Math-Net.Ru
All Russian mathematical portal

V. A. Ivanov, On the influence of outer noises on the finite automata performance,
Tr. Diskr. Mat., 2000, Volume 3, 95–110

https://www.mathnet.ru/eng/tdm39

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
https://www.mathnet.ru/eng/agreement

Download details:
IP: 18.97.14.90
December 15, 2025, 17:05:19

Труды по дискретной математике
Том 3, с. 95–110
М.: ФИЗМАТЛИТ, 2000

О ВЛИЯНИИ ВНЕШНИХ ПОМЕХ НА РАБОТУ ДИСКРЕТНОГО АВТОМАТА

В. А. ИВАНОВ

Рассматривается класс перемешивающих автоматов, на вход и управление которых поступают независимые равновероятные бернуллиевские последовательности. Находятся точные формулы и асимптотические разложения для вероятностей искажений знаков выходной последовательности перемешивающего автомата в предположении, что входные и управляющие символы искажаются независимо с вероятностями, близкими к 1/2.

При разработке датчиков случайных чисел в качестве исходной последовательности часто используются линейные рекуррентные последовательности, вырабатываемые регистрами сдвига с обратной связью, или последовательности, вырабатываемые какими-либо другими устройствами, в частности, автоматами, реализующими смешанный конгруэнтный метод. Свойства таких последовательностей изучались в известных монографиях С. Голомба [1] и Д. Кнута [2], а также в журнальной литературе, см. например, обзор [3].

Для усложнения алгебраической структуры исходной последовательности, введения нелинейности и уменьшения корреляционных связей между символами можно использовать различные дискретные преобразователи, в частности, основанные на применении блока регистров сдвига для перемешивания символов входной последовательности по закону, задаваемому символами другой последовательности. К таким преобразователям с регистрами сдвига единичной длины относится "перемешивающая таблица", исследовавшаяся в работе [4]. Это преобразование можно представить в виде конечного автомата

$$P = \langle Z, X \times \Gamma, Y, \delta, \lambda \rangle, \qquad \text{где} \qquad Z = \{z = (z_1, \ldots, z_m)\}$$

— множество состояний автомата, $X \times \Gamma$ — множество входных состояний автомата (причем $X = \{x\}$ будем называть множеством входных символов, а $\Gamma = \{\gamma\} = \{1, \ldots, m\}$ — множеством управляющих символов), $Y = \{y\}$ — множество выходных символов,

© В. А. Иванов, 2000

$$\delta : Z \times X \times \Gamma \to Z, \qquad \delta(z, x, \gamma) = (\delta_1(z_1, x, \gamma), \ldots, \delta_m(z_m, x, \gamma)),$$

где

$$\delta_j(z_j, x, \gamma) = \begin{cases} z_j, & \text{если } \gamma \neq j, \\ x, & \text{если } \gamma = j, \ j = 1, \ldots, n, \end{cases}$$

— функция переходов автомата,

$$\lambda : Z \times X \times \Gamma \to Y, \qquad \lambda(z, x, \gamma) = z_\gamma$$

— функция выходов автомата. Будем считать, что координата z_j вектора состояний z размещена в ячейке с номером j накопителя длины m. Входящий в автомат в момент времени t символ x_t помещается в ячейку с номером γ_t, а находившийся в ней символ выходит из автомата. В работе [4] оцениваются корреляционные зависимости в выходной последовательности y_t, $t = 1, 2, \ldots$, при известных корреляционных зависимостях во входной последовательности x_t при условии, что значения управляющей последовательности γ_t независимы и равновероятны.

Естественным обобщением "перемешивающей таблицы", основанным на замене ячеек автомата регистрами сдвига, является перемешивающий автомат B_m, состоящий из m регистров сдвига длин $n(1), \ldots, n(m)$ соответственно. Далее остановимся на рассмотрении свойств автоматных преобразований двоичных входных последовательностей.

Определение. Перемешивающим автоматом

$$B_m = B_m(n(1), \ldots, n(m))$$

будем называть конечный автомат

$$B_m = \langle Z, X \times \Gamma, Y, \delta, \lambda \rangle,$$

где

$$Z = \big\{ z = (z_1, \ldots, z_m) \ : \ z_i = (z_{i1}, \ldots, z_{in(i)}), \ z_{ij} \in \mathbf{B} = \{0, 1\}, \\ i = 1, \ldots, m, \ j = 1, \ldots, n(i) \big\}$$

— множество состояний автомата B_m, $X \times \Gamma$ — множество входных состояний автомата B_m, являющееся прямым произведением множества входных символов

$$X = \{x\} = \mathbf{B}$$

и множества управляющих символов $\Gamma = \{\gamma\} = \{1, \ldots, m\}$,

$$Y = \{y\} = \mathbf{B}$$

— множество выходных символов автомата B_m,

$$\delta \ : \ Z \times X \times \Gamma \longrightarrow Z$$

— функция переходов автомата B_m, определяемая набором перестановок

$$a_i = (a_{i1}, \ldots, a_{in(i)}), \qquad b_i = (b_{i1}, \ldots, b_{in(i)}) \tag{1}$$

множеств $\{1, \ldots, n(i)\}$, $i = 1, \ldots, m$, по формулам

$$\delta(z, x, \gamma) = (\delta_1(z_1, x, \gamma), \ldots, \delta_m(z_m, x, \gamma)), \tag{2}$$

где

$$\delta_j(z_j, x, \gamma) = \begin{cases} (z_{ja_{j1}}, \ldots, z_{ja_{jn(j)}}), & \text{если } \gamma \neq j, \\ (x, z_{jb_{j2}}, \ldots, z_{jb_{jn(j)}}), & \text{если } \gamma = j, \ j = 1, \ldots, n, \end{cases}$$

$\lambda : Z \times X \times \Gamma \to Y$ — функция выходов автомата, равная

$$\lambda = \lambda(z, x, \gamma) = z_{\gamma b_{\gamma 1}}.$$

При исследовании вероятностных свойств автоматов B_m представляет интерес рассмотрение следующих вопросов.

1. Как изменяются распределения вероятностей и корреляционные связи между отдельными элементами случайной входной последовательности после ее прохождения через автомат?

2. Каковы вероятностные характеристики времени самонастройки (самовосстановления, отработки начального рассогласования) конечного автомата, в начальном состоянии которого произошел случайный сбой, после которого автомат работал без сбоев и на его вход поступала неискаженная последовательность?

3. Каково распределение вероятностей помех в выходной последовательности автомата при заданном распределении вероятностей помех в его входной последовательности?

Некоторые результаты, относящиеся к исследованию вероятностных характеристик времени самонастройки автомата, приведены в [9]. В настоящей работе остановимся на изучении третьего вопроса. Предположим, для простоты, что $m = 2^r$ и управляющий символ γ записан в виде

$$\gamma = (\gamma^{(1)}, \ldots, \gamma^{(r)}), \qquad \gamma^{(j)} \in \mathbf{B}, \qquad j = 1, \ldots, r.$$

Сначала оценим вероятности ошибок в символах выходной последовательности перемешивающего автомата $P = B_m(1, \ldots, 1)$ при заданном уровне искажений символов входной последовательности.

Будем считать, что начальное состояние z_0 автомата B_m под влиянием начального сбоя переходит в состояние z_0', символы входной последовательности x_t под влиянием аддитивных помех ω_t, $t = 1, 2, 3, \ldots$, переходят в искаженные символы $x_t' = x_t \oplus \omega_t$, а символы управляющей последовательности γ_t под влиянием аддитивных помех w_t переходят в искаженные символы $\gamma_t' = \gamma_t \oplus w_t$. Знак $\oplus$ в данном случае обозначает покомпонентное сложение соответствующих векторов по модулю 2.

В качестве модели для изучения распределений вероятностей ошибок в последовательности состояний или в выходной последовательности автомата A будем использовать пару автоматов (A, A^*), где автомат A^* функционально является точной копией исходного автомата A. Пусть сначала

реализуются независимые входные последовательности независимых случайных величин x_t и γ_t и независимые последовательности независимых помех ω_t и w_t, из которых составляются искаженные входная и управляющая последовательности

$$x'_t = x_t \oplus \omega_t \qquad \text{и} \qquad \gamma'_t = \gamma_t \oplus w_t, \qquad t = 1, 2, \ldots,$$

автомата A. В начальный момент времени автоматы A и A^* находятся в состояниях z'_0 и z_0. В результате переработки последовательностей x'_t, γ'_t на выходе автомата A реализуется выходная последовательность y'_t, а на выходе автомата A^* в результате переработки последовательностей x_t, γ_t — выходная последовательность y_t. Тогда ошибку в знаке y'_t выходной последовательности можно определить как индикатор события $\chi_t = I(y'_t \neq y_t)$, и исследование распределений вероятностей появления ошибок в выходной последовательности сводится к изучению вероятностных характеристик последовательности индикаторов χ_t, $t = 1, 2, \ldots$, при заданных вероятностных характеристиках входных и управляющих последовательностей и возникающих помех.

Следуя [9], автомат A^* будем называть идеальным, а автомат A — реальным, и при изучении работы реального автомата A с искаженным входом будем предполагать, что в основе математической модели для исследования работы реального автомата лежит гипотетический идеальный автомат, который работает без помех и сбоев.

Введем стандартные ограничения на распределения случайных величин $x_t, \gamma_t, \omega_t, w_t$, $t = 1, 2, \ldots$ Предположим, что они являются независимыми в совокупности случайными величинами, распределенными по следующим законам:

$$\mathbf{P}(x_t = 1) = \mathbf{P}(x_t = 0) = \frac{1}{2},$$

$$\mathbf{P}(\omega_t = \mu) = \frac{1}{2} + (-1)^\mu \delta_1 = \frac{1 + (-1)^\mu \delta_1^*}{2}, \qquad \mu = 0, 1, \qquad 0 \le \delta_1 \le \frac{1}{2}, \qquad \delta_1^* = 2\delta_1,$$

$$\mathbf{P}(\gamma_t = j) = 2^{-r}, \quad \mathbf{P}(w_t = j) = \rho_j = 2^{-r} + \delta_{2j}, \quad \mathbf{P}(\gamma'_t = j \mid \gamma_t = i) = p_{ij}.$$

Значения вероятностей p_{ij} определяются распределением случайной величины w_t.

Обозначим

$$\delta_{ij} = \mathbf{P}(z_{it} = z'_{jt}) - \frac{1}{2},$$

где z_{it} — содержимое i-й ячейки памяти идеального автомата в момент времени t, z'_{jt} — содержимое j-й ячейки памяти реального автомата в момент времени t, $\delta_y = \mathbf{P}(y_t = y'_t) - 1/2$ — преобладание для вероятности ошибки в выходной последовательности в момент времени t в стационарном режиме работы автомата.

Теорема 1. *Преобладания δ_{ij} и δ_y для вероятностей искажения координат состояний и выходных символов в стационарном режиме работы перемешивающего автомата $P = B_m(1, \ldots, 1)$ вычисляются по формулам*

$$\delta_{ij} = \frac{p_{ij}}{2 - p_{ij}}\,\delta_1, \qquad \delta_y = \sum_{i,j} \frac{p_{ij}^2}{2 - p_{ij}}\,\delta_1. \tag{3}$$

Доказательство. По формуле полной вероятности имеем

$$p_{ij} = P(z_i = z'_j) = \frac{1}{2} + \delta_{ij} = \mathbf{P}(\gamma = i,\, \gamma' = j)\left(\frac{1}{2} + \delta_1\right) +$$
$$+ \mathbf{P}(\gamma \neq i, \gamma' \neq j)\, p_{ij} + \frac{\mathbf{P}(\gamma = 1,\, \gamma' \neq j) + \mathbf{P}(\gamma \neq i,\, \gamma' = j)}{2}.$$

Замечая, что

$$\mathbf{P}(\gamma = i,\, \gamma' = j) = 2^{-r} p_{ij}, \qquad \mathbf{P}(\gamma = i,\, \gamma' \neq j) = 2^{-r}(1 - p_{ij}),$$

$$\mathbf{P}(\gamma' = j) = \mathbf{P}(\gamma + w = j) = \mathbf{P}(w = 1)\,\mathbf{P}(\gamma = j - 1) + \ldots$$
$$\ldots + \mathbf{P}(w = 2^r)\,\mathbf{P}(\gamma = j - 2^r) = 2^{-r},$$

$$\mathbf{P}(\gamma \neq i, \gamma' = j) = \mathbf{P}(\gamma' = j) - \mathbf{P}(\gamma = i, \gamma' = j) = 2^{-r}(1 - p_{ij}),$$

получаем линейное уравнение, из которого с учетом соотношения

$$\mathbf{P}(y = y') = \sum_{i,j} \mathbf{P}(\gamma = i, \gamma' = j)\left(\frac{1}{2} + \delta_{ij}\right)$$

следуют формулы (3).

Введем два класса перемешивающих автоматов с m накопителями: обозначим символом $B_m(n(1), \ldots, n(m))$ автомат с перестановками (1) вида

$$a_i = (1, 2, \ldots, n(i)) \qquad \text{и} \qquad b_i = (n(i), 1, \ldots, n(i) - 1),$$

преобразующими информацию z_i, содержащуюся в i-м ($i = 1, \ldots, m$); накопителе, обозначим символом $\underline{B}_m(n(1), \ldots, n(m))$ автомат с перестановками (1) вида

$$a_i = b_i = (n(i), 1, \ldots, n(i) - 1),$$

преобразующими информацию z_i, содержащуюся в i-м накопителе. Символом B_{mn} будем обозначать автомат $B_m(n(1), \ldots, n(m))$ с накопителями одинаковой длины $n(1) = \ldots = n(m) = n$.

В качестве следствия теоремы 1 приведем несколько формул для перемешивающих автоматов с двоичным управлением $B_2 = B_2(n(1), n(2))$. Наряду с положительными значениями $n(j)$ будем допускать выражения $n(j) = 0$; в таком автомате входной символ при управлении $\gamma = j$ проходит непосредственно на выход, минуя ячейки внутренней памяти. Полагая

$$\mathbf{P}(\gamma = \gamma') = \frac{1}{2} + \delta_2, \qquad \varepsilon = 2\delta_2, \qquad -1 \leq \varepsilon \leq 1,$$

получаем для определения преобладания δ_y перемешивающих автоматов $B_2(0, 1)$, $B_2(1, 1)$ и $B_2(0, 2)$ следующие формулы:

$$\delta_y(0,1) = \frac{1+\varepsilon}{3-\varepsilon}\,\delta_1, \qquad \delta_y(1,1) = \frac{3+5\varepsilon^2}{9-\varepsilon^2}\,\delta_1, \tag{4}$$

$$\delta_y(0,2) = \delta_y(2,0) = \frac{8+2\varepsilon-4\varepsilon^2+2\varepsilon^3}{(3-\varepsilon)^3}\,\delta_1. \tag{5}$$

Для автомата $B_2 = B_2(2,2)$ справедлива формула

$$\delta_y(2,2) = \frac{135+315\varepsilon^2+53\varepsilon^4+9\varepsilon^6}{(9-\varepsilon^2)^3}\,\delta_1.$$

Заметим, что при решении задач построения помехоустойчивых автоматов основное внимание уделяется изучению случаев, когда помехи появляются с малыми вероятностями (т.е. $\delta_i \approx 1/2$). Однако в задачах изучения датчиков случайных чисел определенный интерес представляет исследование вероятностей появления помех на выходе конечного автомата в условиях наличия сильного входного шума ($\delta_i \approx 0$).

Из формул (4) видно, что при $\delta_2 \to 0$ вероятность появления ошибки в символе выходной последовательности больше, чем вероятность появления ошибки во входной последовательности. Действительно, при $\delta_2 = 0$ справедливы равенства $\delta_y(0,1) = \delta_y(1,1) = \delta_1/3$.

В связи с этим естественно поставить вопрос о построении такого автомата D, который вырабатывал бы выходную последовательность $y'_t(D)$, более близкую к выходной последовательности y_t, вырабатываемой идеальным автоматом $B_2^*(n(1),n(2))$, чем выходная последовательность $y'_t = y'_t(B_2(n(1),n(2)))$, вырабатываемая автоматом $B_2(n(1),n(2))$, при подаче на его вход искаженной входной последовательности x'_t.

Не углубляясь в вопросы оптимизации, приведем пример простого по устройству автомата, применение которого для восстановления выходной последовательности y_t по искаженным входной и управляющей последовательностям x'_t и γ'_t соответственно дает при малых значениях δ_2 больший эффект, чем использование исходного автомата.

Используем в качестве приближающего автомата обычный регистр сдвига $D = R_k$, осуществляющий задержку знака входной последовательности на k тактов. Тогда выходной знак, вырабатываемый автоматом R_k в момент времени t, будет иметь вид $y'_t = y'_t(R_k) = x'_{t-k}$, и выходной знак y_t автомата $B_2^*(0,1)$ будет совпадать с выходным знаком $y'_t(R_0)$ автомата R_0 с вероятностью $(1+\delta_1)/2$, с выходным знаком $y'_t(R_1)$ автомата R_1 с вероятностью $(1+\delta_1)/2$, с выходным знаком $y'_t(R_2)$ автомата R_2 с вероятностью $(2+\delta_1)/4$, и т.д. Выходной знак y_t автомата $B_2^*(1,1)$ будет совпадать с выходным знаком $y'_t(R_k)$ автомата R_k с вероятностью $(1+\delta_1)/2$ при $k=1$ и далее с ростом величины k преобладание будет монотонно убывать. Из (4) следует, что при $\delta_2 < \delta_{\text{гр}} = 1/6$ автомат $D = R_1$ вырабатывает по искаженным входным последовательностям более точное приближение последовательности y_t, вырабатываемой идеальным автоматом $B_2^*(0,1)$, чем автомат $B_2(0,1)$, а при $\delta_2 > \delta_{\text{гр}}$ автомат $B_2(0,1)$ дает более точное приближение, чем автомат $D_1 = R_1$. Аналогичные рассуждения убеждают нас в том, что для перемешивающего автомата $B_2(1,1)$ граничное значение равно $\delta_{\text{гр}} = (3/44)^{1/2} \approx 0,261$.

Следует заметить, что не для всех перемешивающих автоматов задача решения системы алгебраических уравнений относительно стационарных вероятностей является трудоемкой. Например, метод решения алгебраических уравнений для стационарных вероятностей, относящихся к анализу перемешивающего автомата $\underline{B}_2(n,n)$ легко приводит к конечному результату для накопителей произвольной длины n.

Действительно, полагая

$$\mathbf{P}\left(z_{ki}(t) = z'_{ki}(t)\right) = \frac{1+\delta_{ki}}{2}, \qquad k = 1,2, \qquad i = 1,\ldots,n,$$

и применяя формулу полной вероятности, получаем для стационарного режима работы автомата соотношения

$$\begin{aligned}
&\mathbf{P}\left(y_{t+1} = y'_{t+1}\right) = \\
&= \mathbf{P}\left(\gamma_t = \gamma'_t = 0\right)\mathbf{P}\left(z_{1n}(t) = z'_{1n}(t)\right) + \mathbf{P}\left(\gamma_t = \gamma'_t = 1\right)\mathbf{P}\left(z_{2n}(t) = z'_{2n}(t)\right) + \qquad (6)\\
&\quad + \mathbf{P}\left(\gamma_t = 0, \gamma'_t = 1\right)\mathbf{P}\left(z_{1n}(t) = z'_{2n}(t)\right) + \mathbf{P}\left(\gamma_t = 1, \gamma'_t = 0\right)\mathbf{P}\left(z'_{1n}(t) = z_{2n}(t)\right).
\end{aligned}$$

Далее замечаем, что

$$\begin{aligned}
&\mathbf{P}\left(z_{1n}(t) = z'_{1n}(t)\right) = \mathbf{P}\left(z_{1,n-1}(t-1) = z'_{1,n-1}(t-1)\right) = \ldots \\
&\qquad\qquad \ldots = \mathbf{P}\left(z_{11}(t-n-1) = z'_{11}(t-n-1)\right)
\end{aligned}$$

и

$$\begin{aligned}
&\mathbf{P}\left(z_{1n}(t+1) = z'_{1n}(t+1)\right) = \mathbf{P}\left(\gamma_t = \gamma'_t = 0\right)\mathbf{P}\left(x_t = x'_t\right) + \\
&\quad + \mathbf{P}\left(\gamma_t = \gamma'_t = 1\right)\mathbf{P}\left(z_{2n}(t) = z'_{2n}(t)\right) + \mathbf{P}\left(\gamma_t \neq \gamma'_t\right)\mathbf{P}\left(z_{1n}(t+1) = z'_{1n}(t+1)\right).
\end{aligned}$$

Учитывая, что для стационарного режима работы автомата выполняются соотношения

$$\delta_{11} = \delta_{12} = \ldots = \delta_{1n} \qquad \text{и} \qquad \delta_{21} = \delta_{22} = \ldots = \delta_{2n},$$

и принимая во внимание обозначение $\varepsilon = 2\delta_2$, получаем преобладания для вероятностей $\mathbf{P}\left(z_{1n}(t) = z'_{1n}(t)\right)$ и $\mathbf{P}\left(z_{2n}(t) = z'_{2n}(t)\right)$:

$$\delta_{1j} = \frac{p(1+\varepsilon)}{1+p-q\varepsilon}\delta_1, \qquad \delta_{2j} = \frac{q(1+\varepsilon)}{1+q-p\varepsilon}\delta_1, \qquad j = 1,\ldots,n. \qquad (7)$$

Аналогично с учетом равенств

$$\begin{aligned}
&\mathbf{P}\left(z_{1n}(t) = z'_{2n}(t)\right) = \mathbf{P}\left(z_{1,n-1}(t-1) = z'_{2,n-1}(t-1)\right) = \ldots \\
&\qquad\qquad \ldots = \mathbf{P}\left(z_{11}(t-n-1) = z'_{21}(t-n-1)\right)
\end{aligned}$$

и

$$\mathbf{P}\left(z_{1n}(t+1)=z'_{2n}(t+1)\right)=\mathbf{P}\left(\gamma_t=0,\gamma'_t=1\right)\mathbf{P}\left(x_t=x'_t\right)+$$

$$+\mathbf{P}\left(\gamma_t=1,\gamma'_t=0\right)\mathbf{P}\left(z_{1n}(t)=z'_{2n}(t)\right)+\mathbf{P}\left(\gamma_t=\gamma'_t\right)\mathbf{P}\left(z_{1n}(t+1)=z'_{2n}(t+1)\right)$$

получаем:

$$\begin{aligned}\mathbf{P}\left(z_{1n}(t)=z'_{2n}(t)\right)&=1+\frac{p(1-\varepsilon)}{1+p+q\varepsilon}\,\delta_1,\\ \mathbf{P}\left(z'_{1n}(t)=z_{2n}(t)\right)&=1+\frac{q(1-\varepsilon)}{1+q+p\varepsilon}\,\delta_1.\end{aligned}\tag{8}$$

Из (6), (7) и (8) следует справедливость соотношений

$$\delta_y=\left[\frac{p^2(1+p+2\varepsilon^2+q\varepsilon^2)}{(1+p)^2-q^2\varepsilon^2}+\frac{q^2(1+q+2\varepsilon^2+p\varepsilon^2)}{(1+q)^2-p^2\varepsilon^2}\right]\delta_1.$$

В случае $p=q=1/2$ вид выражения для δ_y аналогичен (4): $\delta_y=(3+5\varepsilon^2)\,\delta_1/(9-\varepsilon^2)$. Для $B_2(0,n)$ получаем $\delta_y=p(1+\varepsilon)\,\delta_1/(1+p-q\varepsilon)$, а при $p=q=1/2$ это соотношение переходит в равенство $\delta_y=(1+\varepsilon)\times\times\delta_1/(3-\varepsilon)$.

Практическая реализация описанного выше подхода к нахождению вероятностей ошибок, появляющихся в последовательностях состояний и в выходных последовательностях, основанного на решении алгебраических уравнений, является трудно решаемой задачей для автоматов $B_2(n,n)$ с накопителями даже не слишком больших длин. Поэтому возникает потребность в разработке методов асимптотического анализа различных характеристик предельного распределения вероятностей появления выходных помех при неограниченном росте длин накопителей.

Прежде всего выведем точные формулы для вероятностей появления помех в выходной последовательности.

Рассмотрим множество B_{mn} перемешивающих автоматов с накопителями одинаковой длины $n(1)=\ldots=n(m)=n$ и с перестановками вида

$$a_i=(1,2,\ldots,n(i))\qquad\text{и}\qquad b_i=(n(i),1,\ldots,n(i)-1).$$

Введем вероятности

$$P_{ij}(T)=\mathbf{P}\left(\gamma_1=\gamma_T=i,\ \sum_{k=1}^{T-1}I_i(\gamma_k)=n-1,\ \gamma'_1=\gamma'_T=j,\ \sum_{k=1}^{T-1}I_j(\gamma'_k)=n-1\right),$$

где $I_i(\gamma)$ — индикаторная функция, принимающая значение 1, если $\gamma=i$, и значение 0, если $\gamma\neq i$,

$$\rho_T=\sum_{i,j}P_{ij}(T),\qquad \rho=\rho_{n+1}+\rho_{n+2}+\ldots$$

Лемма 1. *Для перемешивающих автоматов B_{mn} справедлива формула*

$$\lim_{T\to\infty}\mathbf{P}\left(y_T=y'_T\right)=\frac{1+\rho\delta_1}{2}.\tag{9}$$

Доказательство. Прежде всего заметим, что величина ρ является вероятностью события, состоящего в том, что входные символы идеального и реального автоматов, поступившие в один и тот же момент времени, одновременно попадут на выходы этих автоматов. При выполнении этого события условная вероятность совпадения случайных величин y_T и y'_T равна $(1/2)+\delta_1$, при условии выполнения противоположного события эта вероятность равна $1/2$. Из сказанного следует, что

$$\mathbf{P}\left(y_T = y'_T\right) = \rho_{n+1} + \ldots + \rho_T$$

и, следовательно, справедливо соотношение (9).

Перейдем теперь к исследованию стационарных вероятностных характеристик произвольного перемешивающего автомата $B_2(n,n)$ с двоичным входом, выходом и управлением. Исследуем асимптотику вероятности появления ошибки на выходе автомата при условии, что длины его накопителей неограниченно увеличиваются ($n \to \infty$). Как и прежде, предполагаем, что выполняются соотношения

$$p_{\text{вх}} = \mathbf{P}\left(x_t \neq x'_t\right) = \mathbf{P}\left(\omega_t = 1\right) = \frac{1}{2} - \delta_1,$$

$$p_{\text{упр}} = \mathbf{P}\left(\gamma_t \neq \gamma'_t\right) = \mathbf{P}\left(w_t = 1\right) = \frac{1}{2} - \delta_2, \qquad p_{\text{вых}} = \mathbf{P}\left(y_t \neq y'_t\right) = \frac{1}{2} - \delta_y.$$

Теорема 2. *Пусть задан перемешивающий автомат $B_2(n,n)$, на вход и управление которого поступают независимые между собой равновероятные бернуллиевские последовательности. Предположим, что на символы входной и управляющей последовательностей аддитивно и независимо воздействуют бинарные помехи с вероятностями $p_{\text{вх}} = 1/2 - \delta_1$ и $p_{\text{упр}} = 1/2 - \delta_2$ соответственно. Пусть $p_{\text{вых}} = 1/2 - \delta_y$ — вероятность помехи в символах выходной последовательности для стационарного режима работы перемешивающего автомата $B_2(n,n)$. Тогда*

$$\delta_y = \left(c_0(n) + c_1(n)(\delta_2)^2 + \ldots\right)\delta_1, \tag{10}$$

а коэффициенты в представлении (10) при $n \to \infty$ имеют асимптотические разложения

$$c_0(n) = \frac{1}{2(2\pi n)^{1/2}}\left(1 + \frac{13}{32n} + o\left(n^{-2}\right)\right),$$

$$c_1(n) = \frac{1}{4(2\pi n)^{1/2}}\left(19 + \frac{339}{32n} + o\left(n^{-2}\right)\right).$$

Доказательству теоремы предпошлем две леммы. Введем обозначения

$$a(t,k,\delta) = \left(\frac{1}{2}+\delta\right)^{t-2k+1}\left(\frac{1}{2}-\delta\right)^{2k} = a_0(t,k) + a_1(t,k)\,\delta + a_2(t,k)\,\delta^2 + \ldots, \tag{11}$$

$$b(t,k,\delta) = \sum_{k=0}^{\min(n-1,t-n+1)} \binom{n-1}{k}\binom{t-n+1}{k} a(t,k,\delta), \tag{12}$$

$$v(n,p,\delta)=\sum_{t=n-1}^{\infty}\binom{t}{n-1}p^n q^{t-n+1}b(t,k,\delta). \tag{13}$$

Лемма 2. *Пусть*

$$\mathbf{P}(y_t=y'_t)=\frac{1}{2}+\delta_y,\quad \mathbf{P}(\gamma_t=1)=p,\quad \mathbf{P}(\gamma_t=0)=q,\quad p+q=1,$$

$$\mathbf{P}(x_t=0)=\mathbf{P}(x'_t=1)=\frac{1}{2}.$$

Тогда

$$\begin{aligned}\delta_y=\left(\frac{1}{2}+\delta_2\right)\left[pv(n,p,\delta_2)+qv(n,q,\delta_2)\right]\delta_1+\\ +\left(\frac{1}{2}-\delta_2\right)\left[pv(n,p,-\delta_2)+qv(n,q,-\delta_2)\right]\delta_1.\end{aligned} \tag{14}$$

Доказательство. Обозначим z_{int}, $i=1,2$, значение n-й координаты z_{in} вектора состояния автомата в момент времени $t=1,2,\ldots$ Применяя формулу полной вероятности для стационарного режима работы автомата, получаем соотношения

$$\begin{aligned}&\mathbf{P}(y_t=y'_t)=\\ &=\mathbf{P}(\gamma_t=\gamma'_t=0)\,\mathbf{P}\big(z_{1nt}=z'_{1nt}\big)+\mathbf{P}(\gamma_t=\gamma'_t=1)\,\mathbf{P}\big(z_{2nt}=z'_{2nt}\big)+\\ &+\mathbf{P}(\gamma_t=0,\gamma'_t=1)\,\mathbf{P}\big(z_{1nt}=z'_{2nt}\big)+\mathbf{P}(\gamma_t=1,\gamma'_t=0)\,\mathbf{P}\big(z_{2nt}=z'_{1nt}\big).\end{aligned}$$

Найдем $\mathbf{P}\big(z_{int}=z'_{jnt}\big)$ $i,j=1,2$. Учитывая (13), получаем

$$\mathbf{P}\big(z_{1nt}=z'_{1nt}\big)=\frac{1}{2}+v\,(n,p,\delta_2)\,\delta_1,\qquad \mathbf{P}\big(z_{2nt}=z'_{2nt}\big)=\frac{1}{2}+v\,(n,q,-\delta_2)\,\delta_1,$$

$$\mathbf{P}\big(z_{1nt}=z'_{2nt}\big)=\frac{1}{2}+v\,(n,p,-\delta_2)\,\delta_1,\qquad \mathbf{P}\big(z_{2nt}=z'_{1nt}\big)=\frac{1}{2}+v\,(n,q,\delta_2)\,\delta_1,$$

что доказывает (14).

Изучим более подробно формулу (14) при $p=q=1/2$. Прежде всего заметим, что в разложении

$$\frac{\delta_y}{\delta_1}=\psi(n,\delta_2)=\psi_0(n)+\psi_1(n)\,\delta_2+\psi_2(n)\,\delta_2^2+\ldots$$

коэффициенты, стоящие при нечетных степенях переменной δ_2, равны нулю, а при четных степенях имеют вид

$$\psi_{2m}(n)=\sum_{t=n-1}^{\infty}\binom{n-1}{t}\sum_{k=0}^{\min(n-1,t-n+1)}\binom{n}{k}\binom{t-n+1}{k}\lambda(n,k),$$

где

$$\lambda(n,k) = 2\lambda_{2m-1}(n,k) + \lambda_m(n,k), \qquad \lambda_{-1}(n,k) = 0,$$

$$\lambda_m(n,k) = 2^{m-t-1}\sum_{j=0}^{m}(-1)^j\binom{2k}{j}\binom{t-2k+1}{k}, \qquad m = 1,2,\ldots$$

Лемма 3. *Для коэффициентов A_{in} степенных рядов*

$$v\left(n+1,\frac{1}{2},\delta\right) = A_{0n} + A_{1n}\delta + A_{2n}\delta^2 + \ldots$$

при $n \to \infty$ имеют место асимптотические соотношения

$$\begin{aligned} A_{0n} &= \frac{1}{2(2\pi)^{1/2}}\,n^{-1/2} - \frac{3}{64(2\pi)^{1/2}}\,n^{-3/2} + O\left(n^{-2}\right),\\ A_{1n} &= \frac{3}{2(2\pi)^{1/2}}\,n^{-1/2} - \frac{3}{64(2\pi)^{1/2}}\,n^{-3/2} + O\left(n^{-2}\right),\\ A_{2n} &= \frac{7}{4(2\pi)^{1/2}}\,n^{-1/2} + \frac{47}{128(2\pi)^{1/2}}\,n^{-3/2} + O\left(n^{-2}\right). \end{aligned} \tag{15}$$

Доказательство. Сначала докажем утверждение, касающееся коэффициента A_{0n}, который может быть представлен в виде

$$A_{0n} = \sum_{t=n}^{\infty}\binom{t}{n}\left(\frac{1}{2}\right)^n \sum_{k=0}^{\min(n,t-n)}\binom{n}{k}\binom{t-n}{k}a_0(n,k).$$

С учетом соотношений

$$a_0(n,k) = \left(\frac{1}{2}\right)^{t+1}, \qquad \sum_{k=0}^{\min(n,t-n)}\binom{n}{k}\binom{t-n}{k} = \binom{t}{n}$$

и

$$\sum_{k=0}^{\min(n,t-n)} k(k-1)\ldots(k-i)\binom{n}{k}\binom{t-n}{k} = \frac{n\ldots(n-i)(t-n)\ldots(t-n-i)}{t(t-1)\ldots(t-i)}\binom{t}{n}$$

получаем для A_{0n} выражение

$$A_{0n} = \sum_{t=n}^{\infty}\binom{t}{n}^2\left(\frac{1}{2}\right)^{2t+2}. \tag{16}$$

Из теоремы о больших уклонениях (см. [7]) следует, что

$$A_{0n} = \sum_{t\,:\,|t-2n|<2\sqrt{n}\,\ln n}\binom{t}{n}^2\left(\frac{1}{2}\right)^{2t+2} + o\left(n^{-\beta}\right), \tag{17}$$

где β — произвольное положительное число.

Производя в правой части соотношения (17) замену переменных $t = n(x+2)$ и применяя формулу Стирлинга, получаем

$$A_{0n} = \frac{1}{8\pi n} \sum_{|x|\le\varepsilon} g(x) \exp\left\{2nh_1(x) - \frac{h_2(x)}{6n}\right\} \exp\left\{O\left(\frac{x+2}{n^3}\right)\right\} + O\left(\frac{1}{n^\beta}\right), \qquad (18)$$

где

$$h_1(x) = (x+2)\ln(x+2) - (x+1)\ln(x+1) - (x+2)\ln 2,$$

$$h_2(x) = 1 + (x+1)^{-1} - (x+2)^{-1}, \qquad g(x) = (x+2)(x+1)^{-1},$$

$\varepsilon = \mathrm{const}$, $0 < \varepsilon < 1$. Суммирование в (18) ведется по действительным числам вида $x = x_t = (t/n) - 2$, где t — натуральные числа из интервала $(2n - n^{1/2}\ln n,\ 2n + n^{1/2}\ln n)$.

Обозначим

$$f(x,n) = g(x)\exp\left\{2nh_1(x) - (6n)^{-1}h_2(x)\right\}.$$

С помощью формулы Эйлера–Маклорена (см. [8]) оценим сумму

$$S_0(n) = \frac{1}{8\pi n} \sum_{|x|<\varepsilon} f(x,n) =$$

$$= \frac{1}{8\pi}\left\{\int_{-\varepsilon}^{\varepsilon} f(x,n)\,dx + \frac{1}{n}A_1\left[f(\varepsilon,n) - f(-\varepsilon,n)\right] + \frac{1}{n^2}A_2\left[f^{(1)}(\varepsilon,n) - f^{(1)}(-\varepsilon,n)\right] + \ldots\right.$$

$$\left.\ldots + \frac{1}{n^{m-1}}A_{m-1}\left[f^{(m-2)}(\varepsilon,n) - f^{(m-2)}(-\varepsilon,n)\right] + R_m\right\},$$

где

$$R_m = -\sum_{|x|<\varepsilon} \int_0^{n^{-1}} f^{(m)}\left(n, x + n^{-1} - z\right)\varphi_m(z)\,dz, \qquad m \ge 2,$$

$$\varphi_m(z) = \frac{z^m}{m!} + \frac{A_1 z^{m-1}}{n(m-1)!} + \ldots + \frac{A_{m-1}z}{n^{m-1}},$$

$A_1 = -1/2$, $A_{2p-1} = 0$ для $p > 1$, $A_{2p} = (-1)^{p-1}B_p/(2p)!$, B_p — p-е число Бернулли.

Заметим, что сумма $S_0(n)$ приближается интегралом с точностью $O(|R_m|)$, поскольку в рассматриваемом случае величины $f^{(k)}(\varepsilon,n)$ и $f^{(k)}(-\varepsilon,n)$ имеют порядок $O(n^{-\beta})$, где β — произвольное положительное число.

Оценим R_m для $m = 2k$, $k \ge 1$:

$$|R_{2k}| \le \sum_{|x|<\varepsilon} \left|\int_0^{n^{-1}} f^{(2k)}\left(n, x + n^{-1} - z\right)\varphi_{2k}(z)\,dz\right|; \qquad (19)$$

так как функция $\varphi_{2k}(z)$ не меняет знак на отрезке $[0, 1/n]$, то получаем из (16) по теореме о среднем

$$|R_{2k}| \le \sum_{|x|<\varepsilon} \left| f^{(2k)}(n, c(x)) \int\limits_0^{n^{-1}} \varphi_{2k}(z)\, dz \right|,$$

где $c(x)$ — точка, принадлежащая отрезку $[x, x+1/n]$. Поэтому справедлива оценка

$$|R_{2k}| \le \frac{A}{n^{2k+1}} \sum_{|x|<\varepsilon} \left| f^{(2k)}(n, c(x)) \right|, \qquad A = \text{const}. \tag{20}$$

В нашем случае, выбрав значение параметра $k = 2$ и учитывая, что

$$\left| f^{(n)}(n, c(x)) \right| \le cn^2,$$

можно ограничиться лишь $2n^{1/2} \ln n$ слагаемыми. Далее из (16) получаем для $k = 2$ оценку

$$|R_4| = O\left(n^{-5/2} \ln n\right) = o\left(n^{-2}\right).$$

Интеграл

$$I_0 = \frac{1}{8\pi} \int\limits_{-\varepsilon}^{\varepsilon} g(x) \exp\left\{2nh_1(x) - \frac{1}{6n} h_2(x)\right\} dx =$$

$$= \frac{1}{8\pi} \int\limits_{-\varepsilon}^{\varepsilon} g(x) \left(1 - \frac{1}{6n} h_2(x) + O\left(n^{-2}\right)\right) \exp\{2nh_1(x)\}\, dx$$

представляется в виде суммы нескольких интегралов, асимптотическое разложение каждого из которых можно найти с помощью формулы Лапласа (см. [8])

$$\int\limits_{-\infty}^{\infty} \psi(x) \exp\{nh(x)\}\, dx = \sum_{\nu=0}^{\infty} d_\nu n^{-\nu-1/2}, \qquad n \to \infty,$$

где

$$d_\nu = (-a_2)^{-\nu-1/2} \sum_{\nu=0}^{\infty} c_{m,2\nu-m} (-a_2)^{-m} \Gamma\left(m + \nu + \frac{1}{2}\right),$$

$$h(x) = a_2 x^2 + a_3 x^3 + \ldots, \qquad a_2 < 0, \qquad \psi(x) = b_0 + b_1 x + b_2 x^2 + \ldots,$$

$c_{m,k}$ — коэффициент двойного ряда по степеням y и x, в который раскладывается функция $\psi(x) \exp\{y(a_3 + a_4 x + a_5 x^2 + \ldots)\}$.

В рассматриваемом случае интересующие нас функции имеют вид

$$h(x) = 2h_1(x) = 2\left[(x+2)\ln(x+2) - (x+1)\ln(x+1) - (x+2)\ln 2\right] =$$

$$= -\frac{x^2}{2} + \frac{x^3}{4} - \frac{7x^4}{48} + \ldots,$$

$$h_2(x) = 1 + \frac{1}{x+1} - \frac{1}{x+2} = \frac{3}{2} - \frac{3x}{4} + \ldots,$$

$$g(x) = \frac{x+2}{x+1} = 2 - x + x^2 - x^3 + \ldots$$

Собирая вместе приведенные выше формулы, получаем

$$I_0 = \frac{n^{-1/2}}{2(2\pi)^{1/2}} - \frac{3n^{-3/2}}{64(2\pi)^{1/2}} + O\left(n^{-5/2}\right)$$

и, принимая во внимание, что $S_{0n} = I_0 + o(n^{-2})$, убеждаемся в справедливости асимптотического разложения

$$A_{0n} = \frac{n^{-1/2}}{2(2\pi)^{1/2}} - \frac{3n^{-3/2}}{64(2\pi)^{1/2}} + O\left(n^{-2}\right).$$

По той же схеме оцениваются коэффициенты A_{1n}, A_{2n}. Отличие от оценки коэффициента A_{0n} заключается лишь в приведении к удобному виду соответствующих сумм для $i = 1, 2$:

$$A_{in} = \sum_{t=n}^{\infty} \binom{t}{n} \left(\frac{1}{2}\right)^{t+1} \sum_{k=0}^{\min(n,t-n)} \binom{n}{k} \binom{t-n}{k} a_i(n,k),$$

где

$$a_1(n,k) = 2^{-t}(t+1-4k), \qquad a_2(n,k) = 2^{1-t}\left[\frac{t^2+t}{2} - 4(t-1)\,k + 8k(k-1)\right].$$

Теперь для доказательства теоремы 2 остается заметить, что из леммы 2 с учетом формулы (14) вытекает утверждение (10).

Мы исследовали вопросы определения вероятностей появления ошибок на выходе автомата $B_2(n,n)$ при условии, что распределения ошибок на входе и в управлении автомата известны. Другая постановка задачи относится к построению автоматов, которые восстанавливают выходную последовательность с более высокой надежностью. Например, в качестве автомата, восстанавливающего выходную последовательность по искаженным входной и управляющей последовательностям вместо исходного автомата $B_2(n,n)$ возьмем регистр сдвига R_{2n} на $2n$ элементов памяти. Тогда вероятность совпадения соответствующих выходных символов автомата $B_2(n,n)$ (работающего без помех) и регистра сдвига R_{2n} (перерабатывающего искаженную входную последовательность) будет равна $P_{BR} = 1/2 + \Delta_y$, причем $\Delta_y \sim 1/(4\pi n)^{1/2}$, $n \to \infty$. Приближение выходной последовательности автомата $B_2(n,n)$ с помощью переработки на том же автомате искаженных входной и управляющей последовательностей дает величину

$$\delta_y = \frac{1}{2(2\pi n)^{1/2}} \left(1 + \frac{19}{2}\delta_2^2 + \ldots\right).$$

Решение уравнения $\delta_y = \Delta_y$ относительно неизвестного параметра δ_2 приводит к граничному значению $\delta_{\text{гр}} \approx 0,2$. При $\delta_2 > \delta_{\text{гр}}$ автомат $B_2(n,n)$ дает лучшее приближение для выходной последовательности, чем автомат R_{2n}, а при $\delta_2 < \delta_{\text{гр}}$, наоборот, автомат R_{2n} дает лучшее приближение для выходной последовательности, чем автомат $B_2(n,n)$.

В заключение сделаем некоторые замечания относительно поведения вероятности выходной помехи при неравновероятном управлении. Пусть

$$\mathbf{P}(\gamma_t = 1) = p, \qquad \mathbf{P}(\gamma_t = 0) = q, \qquad p > q, \qquad p + q = 1.$$

Выражение для преобладания δ_y дано в (14). Найдем асимптотику первого члена $c_0(n)$ разложения функции

$$v(n+1, p, \delta_2) = c_0(n) + c_1(n)\,\delta_2 + \ldots$$

по степеням δ_2 при $n \to \infty$.

Теорема 3. *Пусть $p > q$, $a_q = \left(\sqrt{2} - \sqrt{q}\right)^{-1}$ и $n \to \infty$. Тогда*

$$c_0(n) \sim \frac{p}{4\sqrt{\pi n}} \frac{\sqrt{2/q}}{\sqrt[4]{2/q} - \sqrt[4]{q/2}} \left(p a_q^2\right)^n. \tag{21}$$

Доказательство. Проводя замену переменных по формуле $t = n(x + a_q\sqrt{2})$ и выполняя те же преобразования, что и в случае $p = q = 1/2$, получаем

$$c_0(n) = \frac{p}{(2\pi n)^{1/2}} \sum_{|x|<\epsilon} g(x) \exp\left\{n h_1(x) - \frac{1}{6n} h_2(x)\right\}\left(1 + O\left(n^{-3}\right)\right),$$

где

$$g(x) = \left[x + a_q\sqrt{2}\right]\left[x + a_q\sqrt{q}\right]^{-1},$$

$$h_1(x) = 2\left[x + a_q\sqrt{2}\right]\ln\left[x + a_q\sqrt{2}\right] - 2\left[x + a_q\sqrt{q}\right]\ln\left[x + a_q\sqrt{q}\right] -$$

$$- \left[x + a_q\sqrt{2}\right]\ln 2 + \left[x + a_q\sqrt{q}\right]\ln q + \ln p =$$

$$= 2\ln a_q + \ln p + \left[2 - \sqrt{\frac{q}{2}} - \sqrt{\frac{2}{q}}\right] x^2 + \frac{1}{3}\left[2\sqrt{\frac{q}{2}} - 2\sqrt{\frac{2}{q}} + \frac{2}{q} - \frac{q}{2}\right] x^3 + \ldots,$$

$$h_2(x) = 1 + \left[x + a_q\sqrt{q}\right]^{-1} - \left[x + a_q\sqrt{2}\right]^{-1} = \sqrt{\frac{q}{2}} + \sqrt{\frac{2}{q}} - 1 + \ldots$$

С учетом приведенных выше формул убеждаемся в справедливости выражения (21).

Автор считает своим приятным долгом выразить глубокую признательность А. М. Зубкову за полезные замечания.

СПИСОК ЛИТЕРАТУРЫ

1. *Golomb S. W.* Shift register sequences. — Aegean Park Press, 1982, 247 p.
2. *Кнут Д.* Искусство программирования для ЭВМ. Т. 2. — М.: Мир, 1977, 726 с.
3. *James F.* A review of pseudorandom number generators. — Comput. Phys. Commun., 1990, v. 60, p. 329–346.
4. *Perko A.* On the effect of a mixing table on a stationary random sequence. — Turun yliopiston julkaisuja. Annales universitatis turkuensis, 1971, ser. A, p. 3–5.
5. *Maclaren M. D., Marsaglia G.* Uniform random number generators. — J. Assoc. Comput. Mach., 1965, v. 12, p. 83–89.
6. *Фихтенгольц Г. М.* Курс дифференциального и интегрального исчисления. — М.: Наука, 1965.
7. *Феллер В.* Введение в теорию вероятностей и ее приложения. Т. 1. — М.: Мир, 1984, 514 с.
8. *де Брейн Н. Г.* Асимптотические методы в анализе. — М.: ИЛ., 1961, 248 с.
9. *Иванов В. А.* Автоматные преобразования случайных последовательностей. — В сб.: Труды по дискретной математике. Т. 2. — М.: ТВП, 1998, с. 151–168.