Math-Net.Ru

Общероссийский математический портал

О. В. Камловский, Свойства распределений строк и столбцов для матричных линейных рекуррентных последовательностей первого порядка, *Матем. вопр. криптогр.*, 2015, том 6, выпуск 4, 65–76

DOI: <https://doi.org/10.4213/mvk168>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.237.59.107

26 апреля 2023 г., 09:17:33

Свойства распределений строк и столбцов для матричных линейных рекуррентных последовательностей первого порядка

О. В. Камловский

ООО «Центр сертификационных исследований», Москва

Получено 10.V.2014

Рассматривается последовательность прямоугольных матриц над кольцом Галуа, удовлетворяющих линейному рекуррентному соотношению первого порядка. Устанавливаются оценки частот появлений векторов-строк и векторов-столбцов в таких последовательностях. Эти оценки обобщают известные аналогичные результаты.

Ключевые слова: кольца Галуа, последовательности матриц, матричные генераторы

Distribution properties of rows and columns for matrix linear recurrent sequences of the first order

O. V. Kamlovskiy

LLC "Certification Research Center", Moscow

Abstract. We consider sequences of matrices over Galois ring satisfying linear recurrent equation of the first order. Estimates of the frequencies of rows and columns in such sequences are obtained. These results generalize previously known bounds.

Key words: Galois rings, matrix sequences, matrix generators

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 6, no. 4, pp. 65–76 (Russian).

Введение

Пусть $R = GR(q^n, p^n)$ — кольцо Галуа характеристики p^n , состоящее из $q^n = p^{dn}$ элементов (см., например, [1]). При $n = 1$ кольцо R совпадает с полем $GF(q)$ из $q = p^d$ элементов, а при $d = 1$ кольцо R совпадает с кольцом вычетов $\mathbb{Z}_{p^n}$ примарного порядка. Обозначим через $R_{s,t}$ множество всех матриц размера $s \times t$ над кольцом R . Матрицу размера $m \times k$, состоящую из нулевых элементов, будем обозначать $O_{m,k}$. Рассмотрим последовательность $V = (V(i))_{i=0}^{\infty}$ матриц $V(i) \in R_{m,k}$, удовлетворяющую условиям

$$V(i+1) = AV(i) + B, \quad i \geq 0, \quad (1)$$

где $A \in R_{m,m}$, $B \in R_{m,k}$, а $V(0) \in R_{m,k}$ — начальная матрица. Последовательность V назовем матричной линейной рекуррентной последовательностью первого порядка.

Пусть $V(i) = (v_{st}(i))_{m \times k}$. Будем рассматривать V и последовательности $v_{st} = (v_{st}(i))_{i=0}^{\infty}$, $s = 1, \dots, m$, $t = 1, \dots, k$, как псевдослучайные последовательности. Выберем натуральные числа $r, i_1, \dots, i_r, j_1, \dots, j_r$ так, что $1 \leq i_1 < \dots < i_r \leq m$, $1 \leq j_1 < \dots < j_r \leq k$. В работе изучаются частота появления вектора $\vec{z} \in R^r$ среди l векторов

$$(v_{i_1 t}(0), \dots, v_{i_r t}(0)), \dots, (v_{i_1 t}(l-1), \dots, v_{i_r t}(l-1)),$$

взятых из t -х столбцов матриц $V(0), \dots, V(l-1)$ соответственно, а также частота появления вектора $\vec{z} \in R^r$ среди l векторов

$$(v_{s j_1}(0), \dots, v_{s j_r}(0)), \dots, (v_{s j_1}(l-1), \dots, v_{s j_r}(l-1)),$$

взятых из s -х строк этих матриц.

Оценки указанных частот в случае, когда $R = GF(q)$, $B = O_{m \times k}$, l — произвольное натуральное число, а характеристический многочлен $F(x)$ матрицы A является примитивным многочленом над полем $GF(q)$, были получены В. И. Нечаевым в [2, теоремы 1 и 2]. Позже В. Н. Цыпышев в [3, утверждение 3] были получены оценки исследуемых величин для случая, когда $R = GR(q^n, p^n)$, B — произвольная матрица, A — матрица с характеристическим многочленом $F(x)$ максимального периода, а l совпадает с периодом этого многочлена. В настоящей работе приводятся оценки рассматриваемых частот, обобщающие результаты указанных двух работ и справедливые, когда $F(x)$ является многочленом Галуа (не обязательно максимального периода).

Отметим, что в некоторых зарубежных работах рассматриваются последовательности V вида (1) при $k = 1$. В этом случае V называют последовательностью, порожденной матричным конгруэнтным генератором (см. [4,

с. 34–35]). Статистические свойства таких последовательностей для случая, когда $R = GF(p)$ — простое поле, достаточно хорошо изучены (см. [5, 6] и цитированную там литературу).

1. Линейные рекурренты векторов

Рассмотрим произвольные последовательности $u_1, u_2, \dots, u_r$ над кольцом $R = GR(q^n, p^n)$. Данную систему последовательностей назовем линейно независимой над кольцом R , если для всех ненулевых векторов $(c_1, c_2, \dots, c_r) \in R^r$ последовательность $c_1 u_1 + c_2 u_2 + \dots + c_r u_r$ является ненулевой. Пусть φ — естественный эпиморфизм кольца R в факторкольцо $\bar{R} = R/pR = GF(q)$. Для произвольного элемента $c \in R$ обозначим через $\bar{c}$ элемент $\varphi(c)$. Аналогично для последовательности $u \in R^\infty$ обозначим через $\bar{u}$ последовательность, элементы которой определены равенством $\bar{u}(i) = \varphi(u(i))$ для всех $i \geq 0$.

Известно, что последовательности $u_1, u_2, \dots, u_r$ линейно независимы над кольцом R тогда и только тогда, когда последовательности $\bar{u}_1, \bar{u}_2, \dots, \bar{u}_r$ линейно независимы над полем $GF(q)$. Кроме того, если u — линейная рекуррентная последовательность (ЛРП) над кольцом R с характеристическим многочленом $F(x)$, то последовательность $\bar{u}$ будет ЛРП над полем $\bar{R}$ с характеристическим многочленом $\bar{F}(x)$, который является образом многочлена $F(x)$ при действии естественного эпиморфизма из кольца $R[x]$ в кольцо $\bar{R}[x]$. Обозначим через $L_R(F)$ множество всех ЛРП над кольцом R с характеристическим многочленом $F(x)$. Унитарный многочлен $F(x) \in R[x]$ называется реверсивным многочленом Галуа, если $\bar{F}(x)$ неприводим над полем $\bar{R}$ и $F(0)$ обратим в R , т. е. $\bar{F}(x) \neq x$. Каждый многочлен $F(x)$ максимального периода над кольцом R является реверсивным многочленом Галуа (см. [7]).

В случае когда система последовательностей $u_1, u_2, \dots, u_r \in L_R(F)$ линейно независима над кольцом R , очевидно, что $r \leq m$, где $m = \deg F(x)$ — степень многочлена $F(x)$. Более того, все рассматриваемые последовательности принадлежат множеству $L_R(F)^*$, состоящему из всех ЛРП множества $L_R(F)$, у которых в начальном векторе есть хотя бы один обратимый элемент кольца R .

Пусть $u_1, u_2, \dots, u_r \in L_R(F)$. Последовательность $(u_1(i), \dots, u_r(i))_{i=0}^\infty$ назовем ЛРП векторов. В дальнейшем нам понадобятся оценки частот $N_l(\vec{z}, u_1, \dots, u_r)$ появления вектора $\vec{z} = (z_1, z_2, \dots, z_r) \in R^r$ среди векторов $(u_1(i), u_2(i), \dots, u_r(i))$, где $i \in \{0, 1, \dots, l-1\}$.

Теорема 1 ([8, 9]). Пусть $F(x)$ — реверсивный многочлен Галуа степени m над кольцом $R = GR(q^n, p^n)$, $T(F) = p^\nu T(\bar{F})$, $u_1, u_2, \dots, u_r$ — линейно независимая система ЛРП из $L_R(F)$. Тогда для всех $\vec{z} \in R^r$ и каждого такого $l \in \mathbb{N}$, что $l \leq T(F)$, справедлива оценка

$$\left| N_l(\vec{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| < \frac{p^\nu (p^n q^{nr} - 1) (q^r - 1)}{q^{nr} (pq^r - 1)} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}}. \quad (2)$$

Отметим, что оценка из теоремы 1 уточняет и обобщает аналогичные оценки из работ [2, теорема 1], [10, теорема 1] и [11, теорема 1].

Величина l/q^{nr} представляет собой «естественное» среднее значение для числа появлений вектора $\vec{z}$ на отрезке длины l последовательности векторов. Теорема 1 устанавливает верхнюю оценку отклонения частоты $N_l(\vec{z}, u_1, \dots, u_r)$ от этого среднего значения. Из результатов работы [8] следует, что оценка (2) является асимптотически неупрощаемой. Отметим, что при $l = T(F)$ множитель $(4/\pi^2) \ln T(\bar{F}) + (9/5)$ из оценки можно убрать (см. [8]).

Приведем более простую, но менее точную оценку, которую будем использовать в дальнейшем.

Следствие 1. В условиях теоремы 1 выполнено неравенство

$$\left| N_l(\vec{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| < \frac{q^{nr} - 1}{q^{nr}} p^{n+\nu-1} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}}. \quad (3)$$

Из неравенства (3) следуют верхняя и нижняя оценки рассматриваемой частоты:

$$N_l(\vec{z}, u_1, \dots, u_r) > \frac{l}{q^{nr}} - \frac{q^{nr} - 1}{q^{nr}} p^{n+\nu-1} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}},$$

$$N_l(\vec{z}, u_1, \dots, u_r) < \frac{l}{q^{nr}} + \frac{q^{nr} - 1}{q^{nr}} p^{n+\nu-1} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}}.$$

При выполнении условия

$$l \geq (q^{nr} - 1) p^{n+\nu-1} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}}$$

нижняя оценка будет нетривиальной, т. е. больше нуля. Если

$$l \geq p^{n+\nu-1} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}},$$

то верхняя оценка является нетривиальной, т. е. меньше l .

2. Однородный способ выработки матриц

Пусть $R = GR(q^n, p^n)$, $U = (U(i))_{i=0}^\infty$ — последовательность матриц из множества $R_{m,k}$, построенная по правилу

$$U(i+1) = AU(i), \quad i \geq 0, \quad (4)$$

где $U(0) \in R_{m,k}$. В этом случае будем говорить, что последовательность U является однородной матричной линейной рекуррентной последовательностью первого порядка.

Из равенства (4) следует, что

$$U(i) = A^i U(0), \quad i \geq 0. \quad (5)$$

Обратно, если выполнено равенство (5), то справедливо равенство (4).

Опишем частотные характеристики последовательности U . Для каждой матрицы $C = (c_{ij})$ над кольцом R обозначим через $\bar{C}$ матрицу над полем $\bar{R} = GF(q)$, в которой все элементы c_{ij} заменены на образы $\bar{c}_{ij}$ при действии естественного эпиморфизма $\varphi : R \rightarrow \bar{R}$.

Пусть $U(i) = (u_{st}(i))_{m \times k}$ для всех $i \geq 0$. Обозначим через u_{st} последовательность $(u_{st}(i))_{i=0}^\infty$, где $s \in \{1, 2, \dots, m\}$, $t \in \{1, 2, \dots, k\}$. Таким образом, u_{st} — последовательность элементов кольца R , расположенных в матрицах $U(0), U(1), \dots$ на пересечении строки с номером s и столбца с номером t . Введем обозначение $\bar{U}(i) = (\bar{u}_{st}(i))_{m \times k}$ при всех $i \geq 0$. Свойства последовательности u_{st} описывает следующая теорема.

Теорема 2. Если $F(x)$ — характеристический многочлен матрицы A , то $u_{st} \in L_R(F)$ для всех $s \in \{1, \dots, m\}$, $t \in \{1, \dots, k\}$. Если к тому же $F(x)$ — многочлен Галуа над кольцом R , то:

1) система $u_{1t}, u_{2t}, \dots, u_{mt}$, $t \in \{1, \dots, k\}$, линейно независима над R тогда и только тогда, когда t -й столбец матрицы $\bar{U}(0)$ отличен от нулевого;

2) все последовательности u_{st} , $s \in \{1, \dots, m\}$, $t \in \{1, \dots, k\}$, принадлежат $L_R(F)^*$ тогда и только тогда, когда все столбцы матрицы $\bar{U}(0)$ отличны от нулевого;

3) все системы $u_{s1}, u_{s2}, \dots, u_{sk}$, $s \in \{1, \dots, m\}$, линейно независимы тогда и только тогда, когда $\text{rang } \bar{U}(0) = k$.

Доказательство. Пусть

$$F(x) = x^m - a_{m-1}x^{m-1} - \dots - a_1x - a_0$$

является характеристическим многочленом матрицы A . Тогда $F(A) = O_{m \times m}$ (см. [12, 13]) и выполнено равенство

$$A^m = \sum_{j=0}^{m-1} a_j A^j.$$

Домножив обе части этого равенства на A^i , получим

$$A^{m+i} = \sum_{j=0}^{m-1} a_j A^{j+i}, \quad i \geq 0.$$

Отсюда и из равенства (5) следует, что

$$A^{m+i}U(0) = U(m+i) = \sum_{j=0}^{m-1} a_j A^{j+i}U(0) = \sum_{j=0}^{m-1} a_j U(i+j), \quad i \geq 0.$$

В частности, для всех $s \in \{1, \dots, m\}$, $t \in \{1, \dots, k\}$

$$u_{st}(m+i) = \sum_{j=0}^{m-1} a_j u_{st}(i+j), \quad i \geq 0.$$

Таким образом, $u_{st} \in L_R(F)$.

Докажем утверждение пункта 1. Пусть $F(x)$ — многочлен Галуа над кольцом R . Обозначим t -й столбец матрицы $U(0)$ через

$$a^\downarrow = \begin{pmatrix} u_{1t}(0) \\ u_{2t}(0) \\ \dots \\ u_{mt}(0) \end{pmatrix}.$$

Тогда согласно (5)

$$A^i a^\downarrow = \begin{pmatrix} u_{1t}(i) \\ u_{2t}(i) \\ \dots \\ u_{mt}(i) \end{pmatrix}, \quad i \geq 0. \quad (6)$$

Если столбец $\bar{a}^\downarrow \in \bar{R}^{(m)}$ нулевой, то система $\bar{u}_{1t}, \dots, \bar{u}_{mt}$ состоит только из нулевых последовательностей и система $u_{1t}, \dots, u_{mt}$ линейно зависима над R . Пусть теперь столбец $\bar{a}^\downarrow$ ненулевой. По доказанному выше последовательности $u_{1t}, \dots, u_{mt}$ принадлежат множеству $L_R(F)$, поэтому согласно [14, гл. 25,

утв. 3] условие линейной независимости рассматриваемой системы равносильно тому, что

$$\text{rang} \begin{pmatrix} \bar{u}_{1t}(0) & \bar{u}_{1t}(1) & \dots & \bar{u}_{1t}(m-1) \\ \bar{u}_{2t}(0) & \bar{u}_{2t}(1) & \dots & \bar{u}_{2t}(m-1) \\ \dots & \dots & \dots & \dots \\ \bar{u}_{mt}(0) & \bar{u}_{mt}(1) & \dots & \bar{u}_{mt}(m-1) \end{pmatrix} = m.$$

Из равенства (6) следует, что достаточно доказать соотношение

$$\text{rang}(\bar{a}^\downarrow, \bar{A}\bar{a}^\downarrow, \bar{A}^2\bar{a}^\downarrow, \dots, \bar{A}^{m-1}\bar{a}^\downarrow) = m. \quad (7)$$

Рассмотрим отображение $\varphi: \bar{R}^{(m)} \rightarrow \bar{R}^{(m)}$, определенное по правилу

$$\varphi(x^\downarrow) = \bar{A}x^\downarrow, \quad x^\downarrow \in \bar{R}^{(m)}.$$

Отображение φ является линейным преобразованием пространства $\bar{R}^{(m)}$, причем в базисе $\bar{e} = (e_1^\downarrow, e_2^\downarrow, \dots, e_m^\downarrow)$, где

$$e_1^\downarrow = \begin{pmatrix} \bar{e} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2^\downarrow = \begin{pmatrix} 0 \\ \bar{e} \\ \vdots \\ 0 \end{pmatrix}, \dots, e_m^\downarrow = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \bar{e} \end{pmatrix},$$

матрица преобразования φ равна $\bar{A}$. Так как характеристический многочлен $\bar{F}(x)$ линейного преобразования φ неприводим над полем $\bar{R}$, то минимальный многочлен ненулевого вектора $\bar{a}^\downarrow$ относительно преобразования φ равен $\bar{F}(x)$. Система $\bar{a}^\downarrow, \varphi(\bar{a}^\downarrow) = \bar{A}\bar{a}^\downarrow, \dots, \varphi^{m-1}(\bar{a}^\downarrow) = \bar{A}^{m-1}\bar{a}^\downarrow$ линейно независима, так как $\deg F(x) = m$. Таким образом, равенство (7) доказано.

Докажем утверждение пункта 2. Если t -й столбец матрицы $\bar{U}(0)$ нулевой, то из равенства (6) следует, что каждая из последовательностей $\bar{u}_{1t}, \dots, \bar{u}_{mt}$ нулевая, а значит, $u_{1t}, \dots, u_{mt} \notin L_R(F)^*$. Пусть теперь все столбцы матрицы $\bar{U}(0)$ ненулевые, тогда согласно пункту 1 система $u_{1t}, \dots, u_{mt}$ линейно независима для всех $t \in \{1, \dots, k\}$. В частности, отсюда следует, что ЛРП u_{st} принадлежит $L_R(F)^*$ для всех $s \in \{1, \dots, m\}$ и $t \in \{1, \dots, k\}$.

Докажем теперь утверждение пункта 3. Система $u_{s1}, \dots, u_{sk}$ по доказанному выше состоит из ЛРП с характеристическим многочленом $F(x)$. Значит, ее линейная независимость равносильна соотношению

$$\text{rang} \begin{pmatrix} \bar{u}_{s1}(0) & \bar{u}_{s1}(1) & \dots & \bar{u}_{s1}(m-1) \\ \bar{u}_{s2}(0) & \bar{u}_{s2}(1) & \dots & \bar{u}_{s2}(m-1) \\ \dots & \dots & \dots & \dots \\ \bar{u}_{sk}(0) & \bar{u}_{sk}(1) & \dots & \bar{u}_{sk}(m-1) \end{pmatrix} = k. \quad (8)$$

Из равенства (5) для транспонированных матриц имеем

$$(\bar{u}_{s1}(i), \bar{u}_{s2}(i), \dots, \bar{u}_{sk}(i))^{\top} = ((e_s^{\downarrow})^{\top} \bar{A}^i \bar{U}(0))^{\top} = \bar{U}(0)^{\top} (\bar{A}^{\top})^i e_s^{\downarrow}.$$

Отсюда получим, что

$$\begin{pmatrix} \bar{u}_{s1}(0) & \bar{u}_{s1}(1) & \dots & \bar{u}_{s1}(m-1) \\ \bar{u}_{s2}(0) & \bar{u}_{s2}(1) & \dots & \bar{u}_{s2}(m-1) \\ & & \dots & \\ \bar{u}_{sk}(0) & \bar{u}_{sk}(1) & \dots & \bar{u}_{sk}(m-1) \end{pmatrix} = \bar{U}(0)^{\top} (e_s^{\downarrow}, (\bar{A}^{\top})e_s^{\downarrow}, \dots, (\bar{A}^{\top})^{m-1}e_s^{\downarrow}). \quad (9)$$

Характеристический многочлен матрицы $\bar{A}^{\top}$ равен $\bar{F}(x)$. В силу того что вектор $e_s^{\downarrow}$ является ненулевым, по аналогии с доказательством пункта 1 получим равенство

$$\text{rang}(e_s^{\downarrow}, (\bar{A}^{\top})e_s^{\downarrow}, \dots, (\bar{A}^{\top})^{m-1}e_s^{\downarrow}) = m.$$

Значит, согласно (9)

$$\text{rang} \begin{pmatrix} \bar{u}_{s1}(0) & \bar{u}_{s1}(1) & \dots & \bar{u}_{s1}(m-1) \\ \bar{u}_{s2}(0) & \bar{u}_{s2}(1) & \dots & \bar{u}_{s2}(m-1) \\ & & \dots & \\ \bar{u}_{sk}(0) & \bar{u}_{sk}(1) & \dots & \bar{u}_{sk}(m-1) \end{pmatrix} = \text{rang} \bar{U}(0)^{\top} = \text{rang} \bar{U}(0).$$

Таким образом, для всех $s \in \{1, \dots, m\}$ условие (8) равносильно соотношению $\text{rang} \bar{U}(0) = k$. $\square$

Отметим, что аналог теоремы 2 для случая конечного поля $R = GF(q)$ впервые был доказан в [2, теорема 2], однако доказательство существенно опиралось на максимальность периода многочлена $F(x)$. Теорема 2 сводит исследование числа появлений вектора $\vec{z} \in R^r$ среди векторов

$$(u_{i_1 t}(0), \dots, u_{i_r t}(0)), \dots, (u_{i_1 t}(l-1), \dots, u_{i_r t}(l-1)),$$

взятых из t -х столбцов матриц $U(0), \dots, U(l-1)$ соответственно, а также среди векторов

$$(u_{s j_1}(0), \dots, u_{s j_r}(0)), \dots, (u_{s j_1}(l-1), \dots, u_{s j_r}(l-1)),$$

взятых из s -х строк этих матриц, к исследованию частотных характеристик ЛРП векторов.

Непосредственно из оценки (3) и теоремы 2 получим следующий результат.

Теорема 3. Пусть $R = GR(q^n, p^n)$, U — последовательность матриц, полученная по правилу (4), и характеристический многочлен $F(x)$ матрицы A является реверсивным многочленом Галуа степени m над кольцом R , $\vec{z} \in R^r$. Тогда для каждого $l \leq T(F)$ справедливы следующие утверждения:

1) если t -й столбец матрицы $\bar{U}(0)$ ненулевой, то для всех $1 \leq i_1 < \dots < i_r \leq m$

$$\left| N_l(\vec{z}, u_{i_1 t}, \dots, u_{i_r t}) - \frac{l}{q^{nr}} \right| < \frac{q^{nr} - 1}{q^{nr}} p^{n+\nu-1} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}};$$

2) если $\text{rang } \bar{U}(0) = k$, то для всех $s \in \{1, \dots, m\}$, $1 \leq j_1 < \dots < j_r \leq k$

$$\left| N_l(\vec{z}, u_{sj_1}, \dots, u_{sj_r}) - \frac{l}{q^{nr}} \right| < \frac{q^{nr} - 1}{q^{nr}} p^{n+\nu-1} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}}.$$

3. Неоднородный способ выработки матриц

Пусть $R = GR(q^n, p^n)$, $V = (V(i))_{i=0}^\infty$ — последовательность матриц из множества $R_{m,k}$, построенная по правилу (1), где $B \neq O_{m \times k}$. В этом случае назовем V неоднородной матричной линейной рекуррентной последовательностью первого порядка. Опишем частотные характеристики последовательности V . Для этого понадобятся некоторые вспомогательные результаты.

Из равенства (1) несложно получить равенство

$$V(i) = A^i V(0) + A^{i-1} B + \dots + AB + B, \quad i \geq 0. \quad (10)$$

Утверждение 1. Пусть $R = GR(q^n, p^n)$, $V = (V(i))_{i=0}^\infty$ — последовательность матриц, построенная по правилу (1). Тогда если матрица $A - E$ обратима над кольцом R , то

$$V(i) = U(i) + C, \quad i \geq 0, \quad (11)$$

где $C = -(A - E)^{-1} B$, а $U = (U(i))_{i=0}^\infty$ — последовательность, удовлетворяющая равенствам

$$U(i) = A^i (V(0) - C), \quad i \geq 0.$$

Доказательство. Заметим, что имеют место равенства

$$(A - E)(A^{i-1} B + \dots + AB + B) = (A - E)(A^{i-1} + \dots + A + E)B = (A^i - E)B.$$

Отсюда получим

$$A^{i-1}B + \dots + AB + B = (A - E)^{-1}(A^i - E)B. \quad (12)$$

Тогда из равенств (10), (12) и перестановочности матриц $(A - E)^{-1}$, A следует, что

$$V(i) = A^i V(0) + (A - E)^{-1}(A^i - E)B = A^i(V(0) - C) + C = U(i) + C. \quad \square$$

Утверждение 1 сводит исследование частотных характеристик последовательности V , построенной по правилу (1), к исследованию частотных характеристик однородной последовательности U .

Нам понадобится следующий вспомогательный результат, вытекающий из результатов работы [7, лемма 5.2].

Лемма 1. Пусть $R = GR(q^n, p^n)$, $A \in R_{m,m}$ и характеристический многочлен $F(x)$ матрицы A является многочленом Галуа. Тогда если $\bar{F}(x) \neq x - \bar{e}$, то матрица $A - E$ обратима над кольцом R .

Отметим, что согласно [12, сл. 1 из теоремы 5] матрица A , у которой характеристический многочлен $F(x)$ является многочленом Галуа, подобна сопровождающей матрице $S(F)$ этого многочлена.

Теорема 4. Пусть $R = GR(q^n, p^n)$, $V = (V(i))_{i=0}^\infty$ — последовательность матриц, построенная по правилу (1), характеристический многочлен $F(x)$ матрицы A является реверсивным многочленом Галуа над кольцом R , $\bar{F}(x) \neq x - \bar{e}$, $C = -(A - E)^{-1}B$. Тогда для каждого $l \leq T(F)$ справедливы утверждения:

1) если t -й столбец матрицы $\bar{V}(0) - \bar{C}$ ненулевой, то для всех $1 \leq i_1 < \dots < i_r \leq m$

$$\left| N_l(\bar{z}, v_{i_1 t}, \dots, v_{i_r t}) - \frac{l}{q^{nr}} \right| < \frac{q^{nr} - 1}{q^{nr}} p^{n+\nu-1} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}};$$

2) если $\text{rang}(\bar{V}(0) - \bar{C}) = k$, то для всех $s \in \{1, \dots, m\}$ и $1 \leq j_1 < \dots < j_r \leq k$

$$\left| N_l(\bar{z}, v_{s j_1}, \dots, v_{s j_r}) - \frac{l}{q^{nr}} \right| < \frac{q^{nr} - 1}{q^{nr}} p^{n+\nu-1} \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) q^{\frac{m}{2}}.$$

Доказательство. Из равенства (11) следует, что для всех $s \in \{1, \dots, m\}$ и $t \in \{1, \dots, k\}$

$$v_{st}(i) = u_{st}(i) + c_{st}, \quad i \geq 0, \quad (13)$$

где $C = (c_{st})_{m \times k}$. Тогда согласно (13) для всех $i \geq 0$

$$\begin{pmatrix} v_{i_1 t}(i) \\ v_{i_2 t}(i) \\ \dots \\ v_{i_r t}(i) \end{pmatrix} = \begin{pmatrix} u_{i_1 t}(i) \\ u_{i_2 t}(i) \\ \dots \\ u_{i_r t}(i) \end{pmatrix} + \begin{pmatrix} c_{i_1 t} \\ c_{i_2 t} \\ \dots \\ c_{i_r t} \end{pmatrix},$$

$$(v_{s_{j_1}}(i), v_{s_{j_2}}(i), \dots, v_{s_{j_r}}(i)) = (u_{s_{j_1}}(i), u_{s_{j_2}}(i), \dots, u_{s_{j_r}}(i)) + (c_{s_{j_1}}, c_{s_{j_2}}, \dots, c_{s_{j_r}}).$$

Таким образом, если $\vec{z} = (z_1, z_2, \dots, z_r)$, то

$$N_l(\vec{z}, v_{i_1 t}, \dots, v_{i_r t}) = N_l((z_{i_1} - c_{i_1 t}, \dots, z_{i_r} - c_{i_r t}), u_{i_1 t}, \dots, u_{i_r t}),$$

$$N_l(\vec{z}, v_{s_{j_1}}, \dots, v_{s_{j_r}}) = N_l((z_{j_1} - c_{s_{j_1}}, \dots, z_{j_r} - c_{s_{j_r}}), u_{s_{j_1}}, \dots, u_{s_{j_r}}),$$

и остается воспользоваться оценками из теоремы 3. $\square$

В заключение отметим, что периодические свойства последовательности V , определенной равенством (1), нетрудно описать, используя теорему 2 и утверждение 1. Некоторые результаты в этом направлении получены в [3, утв. 1].

Список литературы

- [1] Нечаев А. А., “Код Кердока в циклической форме”, *Дискрет. матем.*, **1**:4 (1989), 123–139.
- [2] Нечаев В. И., “Распределение знаков в последовательности прямоугольных матриц над конечным полем”, *Труды Математического института имени В.А.Стеклова*, **218** (1997), 335–342.
- [3] Цыпышев В. Н., “Матричный линейный конгруэнтный генератор над кольцом Галуа нечетной характеристики”, *Чебышевский сборник*, **4**:1 (2003), 112–124.
- [4] Gentle J. E., *Random number generation and Monte Carlo methods*, New York, Springer-Verlag, 2003.
- [5] Afflerbach L., Grothe H., “The lattice structure of pseudo-random vectors generated by matrix generators”, *J. Comput. Appl. Math.*, **23** (1988), 127–131.
- [6] Niederreiter H., “Statistical independence properties of pseudorandom vectors produced by matrix generators”, *J. Comput. Appl. Math.*, **31** (1990), 139–151.
- [7] Нечаев А. А., “Цикловые типы линейных подстановок над конечными коммутативными кольцами”, *Матем. сб.*, **184**:3 (1993), 21–56.
- [8] Камловский О. В., “Частотные характеристики линейных рекуррентных последовательностей над кольцами Галуа”, *Матем. сб.*, **200**:4 (2009), 31–52.
- [9] Камловский О. В., “Частотные характеристики разрядных последовательностей линейных рекуррент над кольцами Галуа”, *Изв. РАН*, **77**:6 (2013), 71–96.
- [10] Коробов Н. М., “Распределение невычетов и первообразных корней в рекуррентных рядах”, *Доклады АН СССР*, **88**:4 (1953), 603–606.

- [11] Niederreiter H., “Distribution properties of feedback shift register sequences”, *Probl. Control and Inform. Theory*, **15**:1 (1986), 19–34.
- [12] Нечаев А. А., “О подобии матриц над коммутативным локальным артиновым кольцом”, *Труды семинара им. Петровского И.Г.*, **184**:9 (1983), 81–101.
- [13] Ленг С., *Алгебра*, М.: Мир, 1968, 564 с.
- [14] Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра: учебник*, **2**, М.: Гелиос АРВ, 2003, 416 с.