Representation of MarkovFunctions byMinimal Polynomials over a Finite Field

V.M. Zakharov[1], S.V. Shalagin[1], B.F. Eminov[1]

[1]KNRTU-KAI, 10 Karl-Marx str., 420111 Kazan, Russia

Abstract. The method of representing Markov functions with minimal characteristic polynomials over a finite field is proposed. These polynomials are defined on the basis of integrated stochastic matrices. The representation accuracy of stochastic matrices is linearly dependent on the minimum degree of the polynomials. The algorithmic implementation of the method is shown to build a sequence of the Markov functions class considered, with a given linear complexity.

Keywords: Markov functions, polynomials of minimal degree, accuracy of representations of stochastic matrices, linear complexity.

1. Introduction

Functions of finite Markov chains can be considered as processes obtained at the output of probabilistic automatons [1-3]. In [1], the obtained class of sequences is shown to be defined in the automaton-based modifications of random series as a class of the functions of finite Markov chains (Markov functions, MF). Probabilistic automaton classes obtained when limiting the function of the automaton outputs generate various classes of MFs [1-5]. The importance of modeling MFs is determined by a wide range of application possibilities for these processes [2-11]. In this paper, MFs of the class are considered, in which the general approach to building MFs consists in the following: A set of states of a given chain is divided into non-overlapping sub-sets, and the chain behavior is studied, provided that the states within the same sub-set do not differ.

A technique of modeling Markov chains (MC) and the functions thereof by polynomials over field $GF(2^n)$ is known [12,13]. Applying the technique [12,13] to representing MFs over Galois fields is validated by the high efficiency of finite fields arithmetic in digital data processing tasks. In a Galois field represented as $GF(2^n)$, it is possible to implement the stream processing of *n*-dimensional bit vectors, particularly using field-programmable gate arrays (FPGA) [13]. The problem in representing MFs over Galois fields is reducing the order of the $GF(2^n)$ field. In [9], a certain solution for this problem is proposed, based on reducing the length of an implying stochastic vector built upon the [3] decomposition of a stochastic matrix in a linear combination of stochastic Boolean matrices. The approach to representing sequences [14,15] has become a frequent practice, based on using Berlekamp-Massey algorithm (BMA) [16] for modeling (reproducing) random, pseudorandom, and Markov sequences by minimal polynomials [14] over finite field $GF(q)$, where q is a prime and

$q \geq 2$. However, the problem of representing Markov functions by minimal polynomials over finite field $GF(q)$ is as yet little understood.

The purpose of this paper is solving the problem of representing the Markov functions of the above class by minimal polynomials over field $GF(q)$, $q \geq 2$.

2. Problem Statement

Suppose a regular Markov chain is represented as system [5]

$$\left(P, S, \overline{\pi_0}\right), \tag{1}$$

where $P = \left(p_{ij}\right), i, j = \overline{0, m-1}$ is the regular stochastic matrix [5] dimensioned as $m \times m$; $S = \left\{s_0, s_1, ..., s_{m-1}\right\}$ is the finite set of the MC states; and $\overline{\pi_0}$ is the *m*-sized vector of the starting distribution of probability MC states.

An MC chain automaton model equivalent to system (1) is the autonomous probabilistic automaton (APA) represented as [2]

$$\left(S, \mu(s'/s), \overline{\pi_0}\right), \tag{2}$$

where the elements of *S*, $\overline{\pi_0}$ are the same as in (1), $\mu(s'/s)$ is the probabilistic automaton transition function defining the transition probability of automaton (2) into the new state of s' provided that the automaton is in the state of *s*; and $\mu(s'/s)$ is given by stochastic matrix (SM) $P = \left(p_{ij}\right)$.

Let us consider the autonomous probabilistic automaton (APA) with an output, represented as [1-3]

$$\left(S, P, Y, \lambda(s) = y, \overline{\pi_0}\right), \tag{3}$$

where the elements of *S*, $\overline{\pi_0}$, and *P* are the same as in (1); $Y = \left\{y_0, y_1, ..., y_{t-1}\right\}$ is the finite output alphabet; and $\lambda(s) = y$, $y \in Y$ is the output function implementing the single-valued transformation of the *S*-set of the chain states (1) into the *Y*-set:

$$\lambda(s): S \to Y = \left\{y_0, y_1, ..., y_{t-1}\right\}, \tag{4}$$

Let us define function $\lambda(s)$ by splitting the *S*-set into *t* sub-sets

$$\left\{A_0, A_1, ..., A_{t-1}\right\}, \bigcup_{j=0}^{t-1} A_j = S, A_j \cap A_k = 0 \text{ at } \forall j, \forall k = \overline{0, t-1}, \text{ and } j \neq k. \tag{5}$$

The A_j-sub-sets shall be called lumped states. Let $\left\{Y_t\right\}$ denote the process with *t* states $y_0, y_1, ..., y_{t-1}$, defined by the condition of $y_j = i$, $j = \overline{0, t-1}$, and $i = \overline{0, m-1}$, if, at some instant, the chain is being in the s_i-state of the A_j-sub-set. Process $\left\{Y_t\right\}$ formed at the output of automaton (3) falls in the class of the functions of finite Markov chains [1]. It should be noted: APA (3) falls in the class of Markov automatons [3].

Any function *u*: $Z \to GF(q)$ defined on the *Z*-set of nonnegative integers and taking its values within field $GF(q)$ [14] will be called the "sequence over field $GF(q)$, $q \geq 2$." Sequence $u = \left(u_i\right)$, $i \in Z$, will be called the linear recurrence sequence (LRS) of the *L* order over field $GF(q)$, if there exist constants $b_0, b_1, ..., b_{L-1} \in GF(q)$ such that $u(i+L) = \sum_{j=0}^{L-2} b_j u(i+j), i \geq 0$ [14]. Polynomial

$$f(x) = x^L - \sum_{j=0}^{L-1} b_j x^j \tag{6}$$

will be called the characteristic LRS polynomial [14].

Vector $\psi = (u(0), ..., u(L-1))$ is the initial LRS vector. Characteristic LRS polynomial *u* having the lowest order is its minimal polynomial [14].

Let u_N denote the LRS *u* of random length *N*, where the LRS length is the number of symbols within LRS. We say that polynomial $f(x)$ (6) yields sequence u_N, if u_N is a sub-sequence of some LRS that has this characteristic polynomial. The LRS is implemented by linear feedback shift register (LFSR), where the order of polynomial $f(x)$ defines the number of *q*-ary register bits and coefficients are a type of feedback [14]. We will consider the minimal polynomial represented as (6) and built over field $GF(q)$ using Berlekamp-Massey algorithm (BMA) [16] as a characteristic polynomial of the LRS that can be obtained based on LFSR.

We will consider solving the problem of representing Markov functions by minimal polynomials over field $GF(q)$ as the successive solutions of the following three stages (tasks).

Stage 1. Defining the law of the Markov function under consideration.

Stage 2. Defining the criteria of assessing the accuracy and length *N* of sequence u_N to represent the Markov function law with the required accuracy on u_N.

Stage 3. Building sequence u_N and constructing on u_N the minimal polynomial by BMA.

3. Defining the Law of the Markov Function under Consideration (Stage 1)

Let us define the law of the Markov function to be represented in model (3). For certain properties [5] of regular stochastic matrix *P*, process $\{Y_t\}$ may have the properties of an MC with the $t < m$ states and the described regular stochastic matrix sized $t \times t$, calculable for a given *P* [5, 17]. In the general case, in the MC function constructed by partitioning represented as (5), the temporal relationship of lumped states cannot be represented as a simple MC [5], i.e., process $\{Y_t\}$ may have no Markov property [5] where the "future" does not depend on the "past at a fixed "present." Representing process $\{Y_t\}$ on the basis of partition (5) as a Markov chain with lumped states allows calculating the characteristics of process $\{Y_t\}$ using Markov chain methods. In paper [5], the properties of a regular stochastic matrix are represented, the presence of which properties at a given partition of the set of states into disjoined classes is interpreted as the possibility to lump an SM, i.e., the possibility to lump the MC. In this case, the MC is called "lumpable." An MC constructed on a lumpable SM is called "lumped." The fulfillment of the condition of the possibility to lump stochastic matrix *P* can be checked using algorithm [17]. According to that [17], matrix *P* may be associated to a lumped regular stochastic matrix sized $t \times t, 2 \le t \le m-1$, that defines the lumped chain with a set of states $Y = \{y_0, y_1, ..., y_{t-1}\}$, where each of sub-sets A_j of set *S* is considered as the state of the lumped MC. Let us denote this lumped regular stochastic matrix by symbol $\hat{P}(p_{ij}), i, j = \overline{0, t-1}$.

Let us introduce a limitation: Suppose, in model (3), regular SM *P* sized $m \times m$ is lumpable at the given partition (5). Then, for this SM *P* and partition (5), let us construct using algorithm [17] the lumped stochastic matrix $\hat{P}(p_{ij}), i, j = \overline{0, t-1}$, sized $t \times t$, that defines the lumped MC with the set of states $Y = \{y_0, y_1, ..., y_{t-1}\}$. Let us assign to model (3) the model represented as

$$\left(Y, \hat{P}(p_{ij}), \overline{\pi_0}\right), \tag{7}$$

similar to model (2), where $\overline{\pi_0}$ is the *t*-sized vector of the initial distribution of MC states. Process $\{Y_t\}$ in model (7) has the Markov property and is described by the law defined by matrix $\hat{P}(p_{ij})$, $i, j = \overline{0, t-1}$.

Let us consider the equivalency of automata (3) and (7) in terms of the following statistic property of the sets generated by those models. Let us introduce the next matrix, *V*. Suppose matrix $V = (v_{ij})$,

$i=\overline{0,m-1}$, $j=\overline{0,t-1}$ is a Boolean matrix sized mґ t, the unity element v_{ij} of which matrix defines that state s_i of the initial chain is included into the lumped state A_j from (5): $v_{ij}=\begin{cases}1, s_i \in A_j \\ 0, s_i \notin A_j\end{cases}$. Let us denote:

$\pi_{np}=(\pi_0, \pi_1,..., \pi_{m-1})$ – is the limiting stochastic vector (SV) [5] of SM *P* in automaton (3);

$\pi_{np}^{(y)}=\left(\pi_0(y_0), \pi_1(y_1),..., \pi_{t-1}(y_{t-1})\right)$ is a SV defining the limit distribution of letters $y \in Y$ of process $\{Y_t\}$ at the output of automaton (3);

SV $\pi_{np}^{(y)}$ can be represented by the expression of $\pi_{np}^{(y)}=\pi_{np}\cdot V$; and

$\hat{\pi}_{np}=\left(\pi_0(y_0'), \pi_1(y_1'),..., \pi_{t-1}(y_{t-1}')\right)$ is the limiting SV of the lumped MC, calculated on SM $\hat{P}(p_{ij})$ and defining the limit distribution of states of the lumped MC in automaton (7).

Theorem 1 [18]. Suppose: 1) Lumpable SM *P* of the initial MC is given;

2) SM $\hat{P}(p_{ij})$ corresponding matrix *P* is given; and

3) States of SM *P* build partition (5). Then

$$\pi_{np}^{(y)}=\hat{\pi}_{np}. \quad (8)$$

Definition. Automata (3) and (7) are stochastically equivalent, if condition (8) is met for their output sequences, i.e., process $\{Y_t\}$ and the lumped chain.

The statistical properties of process $\{Y_t\}$ defined by lumped matrices are represented in [18, 19], in addition to (8).

4. Defining the Criteria of Assessing the Accuracy and Length N of Sequence u_N (Stage 2)

Using the given matrix $\hat{P}(p_{ij})$ and automaton (7), we can model (obtain) the implementations of a Markov chain. For large *Ns*, the p_{ij} elements of matrix $\hat{P}(p_{ij})$ can be assessed using the obtained frequencies of $p_{ij}^{'}=a_{ij}/a_i$ [5], where a_i is the number of s_i-state occurrences in the MC implementation of length *N*, a_{ij} is the number of occurrences of the pair of standing-by states $s_i s_j$, $i, j=\overline{0,t-1}$. However, with increasing *N*, the error in assessment decreases as $1/\sqrt{N}$. Length *N* of the sequence implementation at a given approximation accuracy is unpredictable.

In accordance with [20], let us consider matrix $\hat{P}(p_{ij})$ approximation problem. Solving [20] this problem ensures the convergence of order $1/N$ of relative frequencies $p_{ij}^{'}$ to values p_{ij} of the given matrix $\hat{P}(p_{ij})$ and allows representing matrix $\hat{P}(p_{ij})$ by elements $p_{ij}^{'}=a_{ij}/a_i$ with a given accuracy at a fixed length of *N*.

Approximation problem statement.

Let $\varphi=\left(y_{i1}, y_{i2},..., y_{iN}\right)$ denote the finite sequence of length *N* with the symbols from alphabet *Y*, having the following properties:

- For $\forall i=\overline{0,t-1}$, letter y_i enters $a_i^{(\varphi)} \geq 1$ times into sequence φ;
- Letter y_i ($j=\overline{0,t-1}$) follows y_i (assume y_{iN} is followed by y_{i1}) $a_{ij}^{(\varphi)} \geq 0$ times; and
- The following equalities are satisfied:

$$P_\varphi=(p_{ij}^{(\varphi)})=\left(a_{ij}^{(\varphi)}/a_i^{(\varphi)}\right),\ a_i^{(\varphi)}=\sum_{j=0}^{t-1}a_{ij}^{(\varphi)}=\sum_{j=0}^{t-1}a_{ji}^{(\varphi)}, \text{ and } \sum_{i=0}^{t-1}a_i^{(\varphi)}=N. \quad (9)$$

Assume: Sequence φ (φ-sequence) can be associated to regular stochastic matrix $P_\varphi = (p_{ij}^{(\varphi)})$, $i, j = \overline{0, t-1}$, sized $t \times t$, where the elements (relative frequencies) $p_{ij}^{(\varphi)} = a_{ij}^{(\varphi)} / a_i^{(\varphi)}$ satisfy formula (9) and the limiting vector of matrix P_φ is equal to

$$\overline{\pi}_\varphi = (\pi_i^{(\varphi)} = a_i / N),\ i = \overline{0, t-1}. \quad (10)$$

Given regular stochastic matrix $\hat{P}(p_{ij})$, $\overline{\pi}_{pr} = (\pi_0, \pi_1, ..., \pi_{t-1})$ – the limiting vector of matrix $\hat{P}(p_{ij})$, and number ε, $0 < \varepsilon < 1$. Suppose:

1) The error of approximating matrix $\hat{P}(p_{ij})$ by matrix $P_\varphi = (p_{ij}^{(\varphi)})$, $i, j = \overline{0, t-1}$, satisfies the following conditions:

$$\left| p_{ij}^{(\varphi)} - p_{ij} \right| \le \varepsilon,\ 0 < \varepsilon < 1; \quad (11)$$

$$p_{ij}^{(\varphi)} = \begin{cases} 0 : \text{if } p_{ij} = 0 \\ > 0 : \text{if } p_{ij} > 0 \end{cases}; \quad (12)$$

2) Value ε is related to the length of the $N\varphi$-sequence by linear relation [20]

$$N \ge N^*, \quad N^* = \max\{ \max_{\substack{i,j=0,t-1 \\ p_{ij}\pi_i \ne 0}} \{1/(p_{ij}\pi_i)\},\ \max_{i,j=0,t-1} \{(1 + p_{ij} + \varepsilon)/(\pi_i \varepsilon)\} \}. \quad (13)$$

Under assumptions (11)-(13) made, the achievable accuracy of approximating elements p_{ij} by frequencies $p_{ij}^{(\varphi)}$ depends linearly on N, where the accuracy of representing the number is the number of digits to represent elements p_{ij} of matrix $\hat{P}(p_{ij})$. In [20], we represent the algorithm of approximating matrix $\hat{P}(p_{ij})$ by matrix P_φ at a given value of ε and provided that conditions (9)-(13) are fulfilled. In order to construct minimal polynomial (6), let us define length N of sequence u_N from condition (13). Assume that the accuracy of representing matrix $\hat{P}(p_{ij})$ by matrix P_φ meets conditions (11) and (12).

5. Building Sequence u_N and Minimal Polynomial (Stage 3)

Let us introduce a theorem establishing the existence of a minimal characteristic polynomial representing a given regular stochastic matrix with a given accuracy, represented as (11) and (12).

Let us introduce value N' that meets the following condition:

$$|N' - N| \le t - 1. \quad (14)$$

Theorem 2 (principal theorem). Let stochastic matrix $\hat{P}(p_{ij})$ sized $t \times t$ and numbers $0 < \varepsilon < 1$, $N \ge N^*$ be given. Then there exists minimal polynomial $f(x)$ over field $GF(q)$, producing sequence $u_{N'+1}$ of length $N'+1$ with the law of $P_\varphi = (p_{ij}^{(\varphi)})$ meeting conditions (11)-(14),

$$|\pi_i^{(\varphi)} - \pi_i| \le \frac{1}{N} + \frac{\pi_i |N' - N|}{N}, \quad (15)$$

and order L of polynomial $f(x)$ meets the condition of

$$2L \le N' + 1. \quad (16)$$

Proof.

Lemma 1 [20]. For the given matrix $\hat{P}(p_{ij})$ sized $t \times t$, its limiting stochastic vector $\overline{\pi}_{pr} = (\pi_0, \pi_1, ..., \pi_{t-1})$, $\varepsilon > 0$, and integer $N \ge N^*$, there are stochastic matrix $P_\varphi = (p_{ij}^{(\varphi)})$ and its limiting stochastic vector $\overline{\pi}_\varphi = (\pi_0^{(\varphi)}, \pi_1^{(\varphi)}, ..., \pi_{t-1}^{(\varphi)})$, both meeting the following conditions:

a) $p_{ij}^{(\varphi)} = a_{ij} \Big/ \sum_{j=0}^{t-1} a_{ij}$, $i = \overline{0, t-1}$, where a_{ij} – nonnegative integers;

b) $\pi_i^{(\varphi)} = a_i / N'$, $\sum_{j=0}^{t-1} a_{ij} = \sum_{j=0}^{t-1} a_{ji} = a_i$ and $\sum_{i=0}^{t-1} a_i = N'$;

c) Conditions (11)-(15); and

d) Matrix P_φ can be calculated within $O\left(t^4\right)$ elementary arithmetic and logic (comparison) operations on real numbers.

Lemma 1 proves the existence of a solution for the problem of constructing matrix P_φ meeting conditions (11)-(15) of theorem 2, on arbitrarily given regular stochastic matrix $\hat{P}(p_{ij})$ and numbers $0 < \varepsilon < 1$, $N \geq N^*$.

Assume matrix $\hat{P}(p_{ij})$ and numbers ε, $N \geq N^*$ are given and matrix P_φ meeting conditions (11)-(15) is constructed using algorithm [20].

The next step on stage 3 is constructing the φ-sequence on the given stochastic matrix $P_\varphi = (p_{ij}^{(\varphi)})$. Solving this problem is represented in [21], where sequence φ is constructed using the Eulerian chains fitting algorithm [22] including the probabilistic procedure [21] of choosing by matrix P_φ an arc in each vertex.

Lemma 2 [16]. Suppose sequence u_N of length N of the elements of field $GF(q)$ is given. Then, on sequence u_N, BMA constructs the only minimal polynomial of order L, meeting the condition of

$$2L \leq N. \tag{17}$$

Let us code symbols $y_0, y_1, ..., y_{t-1}$ by the elements of field $GF(q)$, where $q \geq t$.

Let sequence $u_{N'+1}$ over field $GF(q)$ be sequence φ of length $N'+1$, where symbol $s_{iN'}$ is followed by symbol s_{i1}. Let us construct the minimal polynomial of order L from sequence $u_{N'+1}$, using BMA. Then the validity of relation (16) of theorem 2 follows from lemma 2. The theorem is proved.

6. Method of Modeling the Markov Function on the Basis of a Minimal Polynomial

We will consider the constructed polynomial over field $GF(q)$ as the characteristic polynomial of an LRS that can be obtained based on LFSR. From theorem 2 follows the method of modeling MF on the basis of minimal polynomial $f(x)$, consisting of the following stages.

Assume a Markov function is given by a Markov automaton represented as (3), where matrix P is lumpable.

1. Let us assign automaton (7), where matrix $\hat{P}(p_{ij})$ is sized $t' \times t$ to automaton (3) by lumping matrix P using algorithm [17].
2. On the given $\hat{P}(p_{ij})$, ε, and $N \geq N^*$, we use algorithm [20] to construct matrix P_φ meeting conditions (11)-(15), and then use the latter to calculate the value of N'.
3. Using probabilistic algorithm [21] of fitting Eulerian chains, we construct sequence φ of length $N'+1$ from the elements of field $GF(q)$, where $q \geq t$.
4. $u_{N'+1}$ is taken to be sequence φ of length $N'+1$. Let us code symbols $y_0, y_1, ..., y_{t-1}$ by the elements of field $GF(q)$, where $q \geq t$. On sequence $u_{N'+1}$, using the software implementation [23] of BMA [16], we construct minimal polynomial $f(x)$ of order L, L meeting condition (16) of theorem 2. We store initial vector $\mathbf{u} = \left(u(0), ..., u(L-1)\right)$ of sequence $u_{N'+1}$.
5. On polynomial $f(x)$ of order L obtained, we construct the software implementation of LFSR [23] of length L with q-ary bits, where L is defined by the expression of

$$L = \begin{cases} (N'+1)/2: \text{ if } N' \text{ is odd;} \\ ((N'+1)+1)/2: \text{ if } N' \text{ is even.} \end{cases} \quad (18)$$

Having defined vector $\vec{v}$ as the initial state of LFSR, we obtain at the *i*-th output, $i = \overline{1, L}$, of the *q*-ary bit of the LFSR program model sequence $u_{N'+1}$ with the length of $N'+1$ with the law of matrix form P_φ.

7. Conclusion

Markov function, i.e., process $\{Y_t\}$ defined within automaton model (3) by regular stochastic matrix *P* and by output function (4), can be described by a stochastic vector represented as $\pi_{np}^{(y)} = \pi_{np} \cdot V$. Process $\{Y_t\}$ defined within automaton model (3) on the basis of lumpable matrix *P* can be described by the relevant lumped matrix represented as $\hat{P}(p_{ij})$, $i, j = \overline{0, t-1}$ and model as a lumped Markovian chain on the equivalent, in terms of equation (8), automaton model (7). Approximation of matrices represented as $\hat{P}(p_{ij})$, with a specified accuracy and on the specified value of *N*, by matrices represented as P_φ allows constructing polynomials $f(x)$ of the minimal degree defined by expression (18) over field $GF(q)$. The $f(x)$ polynomial constructed represents (identifies) matrix P_φ uniquely. The accuracy of representing stochastic matrices by polynomials depends linearly on the minimal degree of the polynomials constructed using Berlekamp-Massey algorithm. The technique allows obtaining, with a specified accuracy, the quantitative value of the analytic structure complexity, i.e. the "linear complexity," of the Markov functions class under consideration, as well as solving the inverse problem, i.e., constructing sequences from the class of φ-sequences with a given "linear complexity" to be defined by the dimension of the matrix and by the accuracy of representing its elements.

8. Acknowledgment

This work was supported by RFBR Grant 18-01-00120a «Specialized devices for generating and processing data sets in the architecture of programmable logic devices class FPGA».

9. References

[1] Bukharayev, R.G. Automaton transformation of stochastic sequences / R.G. Bukharayev // Stochastic methods and cybernetics. – Kazan University. – 1966. – Vol. 4. – P. 24-33. (in Russian).
[2] Bukharayev, R.G. Basic of the theory of stochastic automatons / R.G. Bukharayev. – M.: "Nauka", 1985. – 287 p. (in Russian).
[3] Pospelov, D.A. Stochastic automatons / D.A. Pospelov. – M.: Energija, 1970. – 88 p. (in Russian).
[4] Romanovskiy, V.I. Discrete Markov chains / V.I. Romanovskiy. – M.: Gostekhizdat, 1949. – 436 p. (in Russian).
[5] Kemeny, J.G. Finite Markov chains / J.G. Kemeny, J.L. Snell // The University Series in Undergraduate Mathematics. Princeton: Van Nostrand, 1960. – 210 p.
[6] Stochastic automatons and its applications. – Kazan State University, 1986. – 214 p.
[7] Maksimov, Yu.I. Some results for the problem lumpability of Markov's chains states / Yu.I. Maksimov // Proceedings of discrete mathematics. – M.: Fizmatlit, 2004. – Vol. 8. – P. 148-154.
[8] Deundyak, V.M. Polynomial representation of the hidden half-Markov model of the Ferguson type / V.M. Deundyak, M.A. Zhdanova // Herald of VGU: System analysis and information technologies. – 2013. – Vol. 2. – P. 71-78.
[9] Zakharov, V.M. Representation of Markov's chains functions over finite field based on stochastic matrices lumpability property / V.M. Zakharov, B.F. Eminov, S.V. Shalagin //

International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), may 19-20, 2016. – P. 1-5. (in Russian).
[10] Pogorelov, B.A. On the features of Markov's approach in the study of block encryption algorithms / B.A. Pogorelov, M.A. Pudovkina // Applied discrete mathematics. Appendix. – 2014. –Vol. 7. – P. 51-52. (in Russian).
[11] Katehakis, M. A Successive Lumping Procedure for a Class of Markov Chains / M. Katehakis, L. Smit // Probability in the Engineering and Informational Sciences. – 2012. – Vol. 26(4). – P. 483-508.
[12] Zakharov, V.M. Polynomial representation of Markov chains over Galois field / V.M. Zakharov, Sh.R. Nurutdinov, S.V. Shalagin // Herald of KSTU named after A.N. Tupolev. – 2001. – Vol. 3. – P. 27-31. (in Russian).
[13] Zakharov, V.M. The method of simulating and transformation of Markov chain functions in Galois fields and its implementation in the FPGA-basis / V.M. Zakharov, Sh.R. Nurutdinov, S.V. Shalagin // Methods and means of information processing: 2 nd All-Russia scientific conf. – Moscow State University, 2005. – P. 256-262. (in Russian).
[14] Alferov, A.P. Basics of cryptography / A.P. Alferov, A.Yu. Zubov, A.S. Kuzmin, A.V. Cheremushkin. – M.: GeliosARV, 2002. – 480 p. (in Russian).
[15] Eminov, B.F. A method for modelling random sequences of a class of inhomogeneous Markov chains by polynomials of minimal degree over a field GF(q) / B.F. Eminov // Control systems and information technologies. Voronezh: Nauchnaya kniga, 2007. – Vol. 4.1(30). – P. 203-207.
[16] Massey J.L. Shift-register synthesis and BCH decoding / J.L. Massey // IEEE Trans. Inform. Theory. – 1969. – Vol. IT-15. – P. 122-127.
[17] Zakharov, V.M. The algorithm for the Markov chains lumpability / V.M. Zakharov, B.F. Eminov // Herald of KSTU named after A.N. Tupolev. – 2013. – Vol. 2(1). – P. 125-133. (in Russian).
[18] Eminov, B.F. The automaton models of Markov functions representation on the basis of lumpability of Markov chains / B.F. Eminov, V.M. Zakharov, M.A. Khusseyn // Information technologies and computing systems. – 2016. – Vol. 1. – P. 32-42. (in Russian).
[19] Eminov, B.F. About asymptotic properties of lumping and lumped Markov chains / B.F. Eminov, V.M. Zakharov // Herald of Technological University. – 2015. – Vol. 18(10). – P. 167-173. (in Russian).
[20] Zacharov, V.M. Complexity of the problem of approximation stochastic matrix by rational elements / V.M. Zacharov, S.E. Kuznetsov // Fundamental of Computation Theory. International conferences FCT-87. Kazan, USSR, June 22-26. Proceedings. Springer-Verlag. Berlin, Heidelberg, 1987. – P. 483-487. (in Russian).
[21] Eminov, B.F. Simulation of Markov sequences with inaccuracy less than the standard error / B.F. Eminov, V.M. Zakharov // Herald of KSTU named after A.N. Tupolev. – 2011. – Vol. 1. – P. 115-122. (in Russian).
[22] Kharari, F. Theory of graphs / F. Kharari. – M.: Mir, 1973. – 300 p. (in Russian).
[23] Khusainov, R.N. Development of a software implementation of the Berlekamp-Massey algorithm for the analysis and synthesis of binary recurrent sequences / R.N. Khusainov, B.F. Eminov, M.D. Galimov, A.I. Kryukov // Herald of Technological University. – 2015. – Vol. 18(24). – P. 89-91. (in Russian).