



Soviet-era science, translated into English

AUTOMATON SUBSTITUTIONS AND WREATH PRODUCTS OF GROUPS

1965

SovietRxiv

View the original and related papers at <https://sovietrxiv.org/items/ru-196501.54863>

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

Abstract

Full Text

CYBERNETICS AND CONTROL THEORY

V. P. Zarovnyi

AUTOMATON SUBSTITUTIONS AND WREATH PRODUCTS OF GROUPS

(Presented by Academician V. M. Glushkov on 17 VII 1964)

In the author's paper ⁽¹⁾ it was shown that the group $A(n)$ of all automaton one-to-one mappings of the set $F(n)$ of words in the alphabet $\mathfrak{X} = (x_1, \dots, x_n)$ of n letters onto itself, as well as its subgroup $K(n)$ of finite-automaton mappings, are isomorphic to the direct products of the groups $K(n, r)$, $r = 1, 2, \dots$, of automaton substitutions of the sets $F(n, r)$ of words of length r in the alphabet \mathfrak{X} . Below we give results of an investigation of the structure of the groups $K(n, r)$, the group $A(n)$, and, on this basis, obtain a new necessary and sufficient criterion for finite-automatonness of automaton one-to-one mappings.

1. In connection with the study of Sylow subgroups of groups of substitutions, a construction called the wreath product of groups ⁽²⁾ was studied: if V_0, \dots, V_{r-1} are given sets, and G_0, \dots, G_{r-1} are groups of substitutions of these sets, respectively, then the **wreath product of the groups** $G_0 \wr G_1 \wr \dots \wr G_{r-1}$ is the group of such substitutions g of the set $V = V_0 \times \dots \times V_{r-1}$ that for any word $p = x_{i_0} \dots x_{i_{r-1}}$ the equality

$$pg = [x_{i_0}g_0({}^0p)] \dots [x_{i_{r-1}}g_{r-1}({}^{r-1}p)], \tag{1}$$

holds, where ${}^\mu p = x_{i_{\mu+1}} \dots x_{i_{r-1}}$, and $g_\mu({}^\mu p)$ is a function defined on $V_{\mu+1} \times \dots \times V_{r-1}$ with values in G_μ , $\mu = 0, \dots, r-1$. Thus the substitution g is specified by the sequence $[g_0({}^0p), \dots, g_{r-1}({}^{r-1}p)]$ and by the action rule (1). In this definition replace ${}^\mu p$ by $p^\mu = x_{i_0} \dots x_{i_{\mu-1}}$ and $V_{\mu+1} \times \dots \times V_{r-1}$ by $V_0 \times \dots \times V_{\mu-1}$. The set of substitutions \bar{g} of the set V for which

$$p\bar{g} = [x_{i_0}\bar{g}_0(p^0)] \dots [x_{i_{r-1}}\bar{g}_{r-1}(p^{r-1})], \tag{2}$$

where $\bar{g}_\mu(p^\mu)$ are functions defined on $V_0 \times \dots \times V_{\mu-1}$ with values in G_μ , is a group, which we shall call the **dual wreath product of the groups** $G_0 \bar{\wr} G_1 \bar{\wr} \dots \bar{\wr} G_{r-1}$. Each substitution from the dual wreath product is determined by the sequence of functions $[\bar{g}_0(p^0), \dots, \bar{g}_{r-1}(p^{r-1})]$ and by the action rule (2).

Theorem 1. *For $n \geq 2$ and any natural $r \geq 1$, the group $K(n, r)$ is the dual wreath product of r symmetric groups of degree n :*

$$K(n, r) = \underbrace{S_n \bar{\wr} S_n \bar{\wr} \cdots \bar{\wr} S_n}_r.$$

The following proposition makes it possible to apply to the study of the groups $K(n, r)$ (taking Theorem 1 into account) the results—still rather few—on wreath products of groups.

Proposition 1. *The wreath product $G_0 \wr G_1 \wr \cdots \wr G_{r-1}$ and the dual wreath product $G_{r-1} \bar{\wr} G_{r-2} \bar{\wr} \cdots \bar{\wr} G_0$ are similar groups of substitutions. Moreover, the indicated similarity can be realized as follows: if*

$$p = x_{i_0} \cdots x_{i_{r-1}} \in V_0 \times \cdots \times V_{r-1},$$

then $p \rightarrow \bar{p} = x_{i_{r-1}} \cdots x_{i_0} \in V_{r-1} \times \cdots \times V_0$,

and if $g = [g_0(p^0), \dots, g_{r-1}(p^{r-1})]$, then $g \rightarrow \bar{g} = [\bar{g}_0(p^0), \dots, \bar{g}_{r-1}(p^{r-1})]$, where

$$\bar{g}_\mu(p^\mu) = g_{r-\mu-1}(p^{r-\mu-1}).$$

2. If $g = [g_0(p^0), \dots, g_{r-1}(p^{r-1})] \in G_0 \wr \cdots \wr G_{r-1}$, then the action of g can be extended to any word p from $V_0 \times \cdots \times V_\mu$, $0 \leq \mu < r - 1$, by setting

$$pg = (x_{i_0} \dots x_{i_\mu})g = [x_{i_0}g_0(p^0)] \dots [x_{i_\mu}g_\mu(p^\mu)]. \quad (3)$$

Thus the dual wreath product $G_0 \bar{\wr} \cdots \bar{\wr} G_{r-1}$ can be regarded as a group of substitutions of the set

$$\bigcup_{\mu=0}^{r-1} (V_0 \times \cdots \times V_\mu).$$

We generalize this approach to the case of a countable set of groups G_μ , $\mu = 0, 1, 2, \dots$; namely, we shall call the set of substitutions g (which turns out to be a group) of the set

$$\bigcup_{\mu=0}^{\infty} (V_0 \times \cdots \times V_\mu),$$

for which, for any r and any $p \in V_0 \times \cdots \times V_{r-1}$, an equality of the form (3) holds, the **dual wreath product** of the groups G_0, G_1, \dots . Together with such an action rule, a sequence of functions

$$[g_0(p^0), \dots, g_r(p^r), \dots]$$

completely determines the substitution g .

Theorem 2. The group $A(n)$, for any $n \geq 2$, is the dual wreath product of a countable set of symmetric groups of degree n :

$$A(n) = S_n \bar{\wr} S_n \bar{\wr} \cdots \bar{\wr} S_n \bar{\wr} \cdots.$$

3. We fix the following numbering of the words of each length in the alphabet $\mathfrak{X} = (x_1, \dots, x_n)$ (each word is numbered by two indices, the first of which denotes the length of the word, and the second its number among the words of this length):

- 1) $p_{1i} = x_i$, where i is the number of the letter in the alphabet \mathfrak{X} ;
- 2) if $p = p_{r-1;j}x_i$, then $p = p_{r;n(i-1)+j}$.

Introduce the function

$$\begin{aligned} \omega(r, i, t; k_1, \dots, k_{t-1}) &= \\ &= n^{t-1}(i-1) + n^{t-2}(k_1-1) + \dots + n(k_{t-2}-1) + k_{t-1}, \end{aligned}$$

where $1 \leq i \leq n^{r-1}$; $t = 0, 1, 2, \dots$; $1 \leq k_1, k_2, \dots, k_{t-1} \leq n$; $r = 1, 2, \dots$. It can be shown that

$$\omega(r, i, t; k_1, \dots, k_{t-1}) < n^{r+t-1}. \quad (4)$$

Now let $\varphi = [\varphi_0(p^0), \dots, \varphi_{r-1}(p^{r-1}), \dots]$ be an automaton mapping from $A(n)$, written as an element of the dual wreath product of a countable set of symmetric groups (see Theorem 2) through the function $\varphi_r(p^r)$, defined on

$$\bigcup_{i=1}^r F(n, i)$$

with values in S_n . Consider the sets of the following values of these functions for fixed r and i :

$$\varphi_{r+1}(p_{r+t-1; \omega(r, i, t; k_1, \dots, k_{t-1})}),$$

where t runs through the natural series, $t = 1, 2, \dots$, and k_j , $j = 1, \dots, t-1$, vary, for each t , within the limits from 1 to n . We denote the system of these values by $E(\varphi, r, i)$:

$$E(\varphi, r, i) = \{\varphi_{r+1}[p_{r+t-1; \omega(r, i, t; k_1, \dots, k_{t-1})}]; t = 1, 2, \dots; k_j = 1, \dots, n\}.$$

This notation is meaningful for all values of t and k_j in the indicated limits, since, according to (4), any corresponding value of the function ω for given fixed r and i can serve as the number of a word of length $r+t-1$: the number of these words is exactly n^{r+t-1} . For any natural nonzero number r and any natural number i lying between 1 and n^{r-1} , we shall call the system $E(\varphi, r, i)$ an **element**, or the (r, i) -**element**, of the mapping φ .

On the set of all possible (r, i) -elements of the mapping, define two relations: $\overset{x_l}{\simeq}$ (x_l -similarity), where $x_l \in \mathfrak{X}$, and \sim (similarity of blocks), by the following conditions:

$$E(\varphi, r, i) \overset{x_l}{\simeq} E(\varphi, s, j) \iff$$

$$\Leftrightarrow \forall k \forall (k_1, \dots, k_{t-1}) \forall t \left\{ \begin{array}{l} [(x_k \varphi_{r+t}(p_{r+t-1}; \omega(r, i, t; k_1, \dots, k_{t-1})) = x_i) \Rightarrow \\ \Rightarrow (x_k \varphi_{s+t}(p_{s+t-1}; \omega(s, j, t; k_1, \dots, k_{t-1})) = x_i)] \& \\ [(x_k \varphi_{r+t}(p_{r+t-1}; \omega(r, i, t; k_1, \dots, k_{t-1})) \neq x_i) \Rightarrow (x_k \varphi_{s+t}(p_{s+t-1}; \omega(s, j, t; k_1, \dots, k_{t-1})) \neq x_i)] \end{array} \right\}$$

$$\begin{aligned} E(\varphi, r, i) \sim E(\varphi, s, j) &\Leftrightarrow \forall k_1, \dots, k_{t-1} \forall t \{ \varphi_{r+t}(p_{r+t-1}; \omega(r, i, t; k_1, \dots, k_{t-1})) = \\ &= \varphi_{s+t}(p_{s+t-1}; \omega(s, j, t; k_1, \dots, k_{t-1})) \}. \end{aligned}$$

It is easy to verify that both these relations are equivalences on the set of all elements of the mapping φ . The equivalence classes with respect to x_l will be called the **x_l -blocks of the mapping φ** , and the equivalence classes with respect to \sim simply **blocks of the mapping**.

4. We now have the possibility of formulating a necessary and sufficient criterion for the finite-automaton property of an automaton mapping.

Lemma 1. If $\varphi \in A(n)$, then the following assertions are equivalent:

- a) φ is a finite-automaton mapping (i.e. $\varphi \in K(n)$);
- b) the number of x_l -blocks of the mapping φ is finite for every $x_l \in \mathfrak{X}$;
- c) the number of blocks of the mapping φ is finite.

The idea of the proof is as follows. We consider the equivalence $\overset{x_l}{\simeq}$ on $F(n)$, for $x_l \in \mathfrak{X}$, defined by the condition

$$p \overset{x_l}{\simeq} q \Leftrightarrow \forall u [(pu \in S_{x_l} \Rightarrow qu \in S_{x_l}) \& (pu \in S_{x_l} \Rightarrow qu \notin S_{x_l})],$$

where S_{x_l} is the event marked by the letter x_l under the mapping φ , i.e. the set of words of $F(n)$ whose images under the mapping φ end in x_l . Further, to each word $p = p_{r_i}$ under the numbering 1), 2) of item 3 we assign the element $E(\varphi, r, i)$ of the mapping φ . This gives a one-to-one correspondence between the classes with respect to $\overset{x_l}{\simeq}$ on $F(n)$ and the x_l -blocks of the mapping φ . To show this, it is necessary to establish that, for $u = x_{k_1} \dots x_{k_t}$,

$$pu = p_{r+t; \omega(r, i, t+1; k_1, \dots, k_{t-1}, k_t)}$$

and that

$$(pu)\varphi = [p_{r_i}\varphi] [x_{k_1}\varphi_r(p_{r; \omega(r, i, 1; \emptyset)})] [x_{k_2}\varphi_{r+1}(p_{r+1; \omega(r, i, 2, k_1)})] \times \dots$$

$$\cdots \times [x_{k_t} \varphi_{r+t-1}(p_{r+t-1; \omega(r, i, t; k_1, \dots, k_{t-1})})].$$

After this it is not difficult to see that the condition $pu \in S_{x_l}$ is equivalent to the condition

$$x_{k_1} \varphi_{r+t}(p_{r+t-1; \omega(r, i, t; k_1, \dots, k_{t-1})}) = x_l.$$

The situation is analogous with qu . Comparing the last condition with the definition of $\overset{x_l}{\simeq}$, we find that the relation $p \overset{x_l}{\simeq} q$ is equivalent to the relation $E(\varphi, r, i) \overset{x_l}{\simeq} E(\varphi, s, j)$.

By theorem 2 of paper (3), representability of the event S_{x_l} in a finite automaton is equivalent to finiteness of the index of the equivalence $\overset{x_l}{\simeq}$, or, as

we see the finiteness of the index of the relation $\overset{x_l}{\sim}$. Thus the implication a) \Rightarrow b) is obtained.

The proof of the implication b) \Rightarrow c) is based on the equality

$$\bigcap_{l=1}^n \overset{x_l}{\sim} = \sim:$$

since l ranges over a finite set, the finiteness of the index of each of the relations $\overset{x_l}{\sim}$, on the basis of this equality, gives the finiteness of the index of the relation \sim .

Without difficulty, from the finiteness of the index of the relation \sim , one now obtains the finiteness of the index of each of the relations $\overset{x_l}{\sim}$, whence, by Theorem 2 from (3), it follows that each S_{x_l} is regular, i.e. φ is finite-automaton.

5. The obtained criterion for being finite-automaton can be made more transparent as follows. Let $\varphi = [\varphi_1(p^1), \dots, \varphi_r(p^r), \dots] \in A(n)$. For $p \in F(n, r)$ denote by φ_p the mapping $\psi = [\psi_1(u^1), \dots, \psi_r(u^r), \dots]$, for which, for $u \in F(n, s)$,

$$\psi_i(u^i) = \varphi_{r+i}[(pu)^{r+i}], \quad i = 1, \dots, s.$$

Introduce the binary relation ∇ on the set $A(n)$ by the condition:

$$(\varphi \nabla \psi) \iff \exists p \in F(n) \quad (\psi = \varphi'_p).$$

This relation is a partial quasi-order. We shall agree to say that the mapping φ is covered by the mapping ψ , if $\varphi \nabla \psi$.

From the equivalence of a) and b) of Lemma 1 there now follows

Theorem 3. *In order that a mapping $\varphi \in A(n)$ be finite-automaton, it is necessary and sufficient that it be covered by a finite number of mappings from $A(n)$. Moreover, if some finite-automaton mapping is covered by a mapping $\varphi \in A(n)$, then φ also is finite-automaton.*

6. On the basis of the results of Sec. 1 and of the work ⁽¹⁾ the following can be proved

Theorem 4. *The groups $A(n)$ and $K(n)$, for $n \geq 2$, do not possess finite systems of generators.*

The idea of the proof is as follows: according to (1), each of the groups $A(n)$ and $K(n)$ is isomorphic to a certain subdirect product of the groups $K(n, r)$, $r = 1, 2, \dots$, as a result of which the least number of generators in $A(n)$ and in $K(n)$ is no smaller than the same number for any $K(n, r)$, $r = 1, 2, \dots$, and therefore, in order to complete the proof of Theorem 4, taking Theorem 1 into account, the following lemma is sufficient:

Lemma 2. *The least number of generators of the group*

$$\underbrace{S_n \wr S_n \wr \dots \wr S}_r$$

is not less than the number r , so that this number for $K(n, r)$ increases with the growth of r and can become arbitrarily large.

The proof of this lemma was kindly communicated to the author by L. A. Kaluzhnin.

The author expresses deep gratitude to Academician V. M. Glushkov and L. A. Kaluzhnin for valuable advice and comments.

Ivanovo-Frankovsk
State Pedagogical Institute

Received
25 V 1964

CITED LITERATURE

¹ V. P. Zarovnyi, DAN, **156**, No. 6 (1964). ² P. Hall, Proc. Cambridge Phil. Soc., **58**, No. 2, 170 (1962). ³ M. O. Rabin, D. Scott, Kibernetich. sborn., **4**, 58 (1962).

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

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