ИНФОРМАТИКА

2014 **январь-март** **№ 1**

ЗАЩИТА ИНФОРМАЦИИ

УДК 004.421.5-519.217.2

И.Б. Бережной, Ю.С. Харин

ВЕРОЯТНОСТНАЯ МОДЕЛЬ ДИНАМИКИ ПАМЯТИ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ МАКЛАРЕНА – МАРСАЛЬИ

Рассматривается класс криптографических генераторов псевдослучайных последовательностей Макларена – Марсальи. Исследуется вероятностная модель динамики памяти генераторов Макларена – Марсальи. Показываются результаты компьютерных экспериментов.

Введение

В криптографической защите информации важную роль играют последовательности случайных чисел [1, 2]. На практике для их генерации в основном используют программные генераторы, когда с помощью детерминированного алгоритма создается псевдослучайная последовательность, как можно больше похожая на случайную. В последнее время особое внимание уделяется генераторам с памятью. Так, в конкурсе eSTREAM, целью которого было создание европейских стандартов для поточных систем шифрования, два из четырех финалистов в профиле «поточные шифры для программного применения с большой пропускной способностью» являются такими генераторами [3]. Современные генераторы в подавляющем большинстве являются комплексами комбинированных определенным образом модулей, представляющих собой различные криптографические примитивы [1, 2]. Данные примитивы для эффективной работы всего генератора должны иметь достаточно простую структуру и при этом обладать хорошими криптографическими свойствами. Одним из таких широко известных примитивов является класс генераторов Макларена – Марсальи [4], который сочетает свойство простоты реализации с достаточно высоким качеством выходной последовательности [5]. Интерес к данному классу генераторов не угасает: один из участников конкурса eSTREAM – поточный шифр Ямб [6] – содержит модуль аналогичной структуры.

Ранее класс генераторов Макларена – Марсальи изучался авторами в статье [7]. Для него получена формула для периода выходной последовательности, уточняющая приведенную в [2] формулу, доказаны некоторые вероятностные свойства, на основании которых построены формулы и оценки, характеризующие влияние генератора на некоторые статистические характеристики выходной последовательности. В настоящей статье продолжено исследование класса генераторов Макларена – Марсальи: исследуется вероятностная модель динамики памяти, найдены некоторые свойства и вероятностные характеристики предельного распределения памяти, приведены результаты компьютерных экспериментов.

1. Математическая модель генераторов Макларена – Марсальи

Генераторы Макларена – Марсальи, исследуемые в данной статье, имеют структуру, представленную на рисунке. Любой генератор данного семейства состоит из модифицируемой памяти X размера L и двух простейших генераторов псевдослучайных последовательностей G_1 и G_2. Генератор G_1 порождает «заполняющую» (исходную) последовательность $\{\xi_t\}$ над некоторым конечным множеством V, генератор G_2 – «управляющую» последовательность $\{\eta_t\}$ над множеством $A = \{0,1,\dots,L-1\}$. Результирующей (выходной) последовательностью является последовательность $\{y_t\}$ над V. Имеется некоторое начальное заполнение памяти – вектор-столбец $X_0 = (x_{0,1}, x_{0,2}, \dots, x_{0,L})^T \in V^L$ (T – знак транспонирования).

Определим функцию $Y = \chi(X, v, a)$, где $X, Y \in V^L$, $v \in V$, $a \in A$, следующим образом:

$$Y = (y_1, y_2, \dots, y_L), \quad y_i = \begin{cases} x_i, & \text{если } i \neq a; \\ v, & \text{если } i = a. \end{cases} \qquad (1)$$

Другими словами, функция $\chi(\mathrm{X}, v, a)$ заменяет в векторе X значение элемента с номером a на значение v.

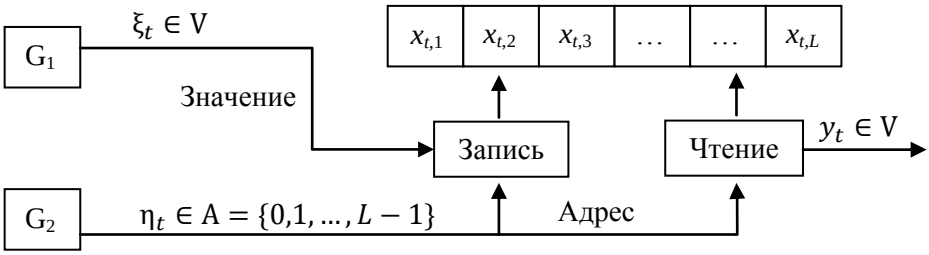

Схема генератора Макларена – Марсальи

Пусть $\{\mathrm{X}_t\colon\ t = 1, 2, \ldots\}$ – последовательность состояний памяти X; X_0 – некоторое начальное заполнение памяти. Тогда динамика генератора на тактах $t = 1, 2, \ldots$ опишется формулами

$$\begin{aligned} y_t &= x_{t-1,\xi_t}; \\ \mathrm{X}_t &= \chi(\mathrm{X}_{t-1}, \xi_t, \eta_t). \end{aligned} \tag{2}$$

Таким образом, на каждом такте в выходную последовательность считывается элемент из памяти X по адресу, определяемому генератором G_2, затем по этому адресу в память заносится новый элемент из последовательности, порождаемой генератором G_1.

2. Вероятностная модель динамики памяти

Пусть $\{\xi_t\}$ и $\{\eta_t\}$ – определенные на некотором вероятностном пространстве $(\Omega, \mathrm{F}, \mathrm{P})$ последовательности независимых в совокупности случайных величин с распределениями вероятностей

$$\mathrm{P}\{\xi_t = i\} = \lambda_i \neq 0,\ i \in \mathrm{V}, \sum_{i\in\mathrm{V}} \lambda_i = 1;\ \mathrm{P}\{\eta_t = j\} = \gamma_j \neq 0,\ j \in \mathrm{A},\ \sum_{j\in\mathrm{A}} \gamma_j = 1. \tag{3}$$

Теорема 1. *Пусть* $\{\xi_t\}$ *и* $\{\eta_t\}$ *— определенные на некотором вероятностном пространстве* $(\Omega, \mathrm{F}, \mathrm{P})$ *последовательности независимых в совокупности случайных величин с распределениями вероятностей* (3)*. Тогда последовательность состояний памяти* $\{\mathrm{X}_t\}$ *представляет собой регулярную цепь Маркова первого порядка с пространством состояний* V^L *и матрицей переходных вероятностей* $P = (p_{\mathrm{J,K}})$*:*

$$p_{\mathrm{J,K}} = \mathrm{P}\{\mathrm{X}_{t+1} = \mathrm{K} | \mathrm{X}_t = \mathrm{J}\} = \sum_{i\in\mathrm{V}} \sum_{j\in\mathrm{A}} \lambda_i \gamma_j \delta_{\mathrm{K},\chi(\mathrm{J},i,j)}\ ,\ \mathrm{J}, \mathrm{K} \in \mathrm{V}^L, \tag{4}$$

где $\delta_{\mathrm{J,K}} = \begin{cases} 1, & \mathrm{J} = \mathrm{K} \\ 0, & \mathrm{J} \neq \mathrm{K} \end{cases}$ *– символ Кронекера.*

Доказательство. В силу формулы (2) и отсутствия зависимости между элементами последовательностей $\{\xi_t\}$ и $\{\eta_t\}$ последовательность $\{\mathrm{X}_t\}$ представляет собой цепь Маркова первого порядка, так как выполняется марковское свойство [8]:

$$\begin{aligned} &\mathrm{P}\{\mathrm{X}_t = \mathrm{W}_t | \mathrm{X}_{t-1} = \mathrm{W}_{t-1}, \mathrm{X}_{t-2} = \mathrm{W}_{t-2}, \ldots, \mathrm{X}_0 = \mathrm{W}_0\} = \\ &= \mathrm{P}\{\chi(\mathrm{X}_{t-1}, \xi_t, \eta_t) = \mathrm{W}_t | \mathrm{X}_{t-1} = \mathrm{W}_{t-1}, \mathrm{X}_{t-2} = \mathrm{W}_{t-2}, \ldots, \mathrm{X}_0 = \mathrm{W}_0\} = \\ &= \mathrm{P}\{\chi(\mathrm{W}_{t-1}, \xi_t, \eta_t) = \mathrm{W}_t | \mathrm{X}_{t-1} = \mathrm{W}_{t-1}\} = \mathrm{P}\{\mathrm{X}_t = \mathrm{W}_t | \mathrm{X}_{t-1} = \mathrm{W}_{t-1}\}, \end{aligned}$$

где $\mathrm{W}_0, \mathrm{W}_1, \ldots, \mathrm{W}_t \in \mathrm{V}^L, t \geq 1$.

На основании формулы (1), а также согласно формуле полной вероятности и в силу отсутствия зависимости между элементами последовательностей $\{\xi_t\}$ и $\{\eta_t\}$ переходная вероятность находится из выражения

$$\mathrm{P}\{\mathrm{X}_t = \mathrm{K}|\mathrm{X}_{t-1} = \mathrm{J}\} = \sum_{i\in\mathrm{V}}\sum_{j\in\mathrm{A}} \mathrm{P}\{\xi_t = i, \eta_t = j\}\mathrm{P}\{\mathrm{X}_t = \mathrm{K}|\mathrm{X}_{t-1} = \mathrm{J}, \xi_t = i, \eta_t = j\}$$
$$= \sum_{\mathrm{i}\in\mathrm{V}}\sum_{j\in\mathrm{A}} \lambda_i\gamma_j\mathrm{P}\{\mathrm{X}_t = \mathrm{K}|\mathrm{X}_t = \chi(\mathrm{X}_{t-1}, i, j)\} = \sum_{i\in\mathrm{V}}\sum_{j\in\mathrm{A}} \lambda_i\gamma_j\delta_{\mathrm{K},\chi(\mathrm{J},i,j)}.$$

Так как $\mathrm{P}\{\mathrm{X}_t = \mathrm{K}|\mathrm{X}_{t-1} = \mathrm{J}\}$ не зависит от *t*, то $\{\mathrm{X}_t\}$ – однородная цепь Маркова. Для ее регулярности необходимо и достаточно существование такого *n*, что P^n не содержит нулевых элементов [8]. Рассмотрим матрицу $P^L = (p^{(L)}_{\mathrm{J,K}})$. Допустим, что существуют такие $\mathrm{U}, \mathrm{W} \in \mathrm{V}^L$, что $p^{(L)}_{\mathrm{U,W}} = 0$. Построим последовательность векторов $\{\mathrm{U}_0, \mathrm{U}_1, \mathrm{U}_2, \dots, \mathrm{U}_L\}$ следующим образом:

$$\mathrm{U}_0 = \mathrm{U},\ \mathrm{U}_1 = \chi(\mathrm{U}_0, w_1, 1), \mathrm{U}_2 = \chi(\mathrm{U}_1, w_2, 2), \dots, \mathrm{U}_L = \chi(\mathrm{U}_{L-1}, w_L, L) = \mathrm{W},$$

где $\mathrm{W} = (w_1, w_2, \dots, w_L)^T$. Для последовательности $\{\mathrm{U}_i\}$ по построению справедливо соотношение $p_{\mathrm{U}_i,\mathrm{U}_{i+1}} > 0,\ i = 0, 1, \dots, L-1$.

Заметим, что в силу обобщенной формулы умножения вероятностей для однородной цепи Маркова первого порядка $\{\mathrm{X}_t\}$ справедлива следующая цепочка равенств:

$$\mathrm{P}\{\mathrm{X}_t = \mathrm{U}_0, \mathrm{X}_{t+1} = \mathrm{U}_1, \dots, \mathrm{X}_{t+L} = \mathrm{U}_L\} =$$
$$= \mathrm{P}\{\mathrm{X}_t = \mathrm{U}_0, \mathrm{X}_{t+1} = \mathrm{U}_1, \dots, \mathrm{X}_{t+L-1} = \mathrm{U}_{L-1}\} \times$$
$$\times \mathrm{P}\{\mathrm{X}_{t+L} = \mathrm{U}_L|\, \mathrm{X}_t = \mathrm{U}_0, \mathrm{X}_{t+1} = \mathrm{U}_1, \dots, \mathrm{X}_{t+L-1} = \mathrm{U}_{L-1}\} =$$
$$= \mathrm{P}\{\mathrm{X}_t = \mathrm{U}_0, \mathrm{X}_{t+1} = \mathrm{U}_1, \dots, \mathrm{X}_{t+L-1} = \mathrm{U}_{L-1}\} \times \mathrm{P}\{\mathrm{X}_{t+L} = \mathrm{U}_L|\, \mathrm{X}_{t+L-1} = \mathrm{U}_{L-1}\} =$$
$$= \mathrm{P}\{\mathrm{X}_t = \mathrm{U}_0, \mathrm{X}_{t+1} = \mathrm{U}_1, \dots, \mathrm{X}_{t+L-1} = \mathrm{U}_{L-1}\} \times p_{\mathrm{U}_{L-1},\mathrm{U}_L} = \dots =$$
$$= \mathrm{P}\{\mathrm{X}_t = \mathrm{U}_0\} \cdot p_{\mathrm{U}_0,\mathrm{U}_1} \cdot p_{\mathrm{U}_1,\mathrm{U}_2} \cdot \dots \cdot p_{\mathrm{U}_{L-1},\mathrm{U}_L}.$$

Тогда согласно уравнению Колмогорова – Чепмена и свойствам условной и совместной вероятностей справедлива цепочка неравенств

$$p^{(L)}_{\mathrm{U,W}} = \mathrm{P}\{\mathrm{X}_{t+L} = \mathrm{W}|\mathrm{X}_t = \mathrm{U}\} = \frac{\mathrm{P}\{\mathrm{X}_t = \mathrm{U}, \mathrm{X}_{t+L} = \mathrm{W}\}}{\mathrm{P}\{\mathrm{X}_t = \mathrm{U}\}} \geq$$
$$\geq \frac{\mathrm{P}\{\mathrm{X}_t = \mathrm{U}_0, \mathrm{X}_{t+1} = \mathrm{U}_1, \dots, \mathrm{X}_{t+L} = \mathrm{U}_L\}}{\mathrm{P}\{\mathrm{X}_t = \mathrm{U}_0\}} = p_{\mathrm{U}_0,\mathrm{U}_1} \cdot p_{\mathrm{U}_1,\mathrm{U}_2} \cdot \dots \cdot p_{\mathrm{U}_{L-1},\mathrm{U}_L} > 0.$$

Таким образом, получено противоречие. Следовательно, в матрице P^L нет нулевых элементов, т. е. $\{\mathrm{X}_t\}$ – регулярная цепь Маркова. ■

Обозначим через $H(\mathrm{U}, \mathrm{W}) = \sum_{i=1}^{L}(1 - \delta_{u_i,w_i})$ количество несовпадающих элементов векторов $\mathrm{U} = (u_1, u_2, \dots, u_L), \mathrm{W} = (w_1, w_2, \dots, w_L) \in \mathrm{V}^L$.

Следствие 1. *При выполнении условий* (3) *элементы матрицы P переходных вероятностей имеют следующий вид:*

$$p_{\mathrm{J,K}} = \begin{cases} \sum_{i=1}^{L}\gamma_i\lambda_{j_i}, \textit{ если } H(\mathrm{J}, \mathrm{K}) = 0, \textit{ т. е. } \mathrm{K} = \mathrm{J} = (j_1, j_2, \dots, j_L); \\ \gamma_i\lambda_s, \textit{ если } H(\mathrm{J}, \mathrm{K}) = 1, \textit{ т. е. } \mathrm{K} = \chi(\mathrm{J}, s, i), s \neq j_i; \\ 0, \textit{ если } H(\mathrm{J}, \mathrm{K}) \geq 2. \end{cases} \quad (5)$$

Доказательство непосредственно следует из формулы (4). ■

Теорема 2. *Пусть* $\{\xi_t\}$ *и* $\{\eta_t\}$ *– определенные на некотором вероятностном пространстве* $(\Omega, \mathrm{F}, \mathrm{P})$ *последовательности независимых в совокупности случайных величин с распределениями вероятностей* (3). *Тогда стационарное распределение вероятностей* α *цепи Маркова* $\{\mathrm{X}_t\}$ *существует и имеет мультипликативный вид*

$$\alpha_{\mathrm{K}} = \lambda_{k_1} \cdot \lambda_{k_2} \cdot \dots \cdot \lambda_{k_L},\ \mathrm{K} = (k_1, k_2, \dots, k_L) \in \mathrm{V}^L. \quad (6)$$

Доказательство. Формулировка теоремы корректна, так как если $\{\xi_t\}$ *и* $\{\eta_t\}$ – последовательности независимых в совокупности случайных величин, то согласно теореме 1 $\{\mathrm{X}_t\}$ – регулярная цепь Маркова, а для регулярных цепей Маркова всегда существует стационарное распределение, причем оно – единственное вероятностное решение уравнения $\alpha^T P = \alpha^T$[8]. Формула (6) описывает корректное распределение вероятностей, так как в силу (3) выполняется условие нормировки $\sum_{\mathrm{K}\in\mathrm{V}^L} \lambda_{k_1} \cdot \lambda_{k_2} \cdot \ldots \cdot \lambda_{k_L} \equiv 1$.

В данном случае уравнение $\alpha^T P = \alpha^T$ можно согласно следствию 1 представить в виде

$$\forall\, \mathrm{K} \in \mathrm{V}^L \;\; \alpha_{\mathrm{K}} = \sum_{\mathrm{J}} \alpha_{\mathrm{J}}\, p_{\mathrm{J,K}} = \alpha_{\mathrm{K}} \sum_{i=1}^{L} \gamma_i \lambda_{k_i} + \sum_{\mathrm{J}:\, \exists i:\, \mathrm{K}=\chi(\mathrm{J},k_i,i),\, j_i \neq k_i} \gamma_i \lambda_{k_i} \alpha_{\mathrm{J}} =$$
$$= \alpha_{\mathrm{K}} \textstyle\sum_{i=1}^{L} \gamma_i \lambda_{k_i} + \sum_{i=1}^{L} \left(\gamma_i \lambda_{k_i} \sum_{\mathrm{J}:\, \mathrm{K}=\chi(\mathrm{J},k_i,i),\, j_i \neq k_i} \alpha_{\mathrm{J}} \right), \tag{7}$$

где $\mathrm{K} = (k_1, k_2, \ldots, k_L),\ \mathrm{J} = (j_1, j_2, \ldots, j_L) \in \mathrm{V}^L$.

В силу формул (1) и (3) для распределения вероятностей α, определяемого формулой (6), справедливы равенства

$$\sum_{\mathrm{J}:\, \mathrm{K}=\chi(\mathrm{J},k_i,i),\, j_i \neq k_i} \alpha_{\mathrm{J}} = \sum_{\mathrm{J}:\, \mathrm{K}=\chi(\mathrm{J},k_i,i),\, j_i \neq k_i} \lambda_{j_1} \cdot \lambda_{j_2} \cdot \ldots \cdot \lambda_{j_L} = \sum_{s\in V,\, s\neq k_i} \lambda_{k_1} \cdot \ldots \cdot \lambda_{k_{i-1}} \cdot \lambda_s \cdot \lambda_{k_{i+1}} \ldots \cdot \lambda_{k_L} =$$
$$= \lambda_{k_1} \cdot \ldots \cdot \lambda_{k_{i-1}} \cdot \lambda_{k_{i+1}} \ldots \cdot \lambda_{k_L} \cdot \sum_{s\in V,\, s\neq k_i} \lambda_s = \lambda_{k_1} \cdot \ldots \cdot \lambda_{k_{i-1}} \cdot (1 - \lambda_{k_s}) \cdot \lambda_{k_{i+1}} \ldots \cdot \lambda_{k_L}.$$

Отсюда для любого α_{K}, определяемого формулой (6), получаем следующие равенства:

$$\alpha_{\mathrm{K}} \sum_{i=1}^{L} \gamma_i \lambda_{k_i} + \sum_{i=1}^{L} \left(\gamma_i \lambda_{k_i} \sum_{\mathrm{J}:\, \mathrm{K}=\chi(\mathrm{J},k_i,i),\, j_i \neq k_i} \alpha_{\mathrm{J}} \right) = \alpha_{\mathrm{K}} \sum_{i=1}^{L} \gamma_i \lambda_{k_i} + \sum_{i=1}^{L} \left(\gamma_i \lambda_{k_i} (1 - \lambda_{k_i}) \prod_{j=1, j\neq i}^{L} \lambda_{k_j} \right) =$$
$$= \alpha_{\mathrm{K}} \sum_{i=1}^{L} \gamma_i \lambda_{k_i} + \sum_{i=1}^{L} \gamma_i (1 - \lambda_{k_i}) \alpha_{\mathrm{K}} = \alpha_{\mathrm{K}} \sum_{i=1}^{L} \gamma_i = \alpha_{\mathrm{K}}.$$

Таким образом, если распределение вероятностей α определяется формулой (6), для него выполняются соотношения (7), а значит, α является решением уравнения $\alpha^T P = \alpha^T$. Так как данное уравнение имеет единственное вероятностное решение, то α совпадает со стационарным распределением вероятностей цепи Маркова $\{\mathrm{X}_t\}$. ■

Следствие 2. *Стационарное распределение вероятностей* (6) *состояний памяти* $\{\mathrm{X}_t\}$ *не зависит от распределения вероятностей* $\{\gamma_i\}$ *управляющей последовательности* $\{\eta_t\}$.

Доказательство непосредственно следует из формулы (6). ■

Следствие 2 показывает, что при моделировании достаточно продолжительной динамики генератора нет необходимости жестко контролировать вероятностные характеристики управляющей последовательности: даже если будут искажения в распределении вероятностей ее элементов, на частоту встречаемости состояний памяти это не повлияет.

Следствие 3. *Пусть выполняются условия теоремы* 2. *Стационарное распределение вероятностей* α *состояний памяти* $\{\mathrm{X}_t\}$ *является равномерным (т. е.* $\forall\, \mathrm{K} \in \mathrm{V}^L \;\; \alpha_{\mathrm{K}} = \frac{1}{|\mathrm{V}|^L}$*) тогда и только тогда, когда распределение вероятностей* $\{\lambda_i\}$ *элементов заполняющей последовательности* $\{\xi_t\}$ *равномерное (*$\lambda_i \equiv \frac{1}{|\mathrm{V}|}$*)*.

Доказательство. Согласно теореме 2 стационарное распределение вероятностей α цепи Маркова $\{\mathrm{X_t}\}$ существует и определяется формулой (6).

Пусть $\lambda_i = \frac{1}{|\mathrm{V}|}, i \in \mathrm{V}$. Тогда в силу (6) выполняется требуемое соотношение

$$\alpha_{\mathrm{K}} = \lambda_{k_1} \cdot \lambda_{k_2} \cdot \ldots \cdot \lambda_{k_L} = \frac{1}{|\mathrm{V}|^L} = \mathrm{const},\ \mathrm{K} = (k_1, k_2, \ldots, k_L) \in \mathrm{V}^L.$$

Пусть α – равномерное стационарное распределение вероятностей. Тогда выполняется условие (7), которое можно представить в следующем виде:

$$1 = \sum_{i=1}^{L} \gamma_i \lambda_{k_i} + \sum_{i=1}^{L} \left(\gamma_i \lambda_{k_i} \sum_{\mathrm{J}:\ \mathrm{K}=\chi(\mathrm{J},k_i,i),\ j_i \neq k_i} 1 \right) =$$

$$= \sum_{i=1}^{L} \gamma_i \lambda_{k_i} + \sum_{i=1}^{L} \left(\gamma_i \lambda_{k_i} (|\mathrm{V}| - 1) \right) = \sum_{i=1}^{L} \left(\gamma_i \lambda_{k_i} |\mathrm{V}| \right). \quad (8)$$

Условие (8) должно выполняться для любого $\mathrm{K} \in \mathrm{V}^L$. Выберем два вектора $\mathrm{U} = (u_1, u_2, \ldots, u_L)$, $\mathrm{W} = (w_1, w_2, \ldots, w_L) \in \mathrm{V}^L$, такие, что $\forall\, i \in \mathrm{A}\backslash\{s\}\ u_i = w_i,\ u_s \neq w_s$, т. е. отличающиеся в одном элементе под номером s. Тогда для данных векторов в силу (8) выполняется соотношение

$$\gamma_s \lambda_{u_s} |\mathrm{V}| = 1 - \sum_{i=1, i \neq s}^{L} \left(\gamma_i \lambda_{u_i} |\mathrm{V}| \right) = 1 - \sum_{i=1, i \neq s}^{L} \left(\gamma_i \lambda_{w_i} |\mathrm{V}| \right) = \gamma_s \lambda_{w_s} |\mathrm{V}|.$$

Из этого следует, что $\lambda_{u_s} = \lambda_{w_s}$. Так как u_s может принимать любое значение из множества $\mathrm{V}\backslash\{w_s\}$, получаем искомое требование

$$\lambda_i = \mathrm{const} = \frac{1}{|\mathrm{V}|},\ \ i \in \mathrm{V}. \blacksquare$$

Следствие 3 определяет, что отклонение стационарного распределения вероятностей последовательности $\{\mathrm{X}_t\}$ от равномерного свидетельствует о наличии искажений в распределении вероятностей последовательности $\{\xi_t\}$. Поэтому, если имеется возможность оценить стационарное распределение вероятностей $\{\mathrm{X}_t\}$, можно получить сведения о параметрах исходной последовательности $\{\xi_t\}$.

Введем следующие обозначения:

$u_{\mathrm{K}}^{(n)}$ – частота вектора $\mathrm{K} \in \mathrm{V}^L$ в последовательности состояний памяти $\{\mathrm{X}_t\}$, $t \in \{1, 2, \ldots, n\}$:

$$u_{\mathrm{K}}^{(n)} = \frac{1}{n} \sum_{i=1}^{n} \delta_{\mathrm{X}_i, \mathrm{K}};$$

f_{K} – время первого возврата в состояние, равное K:

$$f_{\mathrm{K}} = n \in \mathbb{N}: \mathrm{X}_n = \mathrm{X}_0 = \mathrm{K}, \forall i = \overline{1, n-1}\ \mathrm{X}_i \neq \mathrm{K}.$$

Следствие 4. *Пусть выполняются условия теоремы* 2. *Тогда верны следующие утверждения:*

1) вне зависимости от начального распределения математическое ожидание $u_{\mathrm{K}}^{(n)}$ *при* $n \to \infty$ *удовлетворяет предельному соотношению*

$$\mathbf{E}\left\{u_{\mathrm{K}}^{(n)}\right\} \to \lambda_{k_1} \cdot \lambda_{k_2} \cdot \ldots \cdot \lambda_{k_L},\ \mathrm{K} = (k_1, k_2, \ldots, k_L) \in \mathrm{V}^L; \quad (9)$$

2) математическое ожидание времени возврата в исходное состояние памяти K *определяется формулой*

$$\mathbf{E}\{f_{\mathrm{K}}\} = \frac{1}{\lambda_{k_1} \cdot \lambda_{k_2} \cdot \ldots \cdot \lambda_{k_L}}. \quad (10)$$

Доказательство. Согласно [8] для регулярных цепей Маркова выполняются соотношения

$$\mathbf{E}\left\{u_{\mathrm{K}}^{(n)}\right\} \xrightarrow[n \to \infty]{} \alpha_{\mathrm{K}},\quad \mathbf{E}\{f_{\mathrm{K}}\} = \frac{1}{\alpha_{\mathrm{K}}}.$$

Подставляя в данные соотношения формулу (6), получаем искомые утверждения. ■

Следствие 4 описывает частотные характеристики динамики памяти генератора. С их помощью можно оценить, как часто элемент выходной последовательности выбирался из заданного состояния памяти и имел соответствующее условное распределение вероятностей.

Теорема 3. *Пусть* $\{\xi_t\}$ *и* $\{\eta_t\}$ *– определенные на некотором вероятностном пространстве* $(\Omega, \mathrm{F}, \mathrm{P})$ *последовательности случайных величин с распределениями вероятностей* (3), *причем элементы* $\{\eta_t\}$ *независимы в совокупности, а* $\{\xi_t\}$ *представляет собой цепь Маркова первого порядка с матрицей переходных вероятностей* $Q = \left(q_{u,v}\right),\ u, v \in V$. *Тогда случайная последовательность состояний памяти* $\{\mathrm{X}_t\}$ *представляет собой однородную цепь Маркова второго порядка с матрицей переходных вероятностей* $P = (p_{\mathrm{I,J,K}})$*:*

$$p_{\mathrm{I,J,K}} = \mathrm{P}\{\mathrm{X}_{t+1} = \mathrm{K} | \mathrm{X}_t = \mathrm{J}, \mathrm{X}_{t-1} = \mathrm{I}\} = \\ = \frac{\sum_{i\in \mathrm{V}} \sum_{j\in \mathrm{A}} \left(\lambda_i \gamma_j \delta_{\mathrm{J},\chi(\mathrm{I},i,j)} \sum_{l\in \mathrm{V}} \sum_{s\in \mathrm{A}} q_{j,l}\gamma_s \delta_{\mathrm{K},\chi(\mathrm{J},l,s)}\right)}{\sum_{i\in \mathrm{V}} \sum_{j\in \mathrm{A}} \lambda_i \gamma_j \delta_{\mathrm{J},\chi(\mathrm{I},i,j)}},\ \mathrm{I,J,K} \in \mathrm{V}^L. \tag{11}$$

Доказательство. Определим функцию изменяющего элемента $v = \psi(\mathrm{Y}, \mathrm{X}, a) \in \mathrm{V}$, где $\mathrm{Y}, \mathrm{X} \in \mathrm{V}^L, a \in \mathrm{A}$, следующим образом:

$$v = \psi(\mathrm{Y}, \mathrm{X}, a) \Leftrightarrow \mathrm{Y} = \chi(\mathrm{X}, v, a).$$

В силу формулы (2) и представления $\{\xi_t\}$ как цепи Маркова первого порядка для последовательности $\{\mathrm{X}_t\}$ справедливы соотношения

$$\mathrm{P}\{\mathrm{X}_t = \mathrm{U}\} = \mathrm{P}\{\chi(\mathrm{X}_{t-1}, \xi_t, \eta_t) = \mathrm{U}\} = f(\mathrm{U}, \mathrm{X}_{t-1}, \eta_t, \xi_t) = \\ = g(\mathrm{U}, \mathrm{X}_{t-1}, \eta_t, \xi_{t-1}) = g\big(\mathrm{U}, \mathrm{X}_{t-1}, \eta_t, \psi(\mathrm{X}_{t-1}, \mathrm{X}_{t-2}, \eta_{t-1})\big) = \\ = h(\mathrm{U}, \mathrm{X}_{t-1}, \mathrm{X}_{t-2}, \eta_t, \eta_{t-1}), \tag{12}$$

где f, g, h – некоторые вероятностные функции.

В связи с тем что $\{\eta_t\}$ – последовательность независимых в совокупности одинаково распределенных случайных величин, из (12) следует обобщенное марковское свойство [8]:

$$\mathrm{P}\{\mathrm{X}_t = \mathrm{W}_t | \mathrm{X}_{t-1} = \mathrm{W}_{t-1}, \mathrm{X}_{t-2} = \mathrm{W}_{t-2}, \dots, \mathrm{X}_0 = \mathrm{W}_0\} = \mathrm{P}\{\mathrm{X}_t = \mathrm{W}_t | \mathrm{X}_{t-1} = \mathrm{W}_{t-1}, \mathrm{X}_{t-2} = \mathrm{W}_{t-2}\},$$

где $\mathrm{W}_0, \mathrm{W}_1, \dots, \mathrm{W}_t \in \mathrm{V}^L, t \geq 2$. Оно доказывает, что $\{\mathrm{X}_t\}$ представляет собой цепь Маркова второго порядка.

Для $\{\mathrm{X}_t\}$ на основании формулы (2), а также согласно формуле полной вероятности и в силу отсутствия попарной зависимости между элементами последовательностей $\{\xi_t\}$ и $\{\eta_t\}$ выполняется следующее соотношение:

$$\mathrm{P}\{\mathrm{X}_t = \mathrm{K} | \mathrm{X}_{t-1} = \mathrm{J}\} = \\ = \sum_{i\in \mathrm{V}} \sum_{j\in \mathrm{A}} \mathrm{P}\{\xi_t = i, \eta_t = j\} \mathrm{P}\{\mathrm{X}_t = \mathrm{K} | \mathrm{X}_{t-1} = \mathrm{J}, \xi_t = i, \eta_t = j\} = \\ = \sum_{i\in \mathrm{V}} \sum_{j\in \mathrm{A}} \lambda_i \gamma_j \mathrm{P}\{\mathrm{X}_t = \mathrm{K} | \mathrm{X}_t = \chi(\mathrm{X}_{t-1}, i, j)\} = \sum_{i\in \mathrm{V}} \sum_{j\in \mathrm{A}} \lambda_i \gamma_j \delta_{\mathrm{K},\chi(\mathrm{J},i,j)}. \tag{13}$$

Переходная вероятность на основании формул (2) и (13), а также согласно формулам полной и условной вероятностей и в силу свойств последовательностей $\{\xi_t\}$ и $\{\eta_t\}$ определяется выражением

$$\mathrm{P}\{\mathrm{X}_t = \mathrm{U} | \mathrm{X}_{t-1} = \mathrm{W}, \mathrm{X}_{t-2} = \mathrm{Z}\} = \frac{\mathrm{P}\{\mathrm{X}_t = \mathrm{U}, \mathrm{X}_{t-1} = \mathrm{W}, \mathrm{X}_{t-2} = \mathrm{Z}\}}{\mathrm{P}\{\mathrm{X}_{t-1} = \mathrm{W}, \mathrm{X}_{t-2} = \mathrm{Z}\}} = \\ = \frac{\mathrm{P}\{\mathrm{X}_t = \mathrm{U}, \mathrm{X}_{t-1} = \mathrm{W} | \mathrm{X}_{t-2} = \mathrm{Z}\}}{\mathrm{P}\{\mathrm{X}_{t-1} = \mathrm{W} | \mathrm{X}_{t-2} = \mathrm{Z}\}} =$$

$$= \frac{\sum_{j\in \mathrm{V}}\sum_{k\in \mathrm{A}}\lambda_j\cdot\gamma_k\cdot \mathrm{P}\{\mathrm{X}_t=\mathrm{U},\chi(\mathrm{Z},j,k)=\mathrm{W}\mid \mathrm{X}_{t-2}=\mathrm{Z},\ \xi_{t-1}=j,\ \eta_{t-1}=k\}}{\sum_{i\in \mathrm{V}}\sum_{j\in \mathrm{A}}\lambda_i\gamma_j\delta_{\mathrm{W},\chi(\mathrm{Z},i,j)}} =$$

$$= \frac{1}{\sum_{i\in \mathrm{V}}\sum_{j\in \mathrm{A}}\lambda_i\gamma_j\delta_{\mathrm{W},\chi(\mathrm{Z},i,j)}}\sum_{j\in \mathrm{V}}\sum_{k\in \mathrm{A}}\left(\lambda_j\gamma_k\delta_{\mathrm{W},\chi(\mathrm{Z},j,k)}\mathrm{P}\{\chi(\mathrm{W},\xi_t,\eta_t)=\mathrm{U}\mid \xi_{t-1}=j\}\right) =$$

$$= \frac{\sum_{j\in \mathrm{V}}\sum_{k\in \mathrm{A}}\left(\lambda_j\gamma_k\delta_{\mathrm{W},\chi(\mathrm{Z},j,k)}\sum_{l\in \mathrm{V}}\mathrm{P}\{\chi(\mathrm{W},\xi_t,\eta_t)=\mathrm{U}\mid \xi_t=l\}\,\mathrm{P}\{\xi_t=l\mid \xi_{t-1}=j\}\right)}{\sum_{i\in \mathrm{V}}\sum_{j\in \mathrm{A}}\lambda_i\gamma_j\delta_{\mathrm{W},\chi(\mathrm{Z},i,j)}} =$$

$$= \frac{1}{\sum_{i\in \mathrm{V}}\sum_{j\in \mathrm{A}}\lambda_i\gamma_j\delta_{\mathrm{W},\chi(\mathrm{Z},i,j)}}\sum_{j\in \mathrm{V}}\sum_{k\in \mathrm{A}}\left(\lambda_j\gamma_k\delta_{\mathrm{W},\chi(\mathrm{Z},j,k)}\sum_{l\in \mathrm{V}}\mathrm{P}\{\chi(\mathrm{W},l,\eta_t)=\mathrm{U}\}\cdot q_{j,l}\right) =$$

$$= \frac{1}{\sum_{i\in \mathrm{V}}\sum_{j\in \mathrm{A}}\lambda_i\gamma_j\delta_{\mathrm{W},\chi(\mathrm{Z},i,j)}}\sum_{j\in \mathrm{V}}\sum_{k\in \mathrm{A}}\left(\lambda_j\gamma_k\delta_{\mathrm{W},\chi(\mathrm{Z},j,k)}\sum_{l\in \mathrm{V}}\left(q_{j,l}\cdot\sum_{s\in \mathrm{A}}\gamma_s\mathrm{P}\{\chi(\mathrm{W},l,s)=\mathrm{U}\}\right)\right) =$$

$$= \frac{1}{\sum_{i\in \mathrm{V}}\sum_{j\in \mathrm{A}}\lambda_i\gamma_j\delta_{\mathrm{W},\chi(\mathrm{Z},i,j)}}\sum_{j\in \mathrm{V}}\sum_{k\in \mathrm{A}}\left(\lambda_j\gamma_k\delta_{\mathrm{W},\chi(\mathrm{Z},j,k)}\sum_{l\in \mathrm{V}}\sum_{s\in \mathrm{A}}q_{j,l}\gamma_s\delta_{\mathrm{U},\chi(\mathrm{W},l,s)}\right).$$

Так как $\mathrm{P}\{\mathrm{X}_t=\mathrm{U}|\mathrm{X}_{t-1}=\mathrm{W},\mathrm{X}_{t-2}=\mathrm{Z}\}$ не зависит от t, то $\{\mathrm{X}_t\}$ – однородная цепь Маркова второго порядка. ■

Следствие 5. *При выполнении условий теоремы* 3 *элементы матрицы переходных вероятностей* $P=(p_{\mathrm{I,J,K}})$ *имеют следующий вид:*

$$p_{\mathrm{I,J,K}}=\begin{cases}\frac{\sum_{s\in \mathrm{A}}(\gamma_s\lambda_{k_s}\sum_{r\in \mathrm{A}}(\gamma_r q_{k_s,k_r}))}{\sum_{s\in \mathrm{A}}\gamma_s\lambda_{k_s}}, \textit{ если } \mathrm{K}=\mathrm{J}=\mathrm{I};\\ \frac{\sum_{s\in \mathrm{A}}(\gamma_s\lambda_{j_s}\cdot\gamma_r q_{j_s,k_r})}{\sum_{s\in \mathrm{A}}\gamma_s\lambda_{j_s}}, \textit{ если } \mathrm{K}=\chi(\mathrm{J},k_r,r),k_r\neq j_r,\ \mathrm{J}=\mathrm{I};\\ \sum_{r\in \mathrm{A}}(\gamma_r q_{j_s,k_r}), \textit{ если } \mathrm{K}=\mathrm{J}=\chi(\mathrm{I},j_s,s),\ j_s\neq i_s;\\ \gamma_r\cdot q_{j_s,k_r}, \textit{ если } \mathrm{K}=\chi(\mathrm{J},k_r,r),k_r\neq j_r,\ \mathrm{J}=\chi(\mathrm{I},j_s,s),\ j_s\neq i_s;\\ 0, \textit{ если } H(\mathrm{I},\mathrm{J})\geq 2 \textit{ или } H(\mathrm{J},\mathrm{K})\geq 2,\end{cases} \tag{14}$$

где $\mathrm{K}=(k_1,k_2,\dots,k_L),\ \mathrm{J}=(j_1,j,\dots,j_L),\ \mathrm{I}=(i_1,i_2,\dots,i_L)$.

Доказательство непосредственно следует из формулы (11). ■

Следствие 6. *Если в условиях теоремы* 3 *одномерные распределения вероятностей* λ *и* γ *элементов последовательностей* $\{\xi_t\}$ *и* $\{\eta_t\}$ *равномерные, то элементы матрицы переходных вероятностей* $P=(p_{\mathrm{I,J,K}})$ *имеют следующий вид:*

$$p_{\mathrm{I,J,K}}=\begin{cases}\frac{1}{L^2}\sum_{s\in \mathrm{A}}\sum_{r\in \mathrm{A}}q_{k_s,k_r}, \textit{ если } \mathrm{K}=\mathrm{J}=\mathrm{I};\\ \frac{1}{L^2}\sum_{s\in \mathrm{A}}q_{j_s,k_r}, \textit{ если } \mathrm{K}=\chi(\mathrm{J},k_r,r),k_r\neq j_r,\ \mathrm{J}=\mathrm{I};\\ \frac{1}{L}\sum_{r\in \mathrm{A}}q_{j_s,k_r}, \textit{ если } \mathrm{K}=\mathrm{J}=\chi(\mathrm{I},j_s,s),\ j_s\neq i_s;\\ \frac{1}{L}q_{j_s,k_r}, \textit{ если } \mathrm{K}=\chi(\mathrm{J},k_r,r),k_r\neq j_r,\ \mathrm{J}=\chi(\mathrm{I},j_s,s),\ j_s\neq i_s;\\ 0, \textit{ если } H(\mathrm{I},\mathrm{J})\geq 2 \textit{ или } H(\mathrm{J},\mathrm{K})\geq 2.\end{cases} \tag{15}$$

Доказательство непосредственно следует из формулы (14). ■

Следствие 6 наглядно иллюстрирует связь между матрицей переходных вероятностей $P=(p_{\mathrm{I,J,K}})$ последовательности состояний памяти $\{\mathrm{X}_t\}$ и матрицей переходных вероятностей $Q=(q_{u,v})$ заполняющей последовательности $\{\xi_t\}$. Формула (15) также позволяет проводить

оценку параметров заполняющей последовательности $\{\xi_t\}$ по выборке из последовательности $\{X_t\}$.

3. Компьютерные эксперименты

Известно [8], что для регулярных цепей Маркова с матрицей переходных вероятностей P и стационарным распределением α выполняются следующие асимптотические соотношения:

$$\alpha_K = \lim_{n\to\infty} P_{J,K}^{(n)},$$

причем $\exists\, b, r\colon\ 0 < r < 1, P_{J,K}^{(n)} = \alpha_K + e_{J,K}^{(n)}$, где $\left|e_{J,K}^{(n)}\right| < b \cdot r^n$.

Другими словами, имеет место сходимость матрицы P^n к предельной матрице $M = E_L \alpha^T$ ($E_L \in V^L$ – вектор-столбец, все L элементов которого равны 1) при $n \to \infty$ с экспоненциальной скоростью. Поэтому стационарное распределение вероятностей с высокой точностью возможно вычислить путем возведения P в достаточно большую степень. В табл. 1 и 2 приведены результаты соответствующих компьютерных экспериментов. Для различной мощности алфавита V и размера памяти L определялись распределения вероятностей $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_{|V|}\}$ элементов заполняющей последовательности и $\gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_L\}$ управляющей последовательности. Затем на основании формулы (4) вычислялась матрица $P^{2^{10}}$, являющаяся весьма точной ($\left|e_{J,K}^{(n)}\right| < < O(r^{1024})$) аппроксимацией предельной матрицы M.

Таблица 1

Аппроксимация стационарного распределения α при $L = 2$ для различных λ и γ

γ	λ		
	{0,1, 0,3, 0,6}	{0,2, 0,8}	{0,5, 0,5}
{0,25, 0,75}	{0,01, 0,03, …, 0,36}	{0,04, 0,16, 0,16, 0,64}	$\alpha_K \equiv 0{,}25$
{0,5, 0,5}	{0,01, 0,03, …, 0,36}	{0,04, 0,16, 0,16, 0,64}	$\alpha_K \equiv 0{,}25$
{0,001, 0,999}	{0,01, 0,03, …, 0,36}	{0,04, 0,16, 0,16, 0,64}	$\alpha_K \equiv 0{,}25$

Таблица 2

Аппроксимация стационарного распределения α при $L = 3$ для различных λ и γ

γ	λ		
	{0,1, 0,3, 0,6}	{0,2, 0,8}	{0,5, 0,5}
{0,01, 0,01, 0,98}	{0,001, 0,003,…, 0,216}	{0,008, 0,032,…, 0,128, 0,512}	$\alpha_K \equiv 0{,}125$
{0,2, 0,5, 0,3}	{0,001, 0,003,…, 0,216}	{0,008, 0,032,…, 0,128, 0,512}	$\alpha_K \equiv 0{,}125$
{0,33, 0,34, 0,33}	{0,001, 0,003,…, 0,216}	{0,008, 0,032,…, 0,128, 0,512}	$\alpha_K \equiv 0{,}125$

Данные результаты подтверждают теоретическую формулу (6) для стационарного распределения и его независимость от распределения вероятностей управляющей последовательности.

Для оценивания среднего времени возврата в заданное состояние X моделировалось поведение генератора Макларена – Марсальи с размером таблицы, равным L. Последовательности $\{\xi_t\}$ и $\{\eta_t\}$ строились как последовательности независимых в совокупности случайных величин с помощью встроенного в C++ генератора rand(), при этом элементы $\{\eta_t\}$ имели равномерное распределение вероятностей, а $\{\xi_t\}$ – заданное распределение вероятностей λ. Имитировались n реализаций динамики памяти с начальным заполнением памяти $X_0 = K$ и высчитывалось среднее арифметическое времени возврата, являющееся несмещенной оценкой для $\mathbf{E}\{f_K\}$. Результаты для состояния $K = (0, 0, 0)$ при $L = 3$ указаны в табл. 3. Видно, что статистики по выборкам стремятся с увеличением n к теоретическому значению, вычисленному согласно формуле (10). Для других значений K и L получены аналогичные результаты экспериментов.

Таблица 3

Среднее арифметическое времени возврата в состояние $K = (0,0,0)$ при L = 3 для различных λ и n

λ	n = 1000	n =10 000	n =100 000	n =1 000 000	Теоретическое значение по формуле (10)
{0,501, 0,499}	7,994	8,037	8,040	7,942	7,952
{0,51, 0,49}	6,927	7,209	7,503	7,517	7,538
{0,55, 0,45}	5,580	5,989	5,946	6,002	6,0105
{0,6, 0,4}	5,125	4,577	4,624	4,625	4,630
{0,3, 0,7}	37,548	37,190	36,963	37,102	37,037
{0,99, 0,01}	1,021	1,0295	1,031	1,03	1,0306

Также были проведены эксперименты по определению частот встречаемости вектора K в последовательности состояний памяти $\{X_t\}$ длины n. Для этого моделировалось поведение генератора Макларена – Марсальи с размером таблицы, равным L. Последовательности $\{\xi_t\}$ и $\{\eta_t\}$ строились как последовательности независимых в совокупности случайных величин с помощью встроенного в C++ генератора rand(), при этом элементы $\{\eta_t\}$ имели равномерное распределение вероятностей, а $\{\xi_t\}$ – заданное распределение вероятностей λ. Проводились 100 экспериментов по оценке частоты встречаемости состояния K на выборке $\{X_t\}$ длиной n и высчитывалось среднее арифметическое. Результаты для состояния $K = (0,0,0)$ при $L = 3$ указаны в табл. 4. Видно, что выборочные частоты стремятся с увеличением n к теоретическому значению, вычисленному согласно формуле (9). Для других значений K и L получены аналогичные результаты экспериментов.

Таблица 4

Среднее арифметическое частот встречаемости состояния $K = (0,0,0)$ при L=3 для различных λ и n

λ	n =1000	n =10 000	n =100 000	n =1 000 000	Теоретическое значение по формуле (9)
{0,495, 0,505}	0,119790	0,121143	0,121439	0,121271	0,121287
{0,49, 0,51}	0,117020	0,117806	0,117335	0,117614	0,117649
{0,45, 0,55}	0,094080	0,090817	0,091141	0,091124	0,091125
{0,4, 0,6}	0,064480	0,064663	0,064030	0,063984	0,064000
{0,3, 0,7}	0,026510	0,027010	0,026933	0,027030	0,027000
{0,1, 0,9}	0,000890	0,001000	0,001009	0,001003	0,001000
{0,05, 0,95}	0,00010	0,000127	0,000121	0,000123	0,000125

Для исследования случая, когда $\{\xi_t\}$ является цепью Маркова первого порядка, проводились следующие эксперименты. Моделировалось поведение генератора Макларена – Марсальи с размером таблицы, равным L. Последовательность $\{\eta_t\}$ строилась как последовательность независимых в совокупности равномерно распределенных на $\{1,2,\dots,L\}$ случайных величин с помощью встроенного в C++ генератора rand(). Последовательность $\{\xi_t\}$ строилась как двоичная стационарная однородная цепь Маркова первого порядка с бистохастической матрицей переходных вероятностей $Q = \begin{pmatrix} 1-\epsilon & \epsilon \\ \epsilon & 1-\epsilon \end{pmatrix}$ ($\epsilon \in (0,1)$ – задаваемый уровень) и стационарным начальным рапределением вероятностей $\pi = (0{,}5,\ 0{,}5)$. Генерировалась выборка $\{X_t\}$ длиной n, по которой оценивалась матрица переходных вероятностей для цепи Маркова второго порядка. Результаты для выборок длиной $n = 10^4$ и $n = 10^7$ при $L = 2$ и уровне $\epsilon = 0{,}1$ приведены в табл. 5, в которой в столбце T указано соответствующее теоретическое значение, вычисленное согласно формуле (15).

Таблица 5

Выборочная матрица переходных вероятностей при $\boldsymbol{L}$ = 2 и $\boldsymbol{\epsilon = 0,1}$ для $\boldsymbol{n = 10^4}$ и $\boldsymbol{10^7}$

X_{t-2}	X_{t-1}	X_t											
		(0, 0)			(0, 1)			(1, 0)			(1, 1)		
		10^4	10^7	T	10^4	10^7	T	10^4	10^7	T	10^4	10^7	T
(0, 0)	(0, 0)	0,897	0,900	0,9	0,049	0,049	0,05	0,053	0,049	0,05			
(0, 1)	(0, 0)	0,896	0,899	0,9	0,052	0,050	0,05	0,052	0,050	0,05			
(1, 0)	(0, 0)	0,857	0,899	0,9	0,066	0,050	0,05	0,076	0,049	0,05			
(1, 1)	(0, 0)												
(0, 0)	(0, 1)	0,034	0,050	0,05	0,554	0,498	0,5				0,412	0,451	0,45
(0, 1)	(0, 1)	0,264	0,249	0,25	0,500	0,500	0,5				0,235	0,249	0,25
(1, 0)	(0, 1)												
(1, 1)	(0, 1)	0,460	0,451	0,45	0,490	0,498	0,5				0,049	0,049	0,05
(0, 0)	(1, 0)	0,041	0,050	0,05				0,452	0,501	0,5	0,507	0,448	0,45
(0, 1)	(1, 0)												
(1, 0)	(1, 0)	0,243	0,249	0,25				0,533	0,500	0,5	0,223	0,250	0,25
(1, 1)	(1, 0)	0,412	0,451	0,45				0,511	0,498	0,5	0,077	0,050	0,05
(0, 0)	(1, 1)												
(0, 1)	(1, 1)				0,056	0,050	0,05	0,051	0,049	0,5	0,892	0,899	0,9
(1, 0)	(1, 1)				0,039	0,051	0,05	0,026	0,050	0,5	0,934	0,898	0,9
(1, 1)	(1, 1)				0,047	0,049	0,05	0,053	0,049	0,05	0,898	0,900	0,9

Видно, что статистики стремятся с увеличением n к теоретическому значению, вычисленному согласно формуле (15). Для других значений L и ϵ получены аналогичные результаты экспериментов.

Полученные результаты иллюстрируют соответствие результатов компьютерного моделирования теоретическим результатам анализа динамики памяти генератора Макларена – Марсальи.

Заключение

В статье построена и исследуется вероятностная модель динамики памяти генераторов Макларена – Марсальи. Доказан критерий равномерности стационарного распределения вероятностей памяти, получена общая формула для предельного распределения. На основании данной формулы найдены некоторые вероятностные характеристики динамики памяти. Также найдены формулы, позволяющие проводить оценку параметров заполняющей последовательности по выборке из последовательности состояний памяти. Результаты компьютерных экспериментов подтверждают теоретические результаты.

Список литературы

1. Математические и компьютерные основы криптологии / Ю.С. Харин [и др.]. – Минск : Новое знание, 2003. – 382 с.

2. Основы криптографии / А.П. Алферов [и др.]. – М. : Гелиос АРВ, 2005. – 480 с.

3. eSTREAM: the ECRYPT Stream Cipher Project [Electronic resource]. – Mode of access : http://www.ecrypt.eu.org/stream/project.html. – Date of access : 10.04.2013.

4. MacLaren, M. Uniform Random Number Generators / M. MacLaren, G. Marsaglia // J. of the Association for Computing Machinery. – 1965. – Vol. 12(1). – P.83–89.

5. Кнут, Д. Искусство программирования. Получисленные алгоритмы = The Art of Computer Programming. Vol. 2. Seminumerical Algorithms. – 3-е изд. – М. : Вильямс, 2001. – Т. 2. – С. 45–47.

6. Starodubtzev, S.A. «Yamb», LAN Crypto Submission to the ECRYPT Stream Cipher Project / S.A. Starodubtzev, A.N. Lebedev, A.A. Volchkov [Electronic resource]. – Mode of access : http://www.ecrypt.eu.org/stream/yamb.html. – Date of access : 10.04.2013.

7. Бережной, И.Б. О периодичности и вероятностных свойствах генератора Макларена – Марсальи / И.Б. Бережной, Ю.С. Харин // Материалы XI Междунар. науч.-практ. конф. «Информационная безопасность–2010». – Таганрог, 2010. – Ч. 3. – С. 83–85.

8. Кемени, Дж.Дж. Конечные цепи Маркова / Дж.Дж Кемени, Дж.Л. Снелл. – М. : Наука, 1970. – 272 с.

Поступила 9.07.2013

НИИ прикладных проблем математики и информатики
Белорусского государственного университета,
Минск, пр. Независимости, 4
e-mail: berezhnoy@tut.by

I.B. Berezhnoy, Yu.S. Kharin

PROBABILISTIC MODEL OF MEMORY DYNAMICS OF MACLAREN – MARSAGLIA CRYPTOGRAFIC GENERATORS

A family of the Maclaren–Marsaglia cryptographic generators for pseudorandom sequences is considered. A probabilistic model of the memory dynamics for the Maclaren–Marsaglia generators is proposed and analyzed. The results of computer experiments are presented.