Miskolc Mathematical Notes
Vol. 2 (2001), No 1, pp. 61-68

HU e-ISSN 1787-2413
DOI: 10.18514/MMN.2001.36

Algebraic models for disrete systems' analysis

Volodimyr G. Skobelev

Mathematical Notes, Miskolc, Vol. 2., No. 1., (2001), pp. 61–68

ALGEBRAIC MODELS FOR DISCRETE SYSTEMS' ANALYSIS

Volodimyr G. Skobelev
Institute for Applied Mathematics and Mechanics
of the National Academy of Sciences of Ukraine, Donetsk, Ukraine
skbv@iamm.ac.donetsk.ua

[Received February 19, 2001]

Abstract. The present paper deals with algebraic models and methods sufficient to solve effectively problems of investigation of two basic classes of control systems, namely, finite automata and boolean functions. Suggested models for finite automata are based on finite groups and result in establishing basic algebraic characteristics, developing a general scheme for estimating exponential lower bounds and in the design of nonstationary secret locks of arbitrary high complexity. It is also shown that the problem of the identification of boolean vector-functions may be effectively solved via the methods of the Theory of Vector Spaces over $GF(2)$.

Mathematical Subject Classification: 20B30, 20D99, 12Y05, 68R69
Keywords: Automata, boolean functions, finite groups and fields.

1. Introduction

It is well known that solving of the majority of problems of investigation of finite automata and boolean functions is based on exhaustive searching. The main disadvantage of these methods is their high complexity. Besides, many important properties of the structure of investigated objects are not taken into account at all since the applied tools are very limited. On the other hand, many problems of analysis, description, classification, estimation and effective algorithm design may be solved by powerful methods of Modern Algebra. Thus it is natural to present finite automata and boolean functions via basic algebraic structures. This gives the possibility to explore effectively algebraic characteristics of these structures in solving the investigated problems. Three basic problems are solved in what follows.

The first one is the presentation of mappings performed by finite automata via finite groups. This results in an exhaustive investigation of algebraic characteristics and the extraction of a special subclass of permutation automata. This subclass is basic for the design of nonstationary secret locks of arbitrary high complexity.

The second one is the elaboration of a general scheme for establishing the exponential lower bounds. The suggested scheme is based on the selection of permutation with special characteristics. This directly results in establishing the lower bounds for Shennon's functions estimating the maximum of the minimal lengths of distinguishing and synchronizing sequences for weakly initialized automata as well as of the complexity of the secret locks designed.

The third one is the identification of boolean vector-functions via the methods of the Theory of Vector Spaces over $GF(2)$. The suggested scheme is based on presenting the graph of any boolean vector-function via the union of special subspaces of $GF^{m+n}(2)$. This results in the design of a characteristic function in the form of a set of special matrices over the field $GF(2)$.

All notions that are not determined are the same as in [1-7].

2. Automata and groups

An automaton is a quintuple $A = (Q, X, Y, \delta, \lambda)$ (Q is *a set of states*, X and Y are *input* and *output alphabets*, $\delta : Q \times X \to Q$ and $\lambda : Q \times X \to Y$ are *transition* and *output mappings*). It is suggested that Q, X and Y are finite sets. Usually an automaton is interpreted as a model of a discrete device or as an algorithm. It is also evident that an automaton is *a Heterogeneous Algebra*. Thus algebraic methods are directly applied in the Automata Theory. Indeed, the investigation of congruences of *the free semigroup* X^* leads to *the Krohn-Rhodes Decomposition Theory.* Similarly, the investigation under conditions that δ and λ are presented via linear transformations of vector spaces leads to a restricted but very important class of *Linear Sequential Machines.* It is natural to present δ and λ via operations in arbitrary finite groups since the last ones are one of the best examined algebraic systems. Basic properties of this presentation were investigated in [1,2].

Let $\mathcal{A}_{mnk}$ ($m, n, k \in \mathbf{N}, k \geq 2$) be the set of all automata $A = (Q_k, X_m, Y_n, \delta_A, \lambda_A)$, where $Q_k = \{q_1, \ldots, q_k\}$, $X_m = \{x_1, \ldots, x_m\}$, $Y_n = \{y_1, \ldots, y_n\}$ and $\mathcal{G}_1 = (G_1, \circ)$ and $\mathcal{G}_2 = (G_2, \star)$ be finite groups. $\mathcal{F}_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$ denotes the set of all 6-tuples $F = (f_1, f_2, f_3, f_4, f_5, f_6)$ of mappings, where $f_1 : Q_k \to G_1$, $f_2 : X_m \to G_1$, $f_3 : G_1 \to Q_k$, $f_4 : Q_k \to G_2$, $f_5 : X_m \to G_2$, $f_6 : G_2 \to Y_n$. An automaton $B_F = (Q_k, X_m, Y_n, \delta_F, \lambda_F)$ ($F \in \mathcal{F}_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$) is determined by the identities

$$\delta_F(q, x) = f_3(f_1(q) \circ f_2(x)), \lambda_F(q, x) = f_6(f_4(q) \star f_5(x)) \quad (q \in Q_k, x \in X_m).$$

Let $\mathcal{A}_{mnk}(\mathcal{G}_1, \mathcal{G}_2) = \{A_F | F \in \mathcal{F}_{mnk}(\mathcal{G}_1, \mathcal{G}_2)\}$. It is evident that $\emptyset \neq \mathcal{A}_{mnk}(\mathcal{G}_1, \mathcal{G}_2) \subseteq \mathcal{A}_{mnk}$ for any finite groups $\mathcal{G}_1$ and $\mathcal{G}_2$. Moreover, the following characteristics are established.

Theorem 1 [1]. If sequences of finite groups $\{\mathcal{G}_1^{(j)} | j \in \mathbf{N}\}$ and $\{\mathcal{G}_2^{(j)} | j \in \mathbf{N}\}$ are under the conditions $\mathcal{G}_i^{(1)} \leq \mathcal{G}_i^{(2)} \leq \ldots \mathcal{G}_i^{(j)} \leq \ldots$ $(i = 1, 2)$, then

$$\emptyset \neq \mathcal{A}_{mnk}(\mathcal{G}_1^{(1)}, \mathcal{G}_2^{(1)}) \subseteq \mathcal{A}_{mnk}(\mathcal{G}_1^{(2)}, \mathcal{G}_2^{(2)}) \subseteq \cdots \subseteq \mathcal{A}_{mnk}(\mathcal{G}_1^{(j)}, \mathcal{G}_2^{(j)}) \subseteq \cdots \subseteq \mathcal{A}_{mnk}.$$

Theorem 2 [1]. If there exist cyclic groups $\mathcal{Z}_{l_1} = (\mathbf{Z}_{l_1}, \oplus_{mod\ l_1})$ and $\mathcal{Z}_{l_2} = (\mathbf{Z}_{l_2}, \oplus_{mod\ l_2})$ such that $\mathcal{Z}_{l_i} \leq \mathcal{G}_i$ $(i = 1, 2)$ and $\min\{l_1, l_2\} \geq mk$ then $\mathcal{A}_{mnk}(\mathcal{G}_1, \mathcal{G}_2) = \mathcal{A}_{mnk}$.

It is worth noting that Theorem 2 justifies ROM-realizations of finite automata and extracts a sufficiently wide class of these realizations in an explicit form.

If $A = B_F$ $(A \in \mathcal{A}_{mnk}, B_F \in \mathcal{A}_{mnk}(\mathcal{G}_1, \mathcal{G}_2))$ then B_F is $(\mathcal{G}_1, \mathcal{G}_2)$-*presentation* of A. At every instant of time computations performed by an automaton B_F realize the scheme

coding → operations in groups → decoding.

This scheme is inconvenient if for an automaton $A = (Q_k, X_m, Y_n, \delta_A, \lambda_A)$ transition and output mappings' extensions on the set $Q_k \times X_m^*$ are determined by the identities

$$\delta_A(q, \Lambda) = q, \lambda_A(q, \Lambda) = \Lambda, \delta_A(q, px) = \delta_A(\delta_A(q, p), x), \lambda_A(q, px) = \\ = \lambda_A(q, p)\lambda_A(\delta_A(q, p), x),$$

where $q \in Q_k, p \in X_m^*, x \in X_m$ and Λ is the empty string. It is more preferable to code a state in the initial instant of time and to decode an element of a group into a state in the final instant of time only. Thus it is natural to extend a mapping $f_2 : X_m \to G_1$ onto the set X_m^* and extract the following subset $\mathcal{F}^c_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$ of the set $\mathcal{F}_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$: $F = (f_1, \ldots, f_6) \in \mathcal{F}^c_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$ if $\delta_F(q, p) = f_3(f_1(q) \circ f_2(p))$ for all $q \in Q_k$ and $p \in X_m^*$. The subset $\mathcal{F}^c_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$ is determined by the following criteria.

Theorem 3 [2]. $F = (f_1, \ldots, f_6) \in \mathcal{F}^c_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$ if and only if there exists an extension of the mapping f_2 onto the set X_m^* such that the identities

$$f_3(f_1(q) \circ f_2(\Lambda)) = q, \quad f_3(f_1(q) \circ f_2(px)) = f_3(f_1(f_3(f_1(q) \circ f_2(p))) \circ f_2(x))$$

hold for all $q \in Q_k, p \in X_m^*, x \in X_m$.

The following basic characteristics of the subset $\mathcal{F}^c_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$ are established.

Theorem 4 [2]. $\mathcal{F}^c_{mnk}(\mathcal{G}_1, \mathcal{G}_2) = \emptyset$ for any group $\mathcal{G}_1 = (G_1, \circ)$ such that $|G_1| < k$.

Theorem 5 [2]. There exists a group $\mathcal{G}_1 = (G_1, \circ)$ such that $|G_1| = k$ and $\mathcal{F}^c_{mnk}(\mathcal{G}_1, \mathcal{G}_2) \neq \emptyset$.

Theorem 6 [2]. Let $\mathcal{G}_1 = (G_1, \circ)$ be any group such that $|G_1| = k$ and $\mathcal{F}^c_{mnk}(\mathcal{G}_1, \mathcal{G}_2) \neq \emptyset$. Let $F = (f_1, \ldots, f_6) \in \mathcal{F}^c_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$ and f_2 be extended onto the set X_m^*. Then B_F is a permutation automaton consisting of $k/|Val\ f_2|$ strongly connected components, each of $|Val\ f_2|$ states.

Theorem 7 [2]. Let $F = (f_1, \ldots, f_6) \in \mathcal{F}^c_{mnk}(\mathcal{G}_1, \mathcal{G}_2)$ and f_2 be extended onto the set X_m^*. If $f_2(\Lambda)$ is the identity element of the group $\mathcal{G}_1$ and $Val\ f_1 \circ Val\ f_2 = Val\ f_1$, then f_2 is a homeomorphism of the free semigroup X_m^* into the group $\mathcal{G}_1$.

Theorem 6 extracts permutation automata with strongly connected components consisting of the same number of states. It is natural to present these automata via well examined groups. For autonomous automata this problem was investigated in [2,3].

Let $A_i = (Z_{k_i}, \{x\}, \delta_i)$ $(i = 1, \dots, n)$ be a sequence of counters, i.e., $\delta_i(z, x) = z+1$ $(mod\ k_i)$ for all $z \in Z_{k_i}$ and $\chi(A_1, \dots, A_n) = (A_1 \times \dots \times A_n, \{x\}, \delta)$, where

$$\delta(z_1, \dots, z_n) = (\delta_1(z_1, x), \dots, \delta_n(z_n, x))$$

for all $(z_1, \dots, z_n) \in A_1 \times \dots \times A_n$.

Theorem 8 [2,3]. The automaton $\chi(A_1, \dots, A_n)$ consists of $GCD(k_1, \dots, k_n)$ strongly connected components, each of $LCM(k_1, \dots, k_n)$ states.

Theorem 8 implies that an autonomous automaton B with k states consisting of u strongly connected components, each of v states, is isomorphic to an automaton $\chi(A_1, \dots, A_l)$ if and only if canonical forms $k = p_1^{\gamma_1} \dots p_r^{\gamma_r}$, $u = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $v = p_1^{\beta_1} \dots p_r^{\beta_r}$, $k_i = p_1^{\mu_{i1}} \dots p_r^{\mu_{ir}}$ $(i = 1, \dots, l)$ satisfy the conditions

$$\alpha_j + \beta_j = \gamma_j \ \ (j = 1, \dots, r),$$

$$\mu_{1j} + \dots + \mu_{lj} = \gamma_j \ \ (j = 1, \dots, r),$$

$$\min\{\mu_{1j}, \dots, \mu_{lj}\} = \alpha_j \ \ (j = 1, \dots, r),$$

$$\max\{\mu_{1j}, \dots, \mu_{lj}\} = \beta_j \ \ (j = 1, \dots, r).$$

3. Exponential lower bounds

The estimation of Shennon functions' lower bounds is one of the fundamental problems of Discrete Mathematics. Indeed, it is an integral part of algorithms' complexity analysis. The complexity of this problem is justified by the fact that the unique method for solving it is to design an object on which this estimation is accessible explicitly, as a rule. Moreover, the higher the lower bound is, the more difficult is to design the corresponding object. Thus a natural way to reduce the complexity of lower bounds' estimation is to elaborate abstract mathematical schemes with prescribed values of parameters and to give an interpretation in terms of specific discrete problems. In the case when lower bounds are exponents this problem was solved in [4].

Let *a permutation* $g \in S_n$ be presented as the product of cycles, i.e., $g = D_{r_1} \dots D_{r_l}$, where D_h $(h = r_1, \dots, r_l)$ is h-cycle. Then $order(g) = LCM(r_1, \dots, r_l)$. Thus if $f = D_{r+1}, \dots, D_{2r} \in S_n$, then $order(f) = LCM(r+1, \dots, 2r) =$ $= LCM(1, \dots, 2r)$. Since [5] $e^{c_1 x} < LCM(1, \dots, x) < e^{c_1 x}$ $(x \geq 2)$, where c_1, c_2 $(0 < c_1 < c_2)$ are constants, then $order(f) = e^{O(r)}$ $(r \to \infty)$.

Theorem 9. [4]. If $f = D_{r+1} \dots D_{2r} \in S_n$ $(r = \lfloor \frac{1}{6} \sqrt{(24n+1)} - 1 \rfloor)$, then

$$order(f) = e^{O(\sqrt{n})} \ \ (n \to \infty).$$

This scheme was applied in [6] for estimating the lengths of minimal distinguishing and synchronizing sequences for weakly initialized automata and in [3] for the design of recursive locks of arbitrary high complexity.

A weakly initialized automaton (via) is a pair (A, Q_{in}), where $A \in \mathcal{A}_{mnk}$ and $Q_{in} \subseteq Q_k$ $(|Q_{in}| \geq 2)$. For a via (A, Q_{in}) a sequence $p \in X_m^*$ is:

1) *distinguishing*, if $\delta_A(q,p) = \delta_A(q',p) \Longrightarrow \lambda_A(q,p) = \lambda_A(q',p)$ for all $q, q' \in Q_{in}$;

2) *synchronizing*, if $|\delta_A(Q_{in}, p)| = 1$.

Let there be selected pair-wise disjoint subsets $W_1, \ldots, W_{r-1}$ of the set $Q_k \backslash \{q_1\}$, where

$$W_i = \{q_{\alpha(i)+j} | j = 0, 1, \ldots, l+i-1\} \ \ (i = 1, \ldots, r-1)$$

and $\alpha(i) = 2 + l(i-1) + 0.5i(i-1)$. These subsets exist for all $r \in \{2, \ldots, \lfloor 0.5(\sqrt{8k-7} + 1) \rfloor\}$ and $l \in \{0, 1, \ldots, \lfloor \frac{1}{2(r-1)}(2(k-1) - r(r-1)) \rfloor\}$. Let (A, Q_{in}) be the via, where $A \in \mathcal{A}_{2nk}$, $Q_{in} = \{q_1, q_{\alpha(1)}, \ldots, q_{\alpha(r-1)}\}$ and

$$\delta_A(q_u, x_v) = \begin{array}{ll} q_{u+1}, & \text{if } v = 1 \text{ and } q_u \in W_i \backslash \{q_{\alpha(i+1)-1}\} \ (i = 1, \ldots, r-1), \\ q_{\alpha(i)}, & \text{if } v = 1 \text{ and } u = \alpha(i+1) - 1 \ (i = 1, \ldots, r-1), \\ q_1, & \text{if } v = 2 \text{ and } q_u \in W_1 \cup \cdots \cup W_{r-1}, \\ q_1, & \text{if } v = 1, 2 \text{ and } u = 1\,, \end{array}$$

$$\lambda_A(q_u, x_v) = \begin{array}{ll} y_1, & \text{if } v = 1 \text{ and } q_u \in W_1 \cup \cdots \cup W_{r-1}, \\ y_1, & \text{if } v = 2 \text{ and } q_u \in W_i \backslash \{q_{\alpha(i+1)-1}\} \ (i = 1, \ldots, r-1), \\ y_{i+1}, & \text{if } v = 2 \text{ and } u = \alpha(i+1) - 1 \ (i = 1, \ldots, r-1), \\ y_1, & \text{if } v = 1, 2 \text{ and } u = 1\,. \end{array}$$

Similarly, let there be selected pair-wise disjoint subsets $U_1, \ldots, U_{r-1}$ of the set $Q_k \backslash \{q_1, q_2\}$, where $U_i = \{q_{\beta(i)+j} | j = 0, 1, \ldots, l+i-1\}$ $(i = 1, \ldots, r-1)$ and $\beta(i) = \alpha(i) + 1$. These subsets exist for all $r \in \{2, \ldots, \lfloor 0.5(\sqrt{8k-15} + 1) \rfloor\}$. Let (B, Q_{in}) be the via, where $B \in \mathcal{A}_{2nk}$, $Q_{in} = \{q_1, q_{\beta(1)}, \ldots, q_{\beta(r-1)}\}$ and

$$\delta_B(q_u, x_v) = \begin{array}{ll} q_{u+1}, & \text{if } v = 1 \text{ and } q_u \in U_i \backslash \{q_{\beta(i+1)-1}\} \ (i = 1, \ldots, r-1), \\ q_{\beta(i)}, & \text{if } v = 1 \text{ and } u = \beta(i+1) - 1 \ (i = 1, \ldots, r-1), \\ q_2, & \text{if } v = 2 \text{ and } q_u \in U_i \backslash \{q_{\beta(i+1)-1}\}, \\ q_1, & \text{if } v = 2 \text{ and } u = \beta(i+1) - 1 \ (i = 1, \ldots, r-1), \\ q_u, & \text{if } v = 1, 2 \text{ and } u = 1, 2\,. \end{array}$$

$\delta_A|_{W_1 \cup \cdots \cup W_{r-1}}$ and $\delta_B|_{U_1 \cup \cdots \cup U_{r-1}}$ are permutations of the sets $W_1 \cup \cdots \cup W_{r-1}$ and $U_1 \cup \cdots \cup U_{r-1}$, correspondingly, and consist of the cycles of the lengths $l+1, \ldots, l+r-1$. Thus the sequence $x_1^\mu x_2$, where $\mu = LCM(l, l+1, \ldots, l+r-2)$ is the single minimal distinguishing one for the via (A, Q_{in}) and the single minimal synchronizing one for the via (B, Q_{in}). To establish that the lower bound for the maximal lengths of minimal distinguishing and synchronizing sequences for automata $A \in \mathcal{A}_{2nk}$ is $e^{O(\sqrt{k})}$ $(k \to \infty)$, it is sufficient to set $l = r - 2$ and $r = O(\sqrt{k})$ $(k \to \infty)$.

A recursive secret lock [3] is designed in the following way. Let $A_i = (Z_{k_i}, \{x\}, \delta_i)$ $(i = 1, \ldots, l)$ be fixed sequence of counters, where $k_1 \ldots k_l = k$. *The key* is an automaton $\chi(A_1, \ldots, A_l)$ which states are identified with the states of its isomorphic image $B \in \mathcal{A}_{1nk}$, such that

$$\delta_B(q_{r\nu+j}, x) = \begin{array}{ll} q_{r\nu+j+1}, & \text{if } j = 1, \ldots, \nu - 1 \\ q_{r\nu+1}, & \text{if } j = \nu \end{array} \qquad (r = 0, 1, \ldots, \mu - 1)$$

where $\mu = GCD(k_1, \ldots, k_l)$ and $\nu = LCM(k_1, \ldots, k_l)$. It is suggested that the key may be installed instantly at any of the states $q_{r\nu+1}$ $(r = 0, 1, \ldots, \mu - 1)$. Let $\varphi : N \to \{\nu, 2\nu, \ldots, \mu\nu\}$ be any recursive piecewise constant function with the length of any step (i.e. interval of permanent values) higher than ν. *A recursive secret lock* is a predicate $P_\varphi : \mathbf{N} \times Q_k \times \mathbf{N} \to \{0, 1\}$, where

$$P_\varphi(t, q, h) = 1 \Longleftrightarrow (q = q_{r\nu+1})\&(\delta_B(q_{r\nu+1}, x^h) = q_{\varphi(t+h)}).$$

Thus to open the lock it is necessary to install the key correctly and to apply the sequence x^h, where h is multiple of $\nu - 1$. Let $k_i = l + i$ $(i = 1, \ldots, l)$. The minimal admissible value of h is under the condition $h = e^{O(l)}$ $(l \to \infty)$. This implies that the suggested method gives the possibility to design nonstationary secret locks of arbitrary high level of complexity.

4. Identification of boolean functions

On-line control of discrete devices is often reduced to real-time analysis of corresponding input-output pairs. If the analyzed device is a combinational circuit it realizes the prescribed boolean vector-function $f : \{0, 1\}^m \to \{0, 1\}^n$. Thus the Problem is formulated as follows: for the given boolean vector-function f and a set $\Omega \subset \{0, 1\}^{m+n}$ it is necessary to check if the inclusion $\Omega \subseteq graph(f)$ holds. This Problem may be easily reduced to the classic Problem of boolean functions' identification. Thus classic methods based on searching are directly applied. The main disadvantage of these methods is their high complexity. To reduce the complexity it is natural to replace searching by algebraic operations wherever it is possible. This problem was solved in [7]. The main idea of the suggested approach is to explore the fact that $\{0, 1\}^{m+n}$ is the vector space $GF^{m+n}(2)$.

Let $P_{m,n}$ be the set of all boolean vector-functions $f : \{0, 1\}^m \to \{0, 1\}^n$. Any function $f \in P_{m,n}$ may be presented in the form $f = (f_1, \ldots, f_n)$, where $f_i \in P_{m,1}$ $(i = 1, \ldots, n)$. Thus $P_{m,n} = (P_{m,1})^n$. Let $T_0(m) = \{f \in P_{m,1} | f(0, \ldots, 0) = 0\}$ and $L(m)$ be the set of all linear functions $f \in P_{m,1}$.

A set $\chi_f = \{M_i | i = 1, \ldots, l\}$ of matrices over the field $GF(2)$ is called a *characteristic function* for the set $graph(f)$ $(f \in P_{m,n})$ if it satisfies the condition

$$(\forall \mathbf{a} \in \{0, 1\}^{m+n})(\exists M_i \in \chi_f)(\mathbf{a}M_i = \mathbf{0}) \Longleftrightarrow \mathbf{a} \in graph(f).$$

Thus $\mathbf{a} \in graph(f) \Longleftrightarrow \mathbf{0} \in \chi_f(\mathbf{a})$, where $\chi_f(\mathbf{a}) = \{\mathbf{a}M_i | i = 1, \ldots, l\}$.

The basic characteristics of the structure of the set $graph(f)$ $(f \in P_{m,n})$ are the following.

Theorem 10 [7]. The set $graph(f)$ $(f \in P_{m,n})$ is a subspace of the space $GF^{m+n}(2)$ if and only if $f \in (T_0(m) \cap L(m))^n$.

Since $V = \{\mathbf{0}, \mathbf{a}\}$ is a subspace of $GF^{m+n}(2)$ for any $\{\mathbf{a}\} \in \{0,1\}^{m+n} \backslash \{\mathbf{0}\}$, the notion of $lin\ graph(f)$ $(f \in P_{m,n})$ as the set of all maximal (relatively to the inclusion relation) subspaces of $GF^{m+n}(2)$ which are subsets of $graph(f)$ is justified.

Theorem 11 [7]. *lin graph*$(f) \neq \emptyset$ $(f \in P_{m,n})$ if and only if $f \in T_0^{(m)}(m)$.

The significance of Theorem 11 is justified by the fact that $g = f + f(0,\dots,0) \in T_0^{(m)}(m)$ for any $f \in P_{m,n}$.

Theorem 12 [7]. For any $f \in T_0^{(m)}(m)$ there holds the identity

$$graph(f) = \bigcup_{V \in lin\ graph(f)} V.$$

Theorem 12 suggests an effective method for the design of a characteristic function $\chi_f \in T_0^{(m)}(m)$. Indeed, let V be a subspace of $GF^{m+n}(2)$ and $\{\mathbf{e}_1, \dots, \mathbf{e}_{m+n-Dim(V)}\}$ be any basis of its orthogonal complement $V^{\perp}$. M_V denotes the $(m+n) \times (m+nDim(V))$-matrix whose columns are $\mathbf{e}_1, \dots, \mathbf{e}_{m+n-Dim(V)}$.

Theorem 13 [7]. For any $f \in T_0^{(m)}(m)$ the set $\chi_f = \{M_V | V \in lin\ graph(f)$ is a characteristic function for the set $graph(f)$.

Theorem 13 implies that the investigated problem may be solved via applying the following algorithm

Step 1. If $f \notin T_0^{(m)}(m)$, then $f := f + f(0,\dots,0)$, $\Omega := \Omega + f(0,\dots,0)$.

Step 2. Design the characteristic function $\chi_f = \{M_V | V \in lin\ graph(f)$.

Step 3. Compute $\chi_f(\mathbf{a})$ for all $\mathbf{a} \in \Omega$.

Step 4. If $\mathbf{0} \in \chi_f(\mathbf{a})$ for all $\mathbf{a} \in \Omega$, then $\Omega \subseteq graph(f)$, else $\Omega \not\subseteq graph(f)$.

The space and time complexities of the suggested algorithm are equal to

$$V = O((m+n)((m+n)|lin\ graph(f)| + |\Omega| - \sum_{V \in lin\ graph(f)} Dim(V)) \ \ (m,n \to \infty),$$

$$T = O(|\Omega|(m+n)((m+n)|lin\ graph(f)| - \sum_{V \in lin\ graph(f)} Dim(V)) \ \ (m,n \to \infty).$$

5. Conclusions

The presented results illustrate the significance of joining algebraic models and methods with searching for solutions of basic problems of the investigation of fundamental classes of discrete control systems, namely, finite automata and boolean functions. Further investigation of the properties of the suggested presentation of finite automata via detalization of the structure of finite groups gives the possibility to establish subtle relations between The Automata Theory and The Theory of Groups, one of the best examined branch of Modern Algebra. The suggested approach for the identification of boolean vector-functions may be naturally generalized for the case of arbitrary discrete functions. The subtle difference is that Theorem 12 does not hold in the general case.

Acknowledgement: The author is grateful to the staff of the Institute of Mathematics of the University of Miskolc for useful discussion of some of presented results and to the editors of the Journal for the possibility to present these results to a wide audience.

REFERENCES

[1] SKOBELEV, V.G.: *Presentation of automata by groups*, Ukrainian Mathematics Journal, **44**, No. 10 (1992), 1412-1416 (in Russian).

[2] SKOBELEV, V.G.: *Presentation of automata by groups. II*, Ukrainian Mathematics Journal, **52**, No.10 (2000), 1397-1404 (in Russian).

[3] SKOBELEV, V.G.: *Recursive model of a secret lock*, Reports of the National Academy of Sciences of the Ukraine, No. 6 (1995), 73-75 (in Russian).

[4] SKOBELEV, V.G.: *Estimation of exponential lower bounds*, Reports of the National Academy of Sciences of the Ukraine, No. 3 (1997), 115-117 (in Russian).

[5] PRACHAR, K.: Primzahlverteilung, Springer-Verlag, Berlin, 1957.

[6] SKOBELEV, V.G.: *On the lengths of distinguishing and synchronizing sequences for finite automata*, Kybernetika, No. 4 (1987), 114-116 (in Russian).

[7] SKOBELEV, V.G. and SPERANSKIJ, D.V.: *Identification of boolean functions via linear algebra methods*, Ukrainian Mathematics Journal, **47**, No.2 (1995), 260-268 (in Russian).