Моделирование расширенных цепей Маркова минимальными полиномами над полем GF(q)

Б.Ф. Эминов[1], В.М. Захаров[1], С.В. Шалагин[1]

[1]Казанский национальный исследовательский технический университет им. А.Н. Туполева, К. Маркса 10, Казань, Россия, 420111

Аннотация. Предложен метод представления и моделирования минимальными полиномами расширенных и определенного вида сложных цепей Маркова над конечным полем GF(q). Задача моделирования решается как задача построения по алгоритму Берлекэмпа-Мэсси минимального полинома над полем GF(q). Полином вырабатывает последовательность длины N. Соответствующая этой последовательности стохастическая матрица аппроксимирует заданную стохастическую матрицу расширенной цепи Маркова с заданной точностью, пропорциональной величине $1/N$. Построенный полином однозначно определяет структуру q-ичного линейного регистра сдвига для моделирования расширенных цепей Маркова.

1. Введение

В работе рассматривается задача моделирования случайных дискретных процессов из класса расширенных цепей Маркова (РЦМ) [1], получаемых на основе простых цепей Маркова (ЦМ) [2]. Расширение ЦМ позволяет получить большую информацию об исследуемом процессе. Случайные последовательности класса РЦМ характеризуются цепной связью вида "гусениц" (по терминологии Постникова А.Г. [3]). У РЦМ – текущее состояние определяет поведение системы в будущем через r шагов и может быть использовано для предсказания поведения системы.

Частным случаем РЦМ являются цепи Маркова-Брунса [2], определенные Марковым А.А. в [4] как "ненастоящие" цепи. В [2] определен закон (стохастическая матрица) цепи Маркова-Брунса. В [1] задача определения стохастической матрицы РЦМ решена для частного случая. В [5, 6] представлены алгоритмы построения стохастической матрицы РЦМ размера $m^r \times m^r$, $m \geq 2$, $r \geq 2$. В [5] показано, что стохастическую матрицу РЦМ при некоторых ограничениях на задание РЦМ можно рассматривать как закон определенной r–сложной ЦМ [2], $r \geq 2$. В [6, 7] представлен метод моделирования РЦМ на полиномиальных моделях, описываемых полиномиальными функциями над полем GF(2^n). Задача построения полиномиальных моделей в данном подходе решается как задача вычисления коэффициентов полиномов над полем GF(2^n) на основе заданных стохастических матриц. Проблемной задачей в области представления ЦМ над полем GF(2^n) является снижение порядка поля.

В [6, 8] предложен подход моделирования по алгоритму Берлекэмпа-Мэсси (АБМ) [9] минимальными полиномами [10] над конечным полем GF(q), $q \geq 2$, определенного класса [6] неоднородных цепей Маркова, задаваемых эргодическими стохастическими матрицами [1] и укрупненных цепей Маркова [8], задаваемых регулярными стохастическими матрицами. В этом подходе основная проблемная задача связана с заданием точности представления стохастических матриц минимальными полиномами.

Целью работы является решение задач представления с заданной точностью и моделирования минимальными полиномами над полем GF(q), где $q \geq 2$, расширенных цепей Маркова.

2. Постановка задачи

2.1. Определение закона и алгоритма построения РЦМ

Пусть задана последовательность состояний $s_{j\,1}, s_{j\,2}, \ldots$ простой однородной ЦМ с конечным множеством состояний $S = \{s_j\}$ эргодической стохастической матрицей $P = (p_{ij})$ [1] размера $m \times m$, $i, j = \overline{0, m-1}$.

Образуем из этой исходной цепи по аналогии с [1] новую, расширенную цепь Маркова следующим образом [5]. Составим всевозможные цепочки символов $s_j \in S$ длины $r = \nu + \kappa$, $r \geq 2$, $\nu \geq 1$, $\kappa \geq 1$, $j = \overline{0, m-1}$, имеющие вид ($s_{j\,1}, s_{j\,2}, \ldots, s_{j\,\nu}, s_{j\,\nu+1}, \ldots, s_{j\,\nu+\kappa}$). Смежные цепочки содержат $\kappa = r - \nu$ общих символов и ν ("величина сдвига") отличающихся символов.

Предположим, что исходная цепь за $2\nu + \kappa - 1$ шагов последовательно переходит из некоторого состояния $s_{j\,1}$ в $s_{j\,2}$, затем из $s_{j\,2}$ в $s_{j\,3}$, …, из $s_{j\,(2\nu+\kappa-1)}$ в $s_{j\,(2\nu+\kappa)}$. Смежные цепочки длины r будем рассматривать как один шаг перехода нового процесса из состояния ($\boldsymbol{s_{j\,1}, \ldots, s_{j\,\nu}, s_{j\,\nu+1}, \ldots, s_{j\,\nu+\kappa}}$) в состояние ($\boldsymbol{s_{j\,\nu+1}, \ldots, s_{j\,2\nu}, s_{j\,2\nu+1}, \ldots, s_{j\,2\nu+\kappa}}$). Этот новый расширенный процесс (расширенная цепь Маркова) является ЦМ с $m^{\nu+\kappa}$ состояниями (цепочки символов s_j длины r, $j = \overline{0, m-1}$). Обозначим состояния РЦМ символами y_i, из алфавита $Y = \{y_i\}$, $i = \overline{0, m^{\nu+\kappa} - 1}$.

Обозначим через Q стохастическую матрицу размера $m^{\nu+\kappa} \times m^{\nu+\kappa} = t \times t$ этой РЦМ. Определим матрицу Q РЦМ через матрицу P исходной ЦМ при $\nu \geq 2$, $\kappa \geq 2$ в соответствии с [5]. Для частного случая, $\nu = \kappa = 1$, эта задача решена в [1].

Получение матрицы Q РЦМ осуществим на основе понятия "промежуточной" стохастической матрицы [5] размера $m^{\nu+\kappa} \times m^{\nu+\kappa} = t \times t$, вычисляемую на основе матрицы P исходной ЦМ. Промежуточную матрицу обозначим как $W = (w_{ij})$, $i, j = \overline{0, m^r - 1}$.

Ненулевые элементы матрицы W вычисляются по формуле [5, 6]:

$$w_{i,(i \cdot m \bmod m^r + d)} = p_{(i \bmod m),d}\,,\ i = \overline{0, m^r - 1},\ d = \overline{0, m-1}, \tag{1}$$

где i - текущий номер строки матрицы W, d - текущий номер столбца матрицы P.

Матрица Q РЦМ связана с матрицей W соотношением [5, 6]

$$Q = W^{\nu}, \tag{2}$$

где $(\mathrm{W})^{\nu}$ – ν-я степень матрицы W, $\nu \geq 1$, $\kappa \geq 1$.

Введем определение РЦМ на основе матрицы Q.

Определение. Цепь Маркова со стохастической матрицей Q вида (2) размера $m^{\nu+\kappa} \times m^{\nu+\kappa}$, $\nu \geq 1$, $\kappa \geq 1$, полученной по эргодической стохастической матрице $P = (p_{ij})$ размера $m \times m$, $i, j = \overline{0, m-1}$, будем называть расширенной цепью Маркова общего вида.

Отметим следующие свойства РЦМ, представляемой матрицей (2).

Теорема 1 [5]. Пусть дана матрица $P = (p_{ij})$, $\forall p_{ij} > 0$, $i, j = \overline{0, m-1}$, и на ее основе получена матрица Q РЦМ размера $m^r \times m^r$, $r = \nu + \kappa \geq 2$, $\nu \geq 1$, $\kappa \geq 1$. Тогда данная РЦМ - эргодическая.

Эргодичность РЦМ для случая $r = \nu + \kappa = 2$, $\nu = 1$, $\kappa = 1$ показана в [1].

Предельный стохастический вектор матрицы Q РЦМ определяется по аналогии с [1, стр. 183] соотношением

$$\bar{\pi}_{pr} = \bar{\pi}_{pr}^{(w)} W\,,$$

где $\bar{\pi}_{pr}^{(w)}$ - предельный вектор матрицы W.

Утверждение. Пусть дана матрица $P = (p_{ij})$, $\forall p_{ij} > 0$, $i, j = \overline{0, m-1}$, и на ее основе получена матрица Q РЦМ размера $m^r \times m^r$, $r = \nu + \kappa \geq 2$, $\nu = 1$, $\kappa \geq 1$. Тогда данная матрица Q задает стохастическую матрицу r−сложной ЦМ с переходными вероятностями, определяемыми элементами матрицы P. Справедливость утверждения следует из алгоритма [5] построения матрицы Q.

Пример. По ЦМ, заданной матрицей $P = \begin{vmatrix} 3/8 & 5/8 \\ 6/8 & 2/8 \end{vmatrix}$, можно построить на основе соотношения (2) следующие РЦМ, заданные стохастическими матрицами Q_1 и Q_2 (рисунок, а и б), с длиной цепочек $r = 3$ и различными величинами ν и κ.

$$Q_1 = \begin{vmatrix} \frac{3}{8} & \frac{5}{8} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{6}{8} & \frac{2}{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{3}{8} & \frac{5}{8} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{6}{8} & \frac{2}{8} \\ \frac{3}{8} & \frac{5}{8} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{6}{8} & \frac{2}{8} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{3}{8} & \frac{5}{8} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{6}{8} & \frac{2}{8} \end{vmatrix} \qquad Q_2 = \begin{vmatrix} \frac{9}{64} & \frac{15}{64} & \frac{15}{32} & \frac{5}{32} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{9}{32} & \frac{15}{32} & \frac{3}{16} & \frac{1}{16} \\ \frac{9}{64} & \frac{15}{64} & \frac{15}{32} & \frac{5}{32} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{9}{32} & \frac{15}{32} & \frac{3}{16} & \frac{1}{16} \\ \frac{9}{64} & \frac{15}{64} & \frac{15}{32} & \frac{5}{32} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{9}{32} & \frac{15}{32} & \frac{3}{16} & \frac{1}{16} \\ \frac{9}{64} & \frac{15}{64} & \frac{15}{32} & \frac{5}{32} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{9}{32} & \frac{15}{32} & \frac{3}{16} & \frac{1}{16} \end{vmatrix}$$

Рисунок 1. а) матрица Q_1 РЦМ ($\nu = 1$, $\kappa = 2$) и б) матрица Q_2 РЦМ ($\nu = 2$, $\kappa = 1$).

Матрица Q_1 задает стохастическую матрицу r−сложной ЦМ, r=3.

2.2. Постановка задачи моделирования минимальным полиномом над полем GF(q) заданной РЦМ в виде (2)

Последовательностью над полем GF(q) будем называть любую функцию u: $Z \to$ GF(q), заданную на множестве Z целых неотрицательных чисел и принимающую значения в поле GF(q) [10]. Последовательность $u = (u_i)$, $i \in Z$, называется линейной рекуррентной последовательностью (ЛРП) порядка L над полем GF(q), если существуют константы $b_0, b_1, \ldots, b_{L-1} \in$ GF(q) такие, что

$$u(i+L) = \sum_{j=0}^{L-2} b_j \cdot u(i+j),\ i \geq 0\ \ [10].$$

Полином

$$f(x) = x^L - \sum_{j=0}^{L-1} b_j \cdot x^j \tag{3}$$

называется характеристическим полиномом ЛРП [10].

Вектор $\tilde{u}$ = (u(0), …, u(L-1)) – начальный вектор ЛРП. Характеристический полином ЛРП u, имеющий минимальную степень, является ее минимальным полиномом [10]. Обозначим через u_N ЛРП u произвольной длины N, где длина ЛРП - число символов в ЛРП. ЛРП реализуется линейным регистром сдвига (ЛРС) с обратной связью [10], где степень полинома $f(x)$ определяет число q−ичных разрядов регистра, а коэффициенты - вид обратной связи. Построенный минимальный полином вида (3) над полем GF(q) по алгоритму Берлекэмпа-Месси [9] будем рассматривать как характеристический полином ЛРП, которую можно получить на основе ЛРС.

Матрице Q вида (2) можно сопоставить по алгоритму [11] аппроксимации элементов w_{ij} $i, j = \overline{0, m^r - 1}$ рациональными элементами эргодическую стохастическую матрицу $P_\varphi = (p_{ij}^{(\varphi)})$, $i, j = \overline{0, t-1}$, размера $t \times t = m^r \times m^r$, где элементы $p_{ij}^{(\varphi)} = a_{ij}^{(\varphi)} / a_i^{(\varphi)}$ удовлетворяют соотношению

$$P_\varphi = (p_{ij}^{(\varphi)}) = (a_{ij}^{(\varphi)} / a_i^{(\varphi)}),\ a_i^{(\varphi)} = \sum_{j=0}^{t-1} a_{ij}^{(\varphi)} = \sum_{j=0}^{t-1} a_{ji}^{(\varphi)} \text{ и } \sum_{i=0}^{t-1} a_i^{(\varphi)} = N \tag{4}$$

и предельный вектор матрицы P_φ равен

$$\overline{\pi_\varphi} = (\pi_i^{(\varphi)} = a_i / N),\ i = \overline{0, t-1}. \tag{5}$$

Положим:

1) погрешность приближения матрицы Q матрицей $P_\varphi = (p_{ij}^{(\varphi)})$, $i, j = \overline{0, t-1}$, удовлетворяет условиям

$$|\, p_{ij}^{(\varphi)} - w_{ij} \,| \le \varepsilon,\ 0 < \varepsilon < 1; \tag{6}$$

$$p_{ij}^{(\varphi)} = \begin{cases} 0, \text{ если } w_{ij} = 0 \\ > 0, \text{ если } w_{ij} > 0 \end{cases}; \tag{7}$$

2) величина ε связана с N линейным соотношением [11]

$$N \ge N^*,\ N^* = \max\{\max_{\substack{i,j=0,t-1 \\ p_{ij}\pi_i \ne 0}} \{1/(w_{ij}\pi_i)\}, \max_{i,j=0,t-1} \{(1 + w_{ij} + \varepsilon)/(\pi_i \varepsilon)\}\}. \tag{8}$$

При принятом допущении (6)-(8) достигаемая точность приближения элементов матрицы Q элементами $p_{ij}^{(\varphi)}$ линейно зависит от N.

Решаемая задача ставится 1) как задача построения по алгоритму Берлекэмпа-Мэсси минимального полинома над полем GF(q), описывающего последовательность u_N длины N такой, что соответствующая этой последовательности стохастическая матрица $P_\varphi = (p_{ij}^{(\varphi)})$, $i, j = \overline{0, t-1}$, размера $t \times t$ должна с заданной точностью, пропорциональной величине $1/N$, аппроксимировать заданную стохастическую матрицу Q и 2) построение по полученному минимальному полиному ЛРС, позволяющего воспроизводить последовательности u_N длины N.

3.Метод моделирования расширенных цепей Маркова на основе минимального полинома

Введем величину N', удовлетворяющую условию

$$|\, N' - N \,| \le t - 1, \tag{9}$$

Теорема 2. Пусть заданы эргодическая стохастическая матрица Q размера $t \times t$ и числа $0 < \varepsilon < 1$, $N \ge N^*$. Тогда существует минимальный полином $f(x)$ над полем GF(q), вырабатывающий последовательность $u_{N'+1}$ длины $N' + 1$ с законом $P_\varphi = (p_{ij}^{(\varphi)})$, удовлетворяющим условиям (4)-(9),

$$|\, \pi_i^{(\varphi)} - \pi_i \,| \le \frac{1}{N} + \frac{\pi_i \,|\, N' - N \,|}{N}, \tag{10}$$

и степень L полинома $f(x)$ удовлетворяет условию

$$2L \le N' + 1. \tag{11}$$

Доказательство теоремы 2 можно провести в соответствии со схемой доказательства теоремы 2, представленной в [8].

Из теоремы 2 вытекает следующий метод моделирования РЦМ минимальными полиномами $f(x)$ над полем GF(q) с заданной точностью ε представления матрицы Q.

Этап 1. Пусть задана ЦМ эргодической стохастической матрицей $P = (p_{ij})$ размера $m \times m$, с конечным множеством состояний $S = \{s_j\}$, $i, j = \overline{0, m-1}$.
Вычислим матрицу Q РЦМ размера $m^r \times m^r$ через матрицу P при заданных $r = \nu + \kappa \geq 2$, $\nu \geq 1$, $\kappa \geq 1$ по формулам (1) и (2).
Отметим, матрица Q при заданных $r = \nu + \kappa \geq 2$, $\nu = 1$, $\kappa \geq 1$, задает стохастическую матрицу r−сложной ЦМ с переходными вероятностями, определяемыми элементами матрицы P.
Этап 2. По заданным Q, ε и $N \geq N^*$, с помощью алгоритма [11], строим матрицу $P_\varphi = (p_{ij}^{(\varphi)})$, $i, j = \overline{0, t-1}$, удовлетворяющую условиям (4)-(10).
Этап 3. По матрице $P_\varphi = (p_{ij}^{(\varphi)})$, по вероятностному алгоритму [12] выделения эйлеровых цепей [13], строим в алфавите $Y = \{y_i\}$, $i = \overline{0, m^{\nu+\kappa} - 1}$, последовательность $u_{N'+1}$ длины $N'+1$ с законом $P_\varphi = (p_{ij}^{(\varphi)})$, $i, j = \overline{0, t-1}$, удовлетворяющим условиям (4)-(10).
Этап 4. Закодируем символы алфавита Y элементами поля GF(q), где $q \geq t$. По последовательности $u_{N'+1}$ построим с помощью программной реализации [14] алгоритма АБМ минимальный полином $f(x)$ степени L, где L удовлетворяет условию (11) теоремы 2. Начальный вектор $\tilde{u} = (u(0), \ldots, u(L-1))$ последовательности $u_{N'+1}$ храним в памяти.
Построенный полином однозначно идентифицирует матрицу P_φ.
Этап 5. По полученному полиному $f(x)$ степени L строим программную реализацию ЛРС [14] длины L с q-ичными разрядами, где L определяется выражением

$$L = \begin{cases} (N' + 1)/2, \text{ если } N' - \text{нечетное;} \\ ((N' + 1) + 1)/2, \text{ если } N' - \text{четное.} \end{cases}$$

Отметим, алгоритм Берлекэмпа-Мэсси строит по последовательности u_{N+1} единственный минимальный полином $f(x)$ со степенью L, удовлетворяющей условию (11). Задав в качестве начального состояния ЛРС вектор $\tilde{u}$, получаем на i-ом выходе, $i = \overline{1, L}$, q-ичного разряда программной модели ЛРС последовательность $u_{N'+1}$ длины $N'+1$ с законом P_φ.

4. Заключение

Задача моделирования расширенных цепей Маркова и определенного вида сложных цепей Маркова минимальными полиномами над конечным полем решается в работе как задача построения по алгоритму Берлекэмпа-Мэсси минимального полинома над полем GF(q), характеристики $q \geq 2$, вырабатывающего последовательность длины такой, что соответствующая этой последовательности стохастическая матрица P_φ с заданной точностью, пропорциональной величине $1/N$ аппроксимирует исходную эргодическую стохастическую матрицу Q. Точность представления стохастических матриц Q минимальными полиномами линейно зависит от степени полинома. Построенный полином однозначно идентифицирует матрицу P_φ и однозначно определяет структуру q–ичного линейного регистра сдвига для моделирования расширенных цепей Маркова.

5. Литература

[1] Kemeny, J.G. Finite Markov Ghains / J.G. Kemeny, J.L. Snell. – Van Nostrand, Princeton, 1960. – 272 p.
[2] Романовский, В.И. Дискретные цепи Маркова. – М.: Гостехиздат, 1949. – 436 с.

[3] Постников, А.Г. Арифметическое моделирование случайных процессов // Труды математического института им. В.А. Стеклова АН СССР. – М.: Изд-во АН СССР, 1960. – Т. 57. – 84 с.
[4] Марков, А.А. О связанных величинах, не образующих настоящей цепи // ИАН. – 1911. – Т. 6, № 5. – С.113-126.
[5] Захаров, В.М. Представление расширенных цепей Маркова над полем GF(2^n) / В.М. Захаров, Б.Ф. Эминов // Моделирование процессов. Труды Казанского научного семинара "Методы моделирования". – 2007. – Т. 3. – С. 270-286.
[6] Эминов, Б.Ф. Алгоритм построения расширенных цепей Маркова над полем GF(2^n) // Системы управления и информационные технологии. – 2013. – Т. 3, № 1(53). – С. 186-191.
[7] Эминов, Б.Ф. Полиномиальные модели расширенных цепей Маркова над полем GF(2^n) / Б.Ф. Эминов, В.М. Захаров // Системы управления и информационные технологии. – 2014. – Т. 2, № 56. – С. 26-30.
[8] Zakharov, V.M. Representing lumped Markov chains by minimal polynomials over field $F(q)$ / V.M. Zakharov, B.F. Eminov, S.V. Shalagin // International conference information technologies in business and industry. – Journal of Physics: Conference series. – 2018. – Vol. 2015. – P. 1-6.
[9] Massey, J.L. Shift-register synthesis and BCH decoding // IEEE Trans. Inform. Theory. – 1969. – Vol. IT-15. – P. 122-127.
[10] Алферов, А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.
[11] Zakharov, V.M. Complexity of the problem of approximation stochastic matrix by rational elements / V.M. Zakharov, S.E. Kuznetsov // Fundamental of Computation Theory. International conferences. – 1987. – P. 483-487.
[12] Эминов, Б.Ф. Моделирование марковских последовательностей с погрешностью, меньшей стандартной ошибки / Б.Ф. Эминов, В.М. Захаров // Вестник КГТУ им. А.Н. Туполева. – 2011. – Т. 1. – С. 115-122.
[13] Харари, Ф. Теория графов. – М.: Мир, 1973. – 300 с.
[14] Хусаинов, Р.Н. Разработка программной реализации алгоритма Берлекэмпа-Мэсси для анализа и синтеза рекуррентных двоичных последовательностей / Р.Н. Хусаинов, Б.Ф. Эминов, М.Д. Галимов, А.И. Крюков // Вестник Казанского технологического университета. – 2015. – Т. 18, № 24. – С. 89-91.

Благодарности
Работа выполнена при финансовой поддержке гранта РФФИ № 18-01-00120 «Специализированные устройства для генерирования и обработки массивов данных в архитектуре программируемых логических интегральных схем класса FPGA».

Simulating of expanded Markov chains by minimal polynomials over the field GF(*q*)

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

[1]Kazan National State Technical University named after A.N. Tupolev, K. Marks street 10, Kazan, Russia, 420111

Abstract. A method is proposed for representing and simulating minimal polynomials of expanded and definite types of complicated Markov chains over a finite field GF(q). The simulation problem is solved as a construction problem using the Berlekamp-Massey algorithm for the minimal polynomial over the field GF(q). The polynomial produces a sequence of length N. The stochastic matrix corresponding to this sequence approximates the given stochastic matrix of the expanded Markov chain with a given accuracy proportional to the 1/N value. The constructed polynomial uniquely determines the structure of the q-ary linear shift register for modeling expanded Markov chains.