Representing Lumped Markov Chains by Minimal Polynomials over Field GF(q)

V M Zakharov, S V Shalagin, B F Eminov

KNRTU-KAI, 10 Karl-Marx Str., 420111 Kazan, Russia

Abstract. A method has been proposed to represent lumped Markov chains by minimal polynomials over a finite field. The accuracy of representing lumped stochastic matrices, the law of lumped Markov chains depends linearly on the minimum degree of polynomials over field GF(q). The method allows constructing the realizations of lumped Markov chains on linear shift registers with a pre-defined “linear complexity”.

1. Introduction

Lumped Markov chains (MC) are highly demanded in various applications among the lumped stochastic processes [1, 2]. Representing stochastic processes as lumped Markov chains allows researching a complex process using the Markov chains methods and solving various applied problems, such as those in information technology [3, 4], speech recognition using hidden Markov models [5], and block cipher cryptoanalysis [6]. The problem of lumping chains and its applications are actual at present time, as well. Many studies are devoted to this topic, including those published recently [7-9].

The method of simulating Markov chains by polynomials over field GF(2^n) is known [10]. Applying method [10] for representing Markov chains over field GF(2^n) is supported by the high efficiency of the arithmetic of finite fields in the problems of digital information processing. In representing Markov chains over Galois fields, the problem is to reduce the GF(2^n) field order. An approach to represent sequences [11] has become widespread, based on simulating (reproducing) by Berlekamp-Massey algorithm (BMA) [12], random and pseudorandom sequences by minimal polynomials [11] over finite field GF(q), where q is a prime number and q ≥ 2. However, the problem of representing Markovian sequences from the class of lumped Markov chains by minimal polynomials over finite field GF(q) is not adequately investigated.

The purpose of this paper is to solve the problem of representing lumped Markov chains by minimal polynomials over field GF(q), where q ≥ 2.

2. Problem Statement

Let us assume a regular finite MC [2] be prescribed by the system of:

\[(S, P, \pi_0),\]

where \(S = \{s_i\}\) is a finite set of MC states, \(|S| = n; P = (p_{ij}), i, j = 0, n - 1\) is a regular stochastic matrix (SM) sized \(n \times n\); \(p_{ij}\) are the MC transition probabilities, and \(\pi_0\) is the vector of the initial distribution of probabilities of MC states.
Let us divide initial set $S$ of MC (1) into $t$ disjoint subsets (into classes) formed as $A = \{A_0, A_1, \ldots, A_t\}$, where

$$\bigcup_{j=0}^{t-1} A_j = S, A_j \cap A_d = 0, \text{ where } \forall j, \forall d = 0, t-1 \text{ and } j \neq d.$$  

(2)

Let each of subsets $A_j, j = 0, t-1$, be a new state of the lumped MC (in terms of [2]) and the stochastic law of the lumped MC be defined by lumped stochastic matrix $\hat{P} = (\hat{p}_{ij})$ sized $t \times t$, $d, j = 0, t-1$.

Let us assume that:

$$p_{kA_j} = \sum_{i \in A_j} p_{ik}, i, k = 0, n-1, j = 0, t-1$$

is a probability of getting from state $s_k$ into set $A_j$ within one step of the initial MC (1). One should note that, in accordance with [2], the properties of a regular stochastic matrix, the availability of which for the given division of a set of states into disjoint classes is interpreted as a possibility to lump the stochastic matrix, i.e. the possibility of lumping the MC.

**Theorem 1** [2]. For lumping the MC states by dividing into classes $A = \{A_0, A_1, \ldots, A_t\}$, it is necessary and sufficient that for any two classes $A_j$ and $A_d$ and for $\forall s_k \in A_j, k = 0, n-1, d, j = 0, t-1$ probabilities $p_{kA_j}$ have the same value. Transition probabilities $\{\hat{p}_{ij}\} \text{ among the classes form stochastic matrix } \hat{P}$ of the lumped MC.

**Definition 1.** Let us name a Markov chain with regular stochastic matrix $P$, which satisfies theorem 1, lumpable.

**Definition 2.** Let us name a Markov chain with stochastic matrix $\hat{P}$, obtained by lumping Markov chain (1) by division (2), lumped.

Fulfilling the condition of lumping possibility for stochastic matrix $P$ can be particularly checked using algorithm [13].

Let us assume, in model (1), the regular MC $P$ sized $m \times m$ is lumpable for the given division (2). Then, on this MC stochastic matrix $P$ and division (2), let us construct the lumped stochastic matrix $\hat{P} = (\hat{p}_{ij})$, $i, j = 0, t-1$, sized $t \times t$ by algorithm [13], which describes the lumped MC with a set of states $Y = \{y_0, y_1, \ldots, y_m\}$. Let us associate system (1) with a system represented as

$$(Y, \hat{P}(p_{ij}), \pi_0),$$

(3)

where $\pi_0$ is a vector sized $t$ of the initial distribution of probabilities of states of the lumped MC.

Let us use the name of “a sequence over field $GF(q)$” for any function $u: Z \rightarrow GF(q)$ defined on the set $Z$ of non-negative integers and taking values within field $GF(q)$ [11]. Sequence $u = (u_i, i \in Z$, is called a linear recurrence sequence (LRS) of the $L$ order over field $GF(q)$, if there are such constants $b_0, b_1, \ldots, b_{L-1} \in GF(q)$ that $u(i + L) = \sum_{j=0}^{L-1} b_j \cdot u(i + j), i \geq 0$ [11]. Polynomial:

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

(4)

is called the characteristic polynomial of LRS [11].

Vector $\vec{u} = (u(0), \ldots, u(L-1))$ is the initial vector of LRS. Characteristic polynomial $u$ of LRS, which has the minimum degree, is its minimal polynomial [11].

Let us use $u_N$ to denote LRS $u$ of random length $N$, where the length of the LRS is the number of symbols in the LRS. Let us say that polynomial $f(x)$ (4) creates sequence $u_N$ if $u_N$ is a sub-sequence of a certain LRS with that characteristic polynomial. LRS is realized by a feedback linear shift register (LSR), where the degree of polynomial $f(x)$ defines the number of $q$-ary register bits and coefficients
are a form of feedback [11]. Let us consider the minimal polynomial represented as (4) and constructed over field GF(q) by Berlekamp-Massey algorithm [12] as a characteristic polynomial of the LRS that can be obtained based on LSR.

**Remark 1.** For large length $N$ of a Markov chain realization, elements $p_{ij}$ of matrix $\hat{P}(p_{ij})$ can be estimated by the obtained frequencies of $p'_{ij} = a_{ij} / a_i$ [2], where $a_i$ is the number of occurrences of state $s_i$ in the realization of the $N$-long MC; $a_{ij}$ is the number of occurrences of a pair of the standing-by states $s_i s_j$, and $i, j = 0, t - 1$. At the same time, however, the estimation error decreases with increasing $N$ as $N^{-1/2}$. Length $N$ of the sequence realization cannot be forecasted for a pre-determined accuracy of approximation.

Taking Remark 1 into account, let us consider solving the problem of representing a given lumped Markov chain (3) by minimal polynomials over field GF(q) as solving three successive tasks (stages).

Stage 1. Defining the criterion of assessing the accuracy and length $N$ of sequence $u_N$ to represent lumped stochastic matrix $\hat{P}(p_{ij})$, $i, j = 0, t - 1$, sized $\tau \times t$ by $u_N$, with the necessary accuracy that would describe the lumped MC with the set of states $Y = \{y_0, y_1, ..., y_{t-1}\}$.

Stage 2. Constructing sequence $u_N$.

Stage 3. Constructing a minimal polynomial by $u_N$ using the BMA.

3. **Defining the Criteria of Assessing the Accuracy and Length $N$ of Sequence $u_N$ (Stage 1)**

Let us use $\varphi = (y_0, y_1, ..., y_{tN})$ to denote a finite sequence of length $N$ with the symbols from alphabet $Y$, which sequence has the following properties:

- for $\forall i = 0, t - 1$ letter $y_i$ occurs $a_i(\varphi) \geq 1$ times in sequence $\varphi$;
- letter $y_j$ ($j = 0, t - 1$) follows $y_i$ $a_i(\varphi) \geq 0$ times (let us believe that $y_{iN}$ is followed by $y_{i1}$); and
- the following equations are satisfied:

$$P_\varphi = (p'_{ij(\varphi)}) = (a_{ij(\varphi)}/a_i(\varphi)), \ a_i(\varphi) = \sum_{j=0}^{t-1} a_{ij(\varphi)} = \sum_{j=0}^{t-1} a'_{ij(\varphi)} \text{ and } \sum_{i=0}^{t-1} a_i(\varphi) = N. \quad (5)$$

Sequence $\varphi$ ($\varphi$-sequence) can be associated with regular stochastic matrix $P_\varphi = (p_{ij(\varphi)})$, $i, j = 0, t - 1$, sized $\tau \times t$, where elements (relative frequencies) $p_{ij(\varphi)} = a_{ij(\varphi)}/a_i(\varphi)$ satisfy (4) and the finite vector of matrix $P_\varphi$ is equal to:

$$\pi_\varphi = (\pi_i(\varphi) = a_i/N), \ i = 0, t - 1. \quad (6)$$

Given there is regular stochastic matrix $\hat{P}(p_{ij})$, $\pi_{pr} = (\pi_0, \pi_1, ..., \pi_{t-1})$ – the finite vector of matrix $\hat{P}(p_{ij})$, and number $\varepsilon$, $0 < \varepsilon < 1$, let us assume that:

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

$$| p_{ij(\varphi)} - p_{ij} | \leq \varepsilon, \ 0 < \varepsilon < 1; \quad (7)$$

$$p_{ij(\varphi)} = \begin{cases} 0, & \text{if } p_{ij} = 0 \\ > 0, & \text{if } p_{ij} > 0. \end{cases} \quad (8)$$

2) quantity $\varepsilon$ is related to length $N$ of $\varphi$-sequence through a linear relation [14]:

$$N \geq N', \ N' = \max \left\{ \max_{i,j=0,t-1} \left\{ \max_{p_{ij} \neq 0} \frac{1}{\| P_{ij} \pi_j \|} \right\}, \max_{i,j=0,t-1} \left\{ (1 + p_{ij} + \varepsilon)/(\pi_i \varepsilon) \right\} \right\}. \quad (9)$$
Under assumptions (7) and (8), the reached accuracy of approximating elements $p_{ij}$ by frequencies $p_{ij}^{(\varphi)}$ depends linearly on $N$, where the accuracy of representing a quantity is the number of bits for representing elements $(p_{ij})$ of matrix $\hat{P}(p_{ij})$. In [14], there is the algorithm of approximating matrix $\hat{P}(p_{ij})$ by matrix $P_\varphi$ with the given value of $\varepsilon$ and with conditions (5)-(9) being satisfied. In order to construct the minimal polynomial (4), let us find the length $N$ of sequence $u_N$ from condition (9). Let us assume that the accuracy of representing matrix $\hat{P}(p_{ij})$ by matrix $P_\varphi$ satisfies (7) and (8).

4. Constructing Sequence $u_N$ and Minimal Polynomial (Stages 2 and 3)

Let us introduce a theorem stating the existence of the minimal characteristic polynomial representing a given regular stochastic matrix with a given accuracy as in (7)-(8).

Let us introduce quantity $N'$ that would satisfy:

$$|N' - N| \leq t - 1,$$  \hspace{1cm} (10)

**Theorem 2.** Let us assume there is stochastic matrix $\hat{P}(p_{ij})$ sized $t \times t$ and quantities $0 < \varepsilon < 1$ and $N \geq N'$. Then there is the minimal polynomial $f(x)$ over field $GF(q)$, which creates sequence $u_{N'+1}$ of length $N' + 1$ with the law of $P_\varphi = (p_{ij}^{(\varphi)})$, satisfying the conditions of (7)-(11),

$$|\pi_0^{(\varphi)} - \pi_i| \leq 1/N + \pi_i |N' - N|/N,$$  \hspace{1cm} (11)

and degree $L$ of polynomial $f(x)$ satisfies the following condition:

$$2L \leq N' + 1.$$  \hspace{1cm} (12)

**Proof.**

**Lemma 1** [14]. For given matrix $\hat{P}(p_{ij})$ sized $t \times t$, its finite stochastic vector $\pi_{pr} = (\pi_0, \pi_1, \ldots, \pi_{t-1})$, $\varepsilon > 0$, and integer $N \geq N'$, there is stochastic matrix $P_\varphi = (p_{ij}^{(\varphi)})$ and its stochastic vector $\pi_\varphi = (\pi_0^{(\varphi)}, \pi_1^{(\varphi)}, \ldots, \pi_{t-1}^{(\varphi)})$ which both would satisfy the following conditions:

a) $p_{ij}^{(\varphi)} = a_{ij} / \sum_{j=0}^{t-1} a_{ij}$, $i = 0, t - 1$, where $a_{ij}$ are no/n-negative 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 (7)-(12)

d) matrix $P_\varphi$ can be calculated within $O(t^4)$ elementary arithmetic and logical (comparison) operations on real numbers.

Lemma 1 states the existence of a solution for the problem of constructing matrix $P_\varphi$ satisfying conditions (10)-(12) of Theorem 2, for randomly defined regular stochastic matrix $\hat{P}(p_{ij})$ and quantities $0 < \varepsilon < 1$ and $N \geq N'$.

Let us define matrix $\hat{P}(p_{ij})$ and quantities $\varepsilon$ and $N \geq N'$, and use algorithm [14] to construct matrix $P_\varphi$ satisfying conditions (7)-(12).

The next step of Stage 3 is constructing a $\varphi$-sequence on given stochastic matrix $P_\varphi = (p_{ij}^{(\varphi)})$. Solving this problem is represented in [9], where sequence $\varphi$ is being constructed by the algorithm of distinguishing Eulerian chains [15], including the probabilistic procedure [9] of choosing by matrix $P_\varphi$ an arc in each vertex.

**Lemma 2** [12]. Let there be sequence $u_N$ of length $N$ of elements of field $GF(q)$. Then BMA constructs on sequence $u_N$ the only minimal polynomial with the degree of $L$ satisfying the condition of:

$$2L \leq N.$$  \hspace{1cm} (13)
Let us code symbols \(y_0, y_1, \ldots, y_{t-1}\) with the elements of field GF\((q)\), where \(q \geq t\).

Let sequence \(u_{N'+1}\) over field GF\((q)\) be sequence \(\varphi\) of length \(N'+1\), where symbol \(s_{N'}\) is followed by symbol \(s_{N'}\). Let us use BMA to construct on sequence \(u_{N'+1}\) the minimal polynomial of the degree of \(L\). Then it follows from Lemma 2 that the relation (12) of Theorem 2 is true. The theorem is proved.

5. Method of Simulating the Realizations of a Lumped Markov Chain Based on the Minimal Polynomial

Let us consider the minimal polynomial constructed over field GF\((q)\) as a characteristic polynomial of an LRS that may be obtained, based on an LSR. The method of simulating a lumped MC based on minimal polynomial \(f(x)\) follows from Theorem 2 and consists of the stages below.

1. For given \(\hat{P}(p_q), e, \) and \(N \geq N'\), let us use algorithm [14] to construct matrix \(P_\varphi\) satisfying conditions (7)-(12) and calculate the value of \(N'\) on it.

2. Using probabilistic algorithm [9] of finding Eulerian chains, let us construct sequence \(\varphi\) of length \(N'+1\) from the elements of field GF\((q)\), where \(q \geq t\).

3. Let us assume that \(u_{N'+1}\) is sequence \(\varphi\) of length \(N'+1\) and that in sequence \(u_{N'+1}\), the last symbol is followed by the first one.

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

Let us use the program realization [16] of BMA [12] to construct minimal polynomial \(f(x)\) of degree \(L\) on sequence \(u_{N'+1}\), where \(L\) satisfies condition (12) of Theorem 2. Let us keep in memory initial vector \(\vec{u} = (u(0), \ldots, u(L-1))\) of sequence \(u_{N'+1}\).

4. On the obtained polynomial \(f(x)\) of degree \(L\), let us construct a program realization of the LSR of length \(L\) with \(q\)-ary bits, where \(L\) is defined by expression:

\[
L = \begin{cases} 
\frac{(N'+1)}{2}, & \text{if } N' \text{ is odd} \\
\frac{((N'+1)+1)}{2}, & \text{if } N' \text{ is even} 
\end{cases}
\]  

Having pre-defined vector \(\vec{u}\) as the initial state of the LSR, let us obtain the sequence \(u_{N'+1}\) of length \(N'+1\) with the law of \(P_\varphi\) on the \(i\)-th output, \(i = 1, L\), of the \(q\)-th bit of the programmed simulation of the LSR.

6. Conclusion

Representing matrices \(\hat{P}(p_q)\) with a given accuracy or by a given value of \(N\) by the matrices of the \(P_\varphi\) allows constructing polynomials \(f(x)\) of the minimum degree determined by expression (14) over field GF\((q)\). Constructed polynomial \(f(x)\) represents (identifies) unambiguously matrix \(P_\varphi\). The accuracy of representing stochastic matrices by polynomials depends linearly on the minimum degree of polynomials constructed by the Berlekamp-Massey algorithm. The method allows constructing the realizations of lumped Markov chains on linear shift registers with a pre-defined “linear complexity” defined from formulas (9) and (10).

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

References

[1] Romanovskiy V I 1949 Discrete Markov chains (Moscow: Gostekhizdat) p 436
[2] Kemeny J G and Snell J L 1960 Finite Markov chains (Princeton: Van Nostrand) p 210
[3] Maksimov Yu I 2004 Some results for the problem lumpability of Markov chains states Proceedings of discrete mathematics 8 148-154
[4] Eminov B F, Zakharov V M and Khusseyen M A 2016 The automaton models of Markov functions representations on the basis of lumpability of Markov chains Information technologies and computing systems 1 32-42
[5] Zakharov V M, Eminov B F and Shalagin S V 2016 Representation of Markov chains functions over finite field based on stochastic matrices lumpability property 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) 1611-16

[6] Pogorelov B A and Pudovkina M A 2014 On the features of Markov approach in the study of block encryption algorithms Applied discrete mathematics 7 51-52

[7] Katehakis M and Smit L 2012 Successive Lumping Procedure for a Class of Markov Chains Probability in the Engineering and Informational Sciences 26(4) 483-508

[8] Geiger B and Temmel C 2014 Lumpings of Markov chains, entropy rate preservation, and higher-order lumpability Advances in Applied Probability 51(4) 1114-32

[9] Eminov B F and Zakharov V M 2015 About asymptotic properties of lumping and lumped Markov chains Herald of Technological University 18(10) 167-173

[10] Zakharov V M, Nurutdinov Sh R and Shalagin S V 2001 Polynomial representation of Markov chains over Galois field Herald of KSTU named after Tupolev 3 27-31

[11] Alferov A P, Zubov A Yu, Kuzmin A S and Cheremushkin A V 2002 Basics of cryptography (Moscow: GeliosARV) p 480

[12] Massey J L 1969 Shift-register synthesis and BCH decoding IEEE Trans. Inform. Theory IT-15 122-127

[13] Zakharov V M and Eminov B F 2013 The algorithm for the Markov chains lumpability Herald of KSTU named after Tupolev 2(1) 125-133

[14] Zakharov V M and Kuznetsov S E 1987 Complexity of the problem of approximation stochastic matrix by rational elements Fundamental of Computation Theory. International conferences FCT-87 483-487

[15] Kharari F 1973 Theory of graphs (Moscow: Mir) p 300

[16] Khusainov R N, Eminov B F, Galimov M D and Kryukov A I 2015 Development of a software implementation of the Berlekamp-Massey algorithm for the analysis and synthesis of binary recurrent sequences Herald of Technological University 18(24) 89-91