_1[X] + Z_K[X] + D[Z_K[X]] + D^2[Z_K[X]] + \cdots\\
&\qquad\qquad \cdots + D^{K-2}[Z_K[X]].\\
&8.\quad Z_1[Z_K[X]] = Z_1[Z_1[X]] + D[Z_K[X]] + D^3[Z_K[X]] + \cdots + D^{K-2}[Z_K[X]],
\end{aligned} \tag{1}
$$

where K is odd, $K > 1$.

Consider the elements that transform input sequences into output sequences:

1. An element realizing the operator of digitwise addition modulo 2 (Fig. 2, I).

2. The identity element, whose output state coincides with the state of its input at the same instant (Fig. 2, II).

3. A delay—an element realizing the shift operator (Fig. 2, III).

4. Elements realizing the constants 0 and 1 (Fig. 2, IV).

5. An element realizing the operator Z_K of periodic summation (Fig. 2, V). This element can be represented in the form of a circuit with feedback (a "loop" in (6)) from an element realizing the operator of addition modulo 2 and K delays (Fig. 3). We shall call it a feedback element of order K, or simply an element of order K.

The greatest odd divisor of the order of a feedback element will be called the principal part of the order of this element. Elements for which the principal parts of the orders coincide will be called of the same type. Elements without feedback will be called elements of zero order. The collection of elements from which circuits are built will be called a basis. We shall consider

bases consisting of elements 1–4 and of some set of elements of type 5.

We shall consider circuits[1] in such bases. For these circuits, all the data in §1 concerning the definition of subcircuits and rules are preserved in full. Only the definition of equivalence of circuits is somewhat changed: the requirement that both circuits realize one and the same function is replaced by the requirement that the output sequences of both circuits coincide when identical input sequences are applied.* Let us consider two special types of circuits.

Fig. 3

Figure 2: Fig. 3

3°. A finite basis M will be called an **A-basis** if: 1) the basis M, together with each element of order $K = 2_0^{pK}$, where K_0 is odd, contains all elements of orders $K_q = 2_0^{qK}$, where $q = 0, 1, 2, \ldots, p-1$; 2) the main parts of any two nonidentical elements of the basis M are mutually prime; 3) the basis M contains an element of order 1.

Fig. 3

Lemma 1. *For any A-basis M there exists a finite system of rules, all circuits of which are circuits in the basis M, such that every chain consisting of two consecutively connected elements of the basis M of odd orders K_1 and K_2 can be transformed, by means of these rules, into an equivalent circuit in which each chain contains elements of only one order K (and also, possibly, elements of zero order).*

Theorem 2. *For any A-basis M there exists a finite system of rules, all circuits of which are circuits in the basis M, such that any two equivalent circuits in this basis can be transformed into one another by means of this system of rules.*

This finite system of rules decomposes into 5 subsystems:

The I subsystem is defined by rules for formulas composed of variables and the constants 0 and 1, joined by addition modulo 2, and by identity functions. For example, the formula $x + x = 0$ defines the rule in Fig. 4a.

The II subsystem is defined by relations (1) (where relation 6 is not used). For example, relation 5 defines the rule in Fig. 4b.

The III subsystem contains rules for absorption of the constant 0 by one-input elements (see the example in Fig. 4c) and absorption of the identity element by any other element (see the example in Fig. 4d).

The IV and V subsystems are analogous to the II and III subsystems of §1 (with the output of the element realizing the constant 1 playing the role of the input pole of the circuit).

This system of rules makes it possible to reduce any circuit to a "canonical circuit," i.e., to a "sum modulo 2" of chains, each of which contains elements of only one order K and no more than $K-2$ delays, as well as chains of delays (the number of delays in such chains is not bounded) and of the identity element. The canonical circuit contains no graphically coincident chains, i.e., chains consisting of one and the same number of identical elements issuing from one and the same pole.

Any two equivalent circuits can be transformed into one another if they reduce to one and the same canonical circuit. The proof of the uniqueness of the

Fig. 4

Figure 3: Fig. 4

canonical circuit for equivalent circuits is based on Lemma 2.

Lemma 2. *Let a canonical circuit be given, all chains of which contain elements of some odd order $K > 1$. If a sequence of ones is applied to the input of this circuit, then the proper period p of the output sequence will be a multiple of some divisor of the number K.*

* It is important to note that the circuits themselves do not contain "feedbacks."

4°. We shall call a finite basis M a B-basis if the basis M contains an element whose order is equal to the least common multiple of the orders of all elements with feedback belonging to M.

Theorem 3. *For any B-basis M there exists a finite system of rules, all circuits of which are circuits in the basis M, such that any two equivalent circuits in this basis can be transformed into one another by means of this system of rules.**

Fig. 4

This system of rules differs from the system of rules of Theorem 2 only by the rules of subsystem II (here relations 1, 7, and 8 are not used). These rules make it possible to reduce any equivalent circuits to one and the same canonical circuit, which is the "sum modulo 2" of chains containing elements of order N (N is the common least multiple of all orders of the elements with feedback of the basis M) and no more than $N - 1$ delays, as well as chains consisting only of delays (the number of delays in such chains is not bounded) and the identity element.

Remark. If one does not require that all circuits in the rules be circuits in the given basis M, but permits the construction of circuits in the rules in a basis M', enlarged with respect to M by only one element (for example, by an element whose order is equal to the least common multiple of the orders of all elements of the set M), then the following is true.

Theorem 4. *For any finite basis M there exists a finite system of rules in the basis M' such that any two equivalent circuits in the basis M can be transformed into one another by means of this system of rules.*

I express my deep gratitude to O. B. Lupanov for his guidance.

Received
16 I 1963

REFERENCES

1. O. B. Lupanov, *Problems of Cybernetics*, 7, Moscow, 1962.

2. V. L. Murskii, *Problems of Cybernetics*, 5, Moscow, 1961.

3. S. V. Yablonskii, *Proceedings of the Mathematical Institute named after V. A. Steklov*, 51 (1958).

4. J. N. Holland, *J. Franklin Inst.*, 270, No. 3 (1960).

5. D. Hilbert, V. Ackermann, *Principles of Theoretical Logic*, Moscow, 1947.

6. N. E. Kobrinskii, B. A. Trakhtenbrot, *Introduction to the Theory of Finite Automata*, Moscow, 1962.

* An analogous result is valid for a finite basis M' having the following properties: 1. together with each element of order $K = 2^p K_0$, where K_0 is odd, the basis M' contains all elements of orders $K_q = 2^q K_0$, where $q = 0, 1, 2, \dots, p-1$. 2. For the least common multiple N of the principal parts of the orders of all elements with feedback belonging to M', the basis M' contains an element of order N.

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