Representing stand-alone automata by characteristic polynomials over a finite field

V M Zakharov, S V Shalagin and B F Eminov
KNRTU-KAI, Kazan, Russia

E-mail: gilvv@mail.ru

Abstract. This paper proposes a method of representing a deterministic stand-alone output automaton by a minimal characteristic polynomial over a finite field. It is shown that defining various automaton transition and output functions allows using the algorithm developed to build the sets of minimal polynomials, different in their powers. Estimates of the relevant sets are given here. We have identified the relation between a characteristic minimal polynomial and an ergodic stochastic matrix defining the sequence developed by a stand-alone automaton. It is shown that the minimal degree of a characteristic polynomial depends linearly on the power of the automaton state set and on the accuracy of representing the elements of a given limiting vector of a stochastic matrix.

1. Introduction
Works [1, 2] present a method to define ergodic stochastic matrices (ESMs) [3] with rational elements by minimal characteristic polynomials [4] over finite field $\text{GF}(q)$, $q \geq 2$ [5] with a predefined accuracy. It is shown that this method allows building sequences of the predefined length, $N$, from the class of Markovian chains [3] with an accuracy of representing the non-zero elements of the specified chain law of the order of $1/N$ and simulating the sequences from this class with a predefined “linear complexity” [4]. The required accuracy of the method is achieved, based on using approximation algorithm [6] of the initial ESM by rational elements. A weak point of this method is the complexity of implementing the approximation algorithm [6]: Estimation of its complexity is determined by the value of $O(m^4)$, where $m$ is the degree of the stochastic matrix.

Work [7] shows that a stand-alone finite deterministic automaton with the state set power of $N$ and with the output function implementing the surjection, can generate an output sequence of the length of $N$, defined by the $m$-degree ergodic stochastic matrix with rational elements, the accuracy of representing the ESM elements linearly depending on $N$. Power of stochastic matrices represented by the automata of this type is related to the value of $N$ and to the automaton transition and output functions [7, 8].

This study aims is developing a method to represent a stand-alone deterministic automaton by a minimal characteristic polynomial over a finite field and is identifying the relations between such automata and the relevant minimal characteristic polynomials and ergodic stochastic matrices.

2. Defining the automaton model and the minimal characteristic polynomial
Let us consider the following deterministic stand-alone automaton [7]:
\[ DA = (X, S, Y, \delta, \lambda), \] (1)
where $X$ is the input alphabet consisting of one letter; $S = \{s_0, s_1, \ldots, s_{N-1}\}$ is the finite set of states; $Y = \{y_0, y_1, \ldots, y_{m-1}\}$ is the output alphabet; $\delta: S \to S$ is the transition function; and $\lambda: S \to Y$ is the output function definitely mapping $S$ onto $Y$. Automaton transition path forms a loop of length $N$, covering all states. We will define output function $\lambda(S)$ by dividing set $S$ into $m$ disjoint subsets $\{A_0, A_1, \ldots, A_{m-1}\}$, $m=2, 3, \ldots, N-1$. Powers of those subsets are $a_i \geq 1$ and $\sum_{i=0}^{m-1} a_i = N$, respectively. Let us denote the subsets, respectively by the symbols of set $Y = \{y_0, y_1, \ldots, y_{m-1}\}$. At the output of automaton (1), over the time of executing the $N$-long loop, the $N$-long sequence (denoted as $\beta(N)$) of output letters is formed. We should note that sequence $\beta(N)$ can be uniquely associated with the rational matrix (relative frequency matrix) $P' = (p_{ij}) = (a_j / a_i)$ sized $m \times m$, where $a_i$ is the number of occurrences of letter $y_i$ in the $N$-long sequence, $a_i \geq 1$, and $a_{ij}$ is the number of a pair of neighboring letters $y_i y_j$, $i, j = 0, m-1$ (we consider that $y_N$ follows $y_0$). Matrix $P' = (p_{ij}) = (a_j / a_i)$ is an ergodic stochastic matrix having the following properties [7]:

1) Elements $p_{ij} = (a_j / \sum_{j=0}^{m-1} a_j)$,

$$\sum_{j=0}^{m-1} a_j = \sum_{j=0}^{m-1} a_{ji} = a_i \geq 1 \text{ and } \sum_{i=0}^{m-1} a_i = N, i, j = 0, m-1; \quad (2)$$

2) Limiting stochastic vector of matrix $\Pi_{np}$ is

$$\Pi_{np} = \left( \frac{a_0}{N}, \frac{a_1}{N}, \ldots, \frac{a_{m-1}}{N} \right). \quad (3)$$

Note that stochastic matrix represented as $P' = (p_{ij}) = (a_j / a_i)$ with properties (2) and (3) can be computed using algorithm [6] directly by the pre-defined ergodic stochastic matrix, with a specified accuracy, determined value $1/N$. Computational complexity of the algorithm is determined by estimate $O(m^3)$ [6].

Let us introduce the following definitions. We will use the term of “a sequence over field GF($q$)” for any function $u: Z \to GF(q)$ defined on set $Z$ of nonnegative integers and taking its values in field GF($q$) [4]. Sequence $u = (u_i), i \in Z$, is called a linear recurrence sequence (LRS) of order $L \geq 0$ over field GF($q$), if there are constants $b_0, b_1, \ldots, b_{L-1} \in GF(q)$, so that $u(i+L) = \sum_{j=0}^{L-1} b_j \cdot u(i+j), i \geq 0$ [4]. Polynomial

$$f(x) = x^L - \sum_{j=0}^{L-1} b_j \cdot x^j \quad (4)$$

called a characteristic polynomial of LRS $u$. Vector $\vec{u} = (u(0), \ldots, u(L-1))$ is the initial vector of LRS. Characteristic polynomial (4) of LRS $u$, having the minimal degree, is its minimal polynomial [4]. Let us use $u_N$ to denote LRS $u$ of arbitrary length of $N$, where the length of LRS is the number of symbols in the LRS. An efficient algorithm for building the minimal characteristic polynomial (4) on the predefined $u_N$ of LRS is the Berlekamp-Massey algorithm (BMA) [9]. Let us note the following property of the Berlekamp-Massey algorithm.
Theorem [9]. Let sequence $u_N$ of the length of $N$ is defined, consisting of the elements of field $\text{GF}(q)$. Then, on sequence $u_N$, the Berlekamp-Massey algorithm builds the single minimal polynomial with degree $L$ satisfying the condition of

$$2L \leq N.$$  \hfill (5)

3. Method to represent a stand-alone automaton by a minimal polynomial

This method can be represented by the following two algorithmic stages.

Stage 1. Building sequence $\beta(N)$ by the operation algorithm of a given automaton (1). Stochastic matrix that is uniquely determined by the built sequence $\beta(N)$ has the properties of (2) and (3).

Values are set for $N, S, m, Y$, $\delta : S \rightarrow S$, $\lambda : S \rightarrow Y$. Transition function $\delta : S \rightarrow S$ of automaton (1) is implemented by a certain generator of repetitive pseudorandom sequences (PRS) with a period equaling to $N$, such as in [10,11]. Output function defined by partition $\{ A_0, A_1, \ldots, A_{m-1} \}$, where the set of numbers $(a_0, a_1, \ldots, a_{m-1})$ satisfies the following constraint:

$$a_i \geq 1, \sum_{i=0}^{m-1} a_i = N \tag{6}$$

is implemented by algorithm [8] as a converter executing a predefined single-valued transformation $\lambda : S \rightarrow Y$ and forming sequence $\beta(N)$ at the output of automaton (1) over the time of executing by the transition function a loop of the length of $N$.

Stage 2. Building on sequence $\beta(N)$ the minimal characteristic polynomial (4) by the Berlekamp-Massey algorithm.

We will consider sequence $\beta(N)$ built on Stage 1 as sequence $u_N$. Let us encode the symbols of alphabet $Y$ with the elements of field $\text{GF}(q)$, where $q > m$. On sequence $\beta(N)$ of a length of $N + 1$ (it is considered that symbol $y_i$ is followed by symbol $y_{i+1}$), we will use BMA to build the minimal characteristic polynomial $f(x)$ of degree $L$, where $L$ is determined in accordance with the following statement:

Consequence 1 (of the theorem). Berlekamp-Massey algorithm builds on sequence $\beta(N)$ the single minimal characteristic polynomial (4) with degree $L$ satisfying the following expression:

$$L \leq \left\{ \begin{array}{ll} (N + 1)/2, & \text{if } N \text{ is even;} \\ ((N + 1) + 1)/2, & \text{if } N \text{ is odd.} \end{array} \right. \tag{7}$$

From Consequence 1, it follows that the minimal characteristic polynomial of degree (7) built at Stage 2 determines uniquely the stochastic matrix relevant to sequence $\beta(N)$ built at Stage 1.

4. Method implementation illustration sample

Stage 1. Building sequence $\beta(N)$ by automaton (1).

In automaton (1) $S = S_1 = \{s_1, s_2, \ldots, s_{21}\}$, $N = N_1 = 21$, $m = 4$, set $Y = \{y_0, y_1, y_2, y_3\}$, for the output function, let us define a set of numbers $(a_0=6, a_1=5, a_2=5, a_3=5)$, the relevant vector appearing as $\hat{P}_1 = (6/21; 5/21; 5/21; 5/21)$. Let the transition function be implemented by binary linear shift register [4] defined by polynomial $F(x) = (x^3 + x + 1)(x^2 + x + 1) = x^5 + x^4 + 1$ generating a PRS of the automaton states (denoted as $M_i$) with the period of $N_1 = 21$ [12]. We implement the output function in accordance with [8] as a transformer of the $N$-place input PRS of the length of $N$ in the $m$-place PRS of the length of $N$ with a predefined distribution appearing as (3). Then, in automaton (1), $M_i$-sequence can be transformed into sequence $\beta_1(N) = y_1 y_2 y_3 y_0 y_2 y_1 y_3 y_0 y_2 y_1 y_3 y_0 y_2 y_1 y_3 y_0 y_0 y_2$ of the length of $N_1 = 21$ over the time of executing the loop by the transition function.

Sequence $\beta_1(N)$ corresponds uniquely with ESM $P_i$. 

---

**Journal of Physics: Conference Series**

2nd ISPCMMPAM 2020

IOP Publishing

1658 (2020) 012077
doi:10.1088/1742-6596/1658/1/012077
having the properties of (2) and (3) and the predefined limiting vector equaling to \( \overline{P_1} \).

In the context of the example, having defined in automaton (1) another transition function (by another PRS generator), we can obtain at the automaton (1) output another sequence appearing as \( \beta(N) \). For example, let the transition function be implemented by a binary linear shift register defined by polynomial \( F_2(x) = (x^5 + x^2 + 1)(x^2 + x + 1) = x^7 + x + 1 \) generating a PRS (denoted as \( M_2 \)) with the period of \( N_1 = 21 \). Then, in automaton (1), \( M_2 \)-sequence can be transformed by algorithm [8] into sequence \( \beta_2(N) = \ldots, y_2, y_1, y_2, y_3, y_0, y_2, y_3, y_0, y_2, y_3, y_0, y_2, y_3, y_0, y_2, y_1 \).

Sequence \( \beta_2(N) \) corresponds uniquely with ESM \( \mathcal{ECM} P_2 \):

\[
P_2 = \begin{bmatrix}
2/6 & 0 & 4/6 & 0 \\
0 & 1/5 & 0 & 4/5 \\
0 & 4/5 & 0 & 1/5 \\
4/5 & 0 & 1/5 & 0
\end{bmatrix},
\]

having the properties of (2) and (3) and the predefined limiting vector equaling to \( \overline{P_1} \).

Note: Different sequences \( \beta(N) \) obtained on automata appearing as (1) at the same \( N, m \), and output functions, but at different predefined transition functions, can be defined by the same ESM appearing as \( P' \) [7].

Stage 2. Constructing the minimal characteristic polynomial over field \( GF(q) \) by sequence \( \beta_1(N) \).

To encode the letters of sequence \( \beta_1(N) \), we will use field \( GF(q) \), where \( q \) is a prime number equaling to 7.

Below is the minimal characteristic polynomial \( f_1(x) \) computed using BMA [13] on sequence \( \beta_1(N) \) (considering that the last symbol \( y_{N} \) is followed by symbol \( y_1 \)):

\[
f_1(x) = x^{31} - 4x^{10} - 2x^9 - 5x^8 - 5x^6 - 3x^5 - 3x^4 - x^3 - 6x^2 - 3x = L = 11.
\]

Minimal characteristic polynomial computed in a similar manner by sequence \( \beta_2(N) \) appears as

\[
f_2(x) = x^{11} - 3x^{10} - x^8 - 2x^7 - 6x^6 - 6x^5 - 5x^4 - 4x^3 - 2x - 1 = L = 11.
\]

From Consequence 1, it follows that polynomials \( f_1(x) \) and \( f_2(x) \) uniquely represent the respective stochastic matrices, \( P_1 \) and \( P_2 \).

5. Estimating the power of a set of minimal polynomials represented by the predefined automata appearing as (1)

At Stage 1, various sets of sequences \( \beta(N) \) can be obtained on automata (1), based on the following approaches: 1) By implementing different transition functions at a fixed output function, 2) based on specifying different sets of \( (a_0, a_1, \ldots, a_{m-1}) \), \( m=2, \ldots, N-1 \) at a fixed transition function, and 3) based on simultaneously changing the transition and the output functions.

Let us consider the matter of estimating the power of a set of minimal polynomials represented by the predefined automata appearing as (1).

In its structure, sequence \( \beta(N) \) obtained at the output of automaton (1) is a permutation of the elements of set \( Y \) with repetition [14].

Note 1. At the fixed set of numbers \( (a_0, a_1, \ldots, a_{m-1}) \) with property (6) the number of possible permutations of the repeated set \( Y \) is determined by expression [14]

\[
C_N(a_0, a_1, \ldots, a_{m-1}) = h_1 = N/\!\!/a_0^1a_1^1\ldots a_{m-1}^1.
\]  \hspace{1cm} (8)

From consequence 1 and Notes 1, it follows that the statement below is valid.
Statement 1. Let $N$, $m$ and the set of numbers $a_0, a_1, ..., a_{m-1}$ from (6) be defined for automaton (1). Then the upper estimate of the number of minimal polynomials represented as (4) and representing sequences $\beta(N)$ formed by automaton (1) by predefined transition functions is determined by (8).

Note 2 [7]. Number of stochastic matrices $P'$ having the same predefined limiting vector represented as (3) does not exceed the value of (8).

Consequence 2 (of the statement 1). Power of a set of minimal polynomials, appearing as (4), built on sequences $\beta(N)$, and representing the respective stochastic matrices $P' = (p'_{ij}) = (a_j / a_i)$ having the same predefined limiting vector appearing as (3), is defined by estimate $O(h_1)$.

And the fixed values of $N$ and $m$, the number of different sets $(a_0, a_1, ..., a_{m-1})$ having the property of (6) to define a vector appearing as (3), can be defined by estimate [8]

$$h_2 = C_{m-N^{-1}}^{N-1}.$$ (9)

We will consider the value of (9) as the estimation of the power of a set of minimal characteristic polynomials appearing as (4) and obtained on the sequences at changing the sets of numbers $(a_0, a_1, ..., a_{m-1})$, at the fixed $N$, $m$, and transition function in automaton (1).

From Consequence 1 and ratios (8) and (9), there follows the validity of

Statement 2. Power of a set of minimal characteristic polynomials appearing as (4) and representing sequences $\beta(N)$ obtained on automata appearing as (1) at the fixed values of $N$ and $m$, based on changing the sets of numbers $(a_0, a_1, ..., a_{m-1})$ and the transition functions implementing different loops of the length of $N$, is estimated by the value of

$$O(h_1, h_2).$$ (10)

6. Conclusion

Our method proposed for representing a deterministic stand-alone automaton (1) by a minimal characteristic polynomial over field $GF(q)$ is based on building by an automaton output sequence having the properties of (2) and (3), polynomial (4) of a minimal degree, using the Berlekamp-Massey algorithm. The minimal degree of the polynomial is determined by the value of (7). Estimates (8)–(10) allow us to define the set powers of the minimal characteristic polynomials to be represented, based on the predefined powers of the set of states and the set of the output alphabet of an automaton. Minimal polynomial represented for automaton (1) determines uniquely the stochastic matrix – automaton output sequence law.

References

[1] Zakharov V M, Shalagin S V and Eminov B F 2018 Representing Lumped Markov Chains by Minimal Polynomials over Field GF(q) Journal of Physics: Conference Series Vol. 1015 032038 DOI: 10.1088/1742-6596/1015/3/032033

[2] Eminov B F and Zakharov V M 2019 Simulating Extended Markov Chains with a Given Linear Complexity Management Systems and Information Technologies 4 (78) 28–32

[3] Kemeny J G and Snell J L 1960 Finite Markov chains (Princeton: Van Nostrand) p 210

[4] Alferov A P, Zubov A Yu, Kuzmin A S and Cheremushkin A V 2002 Basics of Cryptography (Moscow: Gelios ARV) p 480 [In Russian]

[5] Lidl R and Niederreiter H 2008 Finite Fields (Encyclopedia of Mathematics and its Applications) (Cambridge: Cambridge Univ. Press) 2 p 772

[6] Zacharov V M and Kuznetsov S E Complexity of the problem of approximation of stochastic matrix by rational elements Fundamental of International conferences FCT-87 Proceedings Springer-Verlag (Berlin: Heidelberg) 483–487

[7] Stolov E L 1980 On One Class of Pseudo-Markovian Chain Generators Research in Applied Mathematics 8 (Kazan: Kazan University Publishing House) 66–71 [In Russian]

[8] Zakharov V M, Shalagin S V and Eminov B F 2019 Algorithms for computing the sets of stochastic matrices with predefined properties, based on automaton models MMPAM-2019.
[9] Massey J L 1969 Shift-register synthesis and BCH decoding IEEE Trans. Inform. Theory Vol. IT-15 122–127

[10] Ivanov M A and Chugunkov I V 2003 Theory, Application, and Quality Estimation of Pseudorandom Sequence Generators (Moscow: KUDITs-OBRAZ) p 240 [In Russian]

[11] Pesoshin V A, Kuznetsov V M and Shirshova D V 2016 Generators of the equiprobable pseudorandom nonmaximal-length sequences based on linear-feedback shift registers Automation and Remote control Vol. 77 1622–1631

[12] Nechaev V I 1999 Elements of Cryptography. Basics of Information Theory (Moscow: Vysshaya shkola) p 109 [In Russian]

[13] 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

[14] Bronstein I N and Semendyaev K A 1986 Mathematics Reference for Engineers and Technical College Students (Moscow: Nauka. Chief Editorial Board for Physical and Mathematical Literature) p 544 [In Russian]