Math-Net.Ru
All Russian mathematical portal

V. G. Mikhailov, Investigation of combinatorial-probabilistic model of a controlled shift registers automata,
*Tr. Diskr. Mat.*, 2002, Volume 6, 139–149

https://www.mathnet.ru/eng/tdm95

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: 18.97.9.171
January 23, 2026, 13:48:17

Труды по дискретной математике
Том 6, с. 139–149
М.: ФИЗМАТЛИТ, 2002

# ИССЛЕДОВАНИЕ КОМБИНАТОРНО-ВЕРОЯТНОСТНОЙ МОДЕЛИ АВТОМАТОВ ИЗ РЕГИСТРОВ С НЕРАВНОМЕРНЫМ ДВИЖЕНИЕМ

В. Г. МИХАЙЛОВ

Рассмотрены некоторые естественные обобщения традиционной комбинаторно-вероятностной модели автоматов, состоящих из регистров с неравномерным движением. Получены явные оценки и асимптотические выражения для среднего числа циклических точек и для среднего числа подходов к этим циклам у автомата, выбранного случайно из указанного класса.

Рассмотрим конечный автомат $A$, содержащий $r$ регистров сдвига с линейными или нелинейными обратными связями. Движением регистров управляет специальный блок, который по набору текущих состояний регистров определяет на сколько шагов должен продвинуться (в смысле движения текущего состояния по циклу внутренних состояний) каждый из регистров за один такт. При неравномерном движении регистров граф внутренних состояний автомата $A$, вообще говоря, не будет циклическим, а будет отвечать некоторому отображению на множестве внутренних состояний. Особый интерес представляют точки, лежащие на циклах графа этого отображения (циклические точки) и точки, лежащие на подходах недалеко от циклов. В семидесятые годы А. П. Алферовым и Г. В. Проскуриным для изучения свойств автоматов с неравномерным движением была предложена естественная вероятностная модель таких автоматов. Согласно этой модели эволюция внутреннего состояния датчика описывается случайным блужданием на окружности (при $r = 1$) или торе (при $r \geq 2$). С ее помощью удалось получить оценки и асимптотические выражения для среднего числа циклов заданной длины и для среднего числа циклических точек в случайном автомате указанного вида (подробнее см. в [1]).

Однако за пределами упомянутой математической модели оказался ряд интересных классов автоматов. В настоящей работе традиционная модель обоб-

© В. Г. Михайлов, 2002

щается с таким расчетом, чтобы охватить эти классы автоматов. В рамках обобщенной модели получены выражения и оценки как для среднего числа точек, лежащих на циклах заданной длины, так и для среднего числа подходов к этим циклам.

С математической точки зрения программный датчик представляет собой автономный конечный автомат, определяемый конечными множествами $Q$ и $Y$ и функциями $g\colon Q \to Q$, $f\colon Q \to Y$, описывающими правило смены внутреннего состояния $q_{t+1} = g(q_t)$ и правило выработки знака выходной последовательности $y_t = f(q_t)$.

Если ограничиться исследованием внутренних состояний, то автономный конечный автомат можно изобразить в виде ориентированного графа $G$, вершинами которого являются элементы множества $Q$ (внутренние состояния), а дугами (направленными ребрами) — пары $(q, g(q))$. В нашем случае внутреннее состояние естественно описывать вектором $q = (q^1, \ldots, q^r)$, где $q^i \in Q^i = \{0, \ldots, l_i - 1\}$, $i = 1, \ldots, r$. Функция переходов описывается равенствами

$$g(q) = (q^1 + k^1(q), \ldots, q^r + k^r(q)), \tag{1}$$

с заранее заданными функциями $k = (k^1, \ldots, k^r)$

$$k\colon Q \to \mathcal{K} \subseteq \{0, \ldots, K_1\} \times \ldots \times \{0, \ldots, K_r\} \backslash \{(0, \ldots, 0)\} \tag{2}$$

при некоторых заданных числах $1 \le K_i < l_i$, причем сложения в (1) производятся по модулям $l_1, \ldots, l_r$ соответственно. Для систем уравнений в $\mathbf{Z}_{l_1} \times \ldots \times \mathbf{Z}_{l_r}$ будем использовать векторную запись. Например, система

$$q^i_{t+1} = q^i_t + k^i(q) \bmod l_i, \quad i = 1, \ldots, r,$$

будет записана в виде $q_{t+1} \equiv q_t + k(q)$.

Множество $\mathcal{K}$ и параметры $l_1, \ldots, l_r$ определяют интересующий нас класс конечных автоматов $\mathcal{A}(\mathcal{K})$. Всего в классе $\mathcal{A}(\mathcal{K})$ содержится $|\mathcal{A}(\mathcal{K})| = |\mathcal{K}|^L$ конечных автоматов. Здесь $L = l_1 \ldots l_r$ — число внутренних состояний автомата.

Основной результат работы формулируется следующим образом. Выберем случайно и равновероятно автомат $A_{rnd}$ из $\mathcal{A}(\mathcal{K})$. (Все характеристики этого автомата также будем помечать индексом $rnd$.) Отвечающие этому случайному автомату векторы $k_{rnd}(q)$, $q \in Q$, будут независимыми и распределенными равновероятно на $\mathcal{K}$.

Пусть $C_0(A, n)$ — множество точек автомата $A$, лежащих на циклах длины $n$, $C_h(A, n)$ — множество точек, лежащих на продходах к циклам длины $n$ на расстоянии $h > 0$ от цикла, а $C_h(A) = \bigcup_n C_h(A, n)$. В частности, $C_0(A)$ — множество всех циклических точек автомата $A$, $C_1(A, n)$ — множество точек, расположенных на подходах на расстоянии один от циклов длины $n$, а $|C_1(A, n)|$ совпадает с числом подходов к таким циклам.

Обозначим через $\xi$ случайный вектор, распределенный равновероятно на $\mathcal{K}$, и пусть $\xi_1, \xi_2, \ldots$ — его независимые копии. Выберем произвольное начальное внутреннее состояние $q_0 \in Q$.

Теорема 1. *При* $n \geq 1$ *и* $0 \leq h \leq L - n$

$$\mathbf{P}\{q_0 \in C_h(A_{rnd}, n)\} = \mathbf{P}\{\xi_{h+1} + \ldots + \xi_{h+n} \equiv \bar{0}, \\ \text{векторы } \bar{0}, \xi_1, \xi_1 + \xi_2, \ldots, \xi_1 + \ldots + \xi_{n+h-1} \text{ все различны}\}. \quad (3)$$

Здесь и далее $\bar{0} = (0, \ldots, 0)$.

Равенство (3) выражает тот факт, что распределение отрезка траектории точки на графе внутренних состояний автомата $A_{rnd}$ до момента ее самопересечения совпадает с распределением аналогичного отрезка случайного блуждания $\xi_1 + \ldots + \xi_t$, $t = 0, 1, \ldots$.

Теорема 1 позволяет получить много интересных утверждений о свойствах графа автомата $A_{rnd}$. Приведем некоторые из них.

Следствие 1.1. *При* $n \geq 1$ *и* $0 \leq h \leq L - n$

$$\mathbf{E}\,|C_h(A_{rnd}, n)| = L\,\mathbf{P}\{\xi_{h+1} + \ldots + \xi_{h+n} \equiv \bar{0}, \\ \text{векторы } \bar{0}, \xi_1, \xi_1 + \xi_2, \ldots, \xi_1 + \ldots + \xi_{n+h-1} \text{ все различны}\}.$$

Следствие 1.2. *При* $n \geq 1$ *и* $1 \leq h \leq L - n$

$$\mathbf{E}\,|C_h(A_{rnd}, n)| \leq \mathbf{E}\,|C_{h-1}(A_{rnd}, n)|. \quad (4)$$

Положим

$$B_n(s_1, \ldots, s_r) = \mathbf{P}\{\xi_1 + \ldots + \xi_n = (s_1, \ldots, s_r)\}.$$

Следствие 1.3. *При* $n \geq 1$ *и* $0 \leq h \leq L - n$

$$\mathbf{E}\,|C_h(A_{rnd}, n)| \leq L \sum_{d_1=0}^{\infty} \ldots \sum_{d_r=0}^{\infty} B_n(d_1 l_1, \ldots, d_r l_r). \quad (5)$$

Замечание 1. Каждое из неравенств $s_1 + \ldots + s_r < n$, $s_i > K_i n$ влечет равенство $B_n(s_1, \ldots, s_r) = 0$. Поэтому в сумме в правой части (5) отлично от нуля лишь конечное число слагаемых. Кроме этого, в сумме отсутствует (равно нулю) слагаемое при $d_1 = \ldots = d_r = 0$.

При $h = 0$ и $h = 1$ неравенства (4) и (5) можно уточнить. Положим

$$M = \min\{m \geq 1 \colon \exists\, k_1, \ldots, k_m \in \mathcal{K} \colon k_1 + \ldots + k_m \equiv \bar{0}\}.$$

Введем также обозначение

$$N = \max\{m \geq 2 \colon \mathcal{K} \cap \{\mathcal{K} + \ldots + \mathcal{K}\ (m \text{ слагаемых})\} = \varnothing\}.$$

З а м е ч а н и е 2. Если множество $\mathcal{K}$ не содержит векторов с нулевыми координатами, то $M, N \geq \max_i\{l_i/K_i\}$.

Теорема 2. *При $n \geq 1$ и $n < 2M$*

$$\mathbf{E}\,|C_0(A_{rnd}, n)| = L \sum_{d_1=0}^{\infty} \dots \sum_{d_r=0}^{\infty} B_n(d_1 l_1, \dots, d_r l_r), \tag{6}$$

$$\mathbf{E}\,|C_1(A_{rnd}, n)| \leq \left(1 - \frac{1}{|\mathcal{K}|}\right) \mathbf{E}\,|C_0(A_{rnd}, n)|. \tag{7}$$

*Если же $1 \leq n < \min\{2M, M+N\}$, то в (7) имеет место знак равенства.*

Равенство (6) (при $n < 2M$) вместе с очевидным неравенством

$$\mathbf{E}\,|C_0(A_{rnd})| \geq \sum_{n=1}^{m} \mathbf{E}\,|C_0(A_{rnd}, n)|, \quad 1 \leq m \leq L,$$

влекут следующую оценку.

Следствие 2.1. *Выполняется неравенство*

$$\mathbf{E}\,|C_0(A_{rnd})| \geq L \sum_{n=1}^{2M-1} \sum_{d_1,\dots,d_r} B_n(d_1 l_1, \dots, d_r l_r).$$

З а м е ч а н и е 3. Соотношения (4)–(6) при некоторых $h$ и $\mathcal{K}$ имеют довольно простой вид. Так, при $\mathcal{K} = \{1,2\} \times \dots \times \{1,2\}$, $l_1 \leq \dots \leq l_r$ и $l_r/2 \leq n < l_1$ соотношение (6) имеет вид

$$\mathbf{E}\,|C_0(A_{rnd}, n)| = \frac{l_1 \dots l_r}{2^{rn}} \prod_{i=1}^{r} \frac{n!}{(l_i - n)!(2n - l_i)!}. \tag{8}$$

З а м е ч а н и е 4. В работе [1] были получены явные выражения для вероятностей $\mathbf{P}\{q_0 \in C_0(A_{rnd})\}$ и оценки для среднего числа циклических точек в случае, когда $r \geq 1$ и

$$\mathcal{K} = \{1, \dots, K_1\} \times \dots \times \{1, \dots, K_r\}. \tag{9}$$

Там было показано, что при $K_1 = \dots = K_r = 2$ среднее число циклических точек автомата $A_{rnd}$ много больше, чем среднее число циклических точек в равновероятном случайном отображении на множестве из $L$ точек.

Постановки настоящей работы существенно шире постановок работы [1]. Чтобы продемонстрировать возникшие при этом расширении возможности, рассмотрим класс автоматов $\mathcal{S}(l_1, \dots, l_r) = \mathcal{A}(\mathcal{K})$, где

$$\mathcal{K} = \{(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1)\}.$$

Приводимое ниже утверждение вытекает непосредственно из следствия 1.2.

Следствие 1.4. *Для автомата $A_{rnd}$, выбранного случайно и равновероятно из множества $\mathcal{S}(l_1, \ldots, l_r)$, выполняется неравенство*

$$\mathbf{E}\,|C_0(A_{rnd}, n)| \le L\frac{n!}{r^n}\sum\frac{1}{(d_1 l_1)!\ldots(d_r l_r)!}, \tag{10}$$

*где сумма берется по всем решениям уравнения $n = d_1 l_1 + \ldots + d_r l_r$ относительно $d_1, \ldots, d_r \in \{0, 1, \ldots\}$.*

Из этого утверждения вытекает

Следствие 1.5. *Для чисел $n$, не представимых в виде $d_1 l_1 + \ldots + d_r l_r$ с $d_1, \ldots, d_r \in \{0, 1, \ldots\}$, выполняется равенство*

$$\mathbf{E}\,|C_0(A_{rnd}, n)| = 0. \tag{11}$$

З а м е ч а н и е 5. Множество $\{n\colon \mathbf{E}\,|C_0(A_{rnd}, n)| > 0\}$ назовем спектром и будем использовать для него обозначение $Sp(\mathcal{A}(\mathcal{K}))$. Следствие 1.4 показывает, что

$$Sp(\mathcal{S}(l_1, \ldots, l_r)) \subseteq \{n\colon n = d_1 l_1 + \ldots + d_r l_r\}.$$

Таким образом, цикловые свойства автоматов из $\mathcal{S}(l_1, \ldots, l_r)$ радикально отличаются от цикловых свойств случайных автоматов из множеств $\mathcal{A}(\mathcal{K})$ при $\mathcal{K}$ вида (8) и (9), у которых, согласно результатам работы [1], «спектры» длин циклов были «непрерывными».

Рассмотрим свойства случайного автомата из $\mathcal{S}(l_1, l_2)$ при не слишком различающихся длинах $l_1 \le l_2$, $3l_1 > 2l_2$, более детально. В этом случае в качестве начальных точек спектра выступают точки $l_1, l_2, 2l_1, l_1 + l_2, 2l_2$ (если $l_1 < l_2$) или точки $l_1, 2l_1 = l_1 + l_2 = 2l_2$, если $l_1 = l_2$.

Теорема 3. *Пусть автомат $A_{rnd}$ выбран случайно и равновероятно из множества автоматов $\mathcal{S}(l_1, l_2)$, где $l_1 \le l_2$, $3l_1 > 2l_2$.*

1) *Выполняются неравенства*

$$\mathbf{E}\,|C_0(A_{rnd}, l_1 + l_2)| = l_1 l_2\,\mathbf{P}\{q_0 \in C_0(A_{rnd}, l_1 + l_2)\} \le \frac{l_1 l_2}{2^{l_1+l_2}} C_{l_1+l_2}^{l_1}, \tag{12}$$

$$\mathbf{E}\,|C_0(A_{rnd}, l_1 + l_2)| \ge l_1 l_2 \frac{1}{2^{l_1+l_2}}\left(C_{l_1+l_2}^{l_1} - 2(l_1 + l_2)\right). \tag{13}$$

2) *Если $l_1 < l_2$, то при $i = 1, 2$*

$$\mathbf{E}\,|C_0(A_{rnd}, l_i)| = l_1 l_2 2^{-l_i}, \quad \mathbf{E}\,|C_0(A_{rnd}, 2l_i)| = l_1 l_2 2^{-2l_i}. \tag{14}$$

*Если $l_1 = l_2$, то*

$$\mathbf{E}\,|C_0(A_{rnd}, l_1)| = l_1 l_2 2^{1-l_1}. \tag{15}$$

Следствие 3.1. *Пусть автомат $A_{rnd}$ выбран случайно и равновероятно из множества автоматов $\mathcal{S}(l_1, l_2)$. Тогда*

$$\mathbf{E}\,|C_0(A_{rnd})| \geq \mathbf{E}\,|C_0(A_{rnd}, l_1 + l_2)| = l_1\sqrt{\frac{l_1}{\pi}}(1 + o(1)),$$

*если $l_1 \to \infty$ и $l_2 = l_1 + o(\sqrt{l_1})$.*

Замечание 6. Ясно, что значения $\mathbf{P}\{q_0 \in C_0(A_{rnd}, n)\}$ для $n = l_1, l_2$, $n = 2l_1, 2l_2$ при $n \to \infty$ бесконечно малы по сравнению с вероятностью $\mathbf{P}\{q_0 \in C_0(A_{rnd}, l_1 + l_2)\}$. Вычислительные эксперименты на компьютере показывают, что в случае $r = 2$, $l_1 \approx l_2$ среднее число точек на циклах длиной больше $l_1 + l_2$ весьма мало. Поэтому есть основания полагать, что для случайного автомата $A_{rnd}$ из $\mathcal{S}(l_1, l_2)$ при $l_1 \to \infty$, $l_2 = l_1 + o(\sqrt{l_1})$ выполнено соотношение

$$\mathbf{E}\,|C_0(A_{rnd})| = \frac{l_1 l_2 C_{l_1+l_2}^{l_1}}{2^{l_1+l_2}}(1 + o(1)). \tag{16}$$

Замечание 7. Сравнивая оценку следствия 3.1 с соотношением (8) работы [1], убеждаемся, что для среднего числа циклических точек случайного автомата $A_{rnd}$ из $\mathcal{S}(l_1, l_2)$ выполнена такая же оценка, как и для автоматов из $\mathcal{A}(\mathcal{K})$ при $\mathcal{K}$ вида (8) и (9).

Теорема 4. *Пусть автомат $A_{rnd}$ выбран случайно и равновероятно из множества автоматов $\mathcal{S}(l_1, l_2)$, где $l_1 \leq l_2$, $3l_1 > 2l_2$. Тогда*

$$\mathbf{E}\,|C_1(A_{rnd}, l_1 + l_2)| \leq \frac{l_1 l_2}{2^{1+l_1+l_2}} C_{l_1+l_2}^{l_1},$$

$$\mathbf{E}\,|C_1(A_{rnd}, l_1 + l_2)| \geq \frac{l_1 l_2}{2^{1+l_1+l_2}}\left(C_{l_1+l_2}^{l_1} - 2(l_1 + l_2)\right) -$$

$$- l_1 l_2 (l_1 + l_2)\left(2^{-l_1-1} + 2^{-2l_1-1} + 2^{-l_2-1}\right).$$

Следствие 4.1. *Пусть автомат $A_{rnd}$ выбран случайно и равновероятно из множества автоматов $\mathcal{S}(l_1, l_2)$ и $l_1 \to \infty$, $l_2 = l_1 + o(\sqrt{l_1})$. Тогда*

$$\mathbf{E}\,|C_1(A_{rnd}, l_1 + l_2)| = \frac{l_1}{2}\sqrt{\frac{l_1}{\pi}}(1 + o(1)).$$

Перейдем к доказательствам сформулированных теорем.

Доказательство теоремы 1 проводится по схеме доказательства теоремы 1 из [1]. Рассмотрим случайное блуждание $S(t) = (S_1(t), \ldots, S_r(t))$ на множестве $Q$, выходящее из точки $S(0) = q_0$ и определяющееся при $t = 1, 2, \ldots$ равенствами

$$S_i(t) = S_i(t-1) + X_i(t) \bmod l_i, \quad i = 1, \ldots, r, \tag{17}$$

где $\{X(t) = (X_1(t), \dots, X_r(t)) \in \mathcal{K},\ t = 1, 2, \dots\}$ — система независимых в совокупности равновероятно распределенных на $\mathcal{K}$ случайных векторов. Далее будем использовать векторную запись равенств (17):

$$S(t) \equiv S(t-1) + X(t).$$

Аналогично запишем уравнение эволюции внутренних состояний случайного автомата:

$$q_{rnd}(t+1) \equiv q_{rnd}(t) + k_{rnd}(q(t)).$$

Наши рассуждения опираются на следующее свойство, вытекающее из равновероятности и независимости величин $k_{rnd}(q)$, $q \in Q$.

Лемма 1. *При всех неотрицательных целых $n \le |Q|$ и всех наборах попарно различных $q_0, q_1, \dots, q_{n-1} \in Q$ условные функции распределения*

$$\mathcal{L}(X(1), \dots, X(n) | S(1) = q_1, \dots, S(n-1) = q_{n-1}),$$
$$\mathcal{L}(k_{rnd}(q_{rnd,0}), \dots, k_{rnd}(q_{rnd,n-1}) | q_{rnd,1} = q_1, \dots, q_{rnd,n-1} = q_{n-1})$$

*совпадают (заметим, что $q_{rnd,0} = q_0$).*

Вернемся к доказательству теоремы 1. Нам достаточно рассмотреть случай $m \le L$. Воспользуемся леммой 1 при анализе вероятности события $\{q_0 \in C_h(A_{rnd}, m)\}$. Обозначим через $Q_m$ множество всех наборов $(q_1, \dots, q_m)$ из попарно различных $q_1, \dots, q_m \in Q \backslash \{q_0\}$.

Очевидно, что

$$\{q_0 \in C_h(A_{rnd}, n)\} = \\ = \bigcup_{Q_{n+h-1}} \{k_{rnd,s} \equiv q_t - q_{t-1},\ t = 1, \dots, n-1,\ k_{rnd,n+h-1} \equiv q_h - q_{n+h-1}\}.$$

Используя лемму 1, можем записать:

$$\mathbf{E}\,|C_h(A_{rnd}, m)| = L\,\mathbf{P}\{q_0 \in C_h(A_{rnd}, m)\} = L\,\mathbf{P}\{H_h\}, \tag{18}$$

$$H_h = \bigcup_{Q_{n+h-1}} A(q_1, \dots, q_{n+h-1}; q_h), \tag{19}$$

где множества $A(q_1, \dots, q_{n+h-1}; q_h)$ попарно не пересекаются и имеют вид

$$A(q_1, \dots, q_{n+h-1}; q_h) = \\ = \{X(t) \equiv q_t - q_{t-1},\ t = 1, \dots, n+h-1,\ X(n) \equiv q_h - q_{n+h-1}\} = \\ = \{S(t) = q_t,\ t = 1, \dots, n-1,\ S(n+h) = q_h\}.$$

Из равенств (18) и (19) следует (3). Теорема 1 доказана.

При доказательстве теоремы 2 нам понадобится следующая лемма.

Лемма 2. *Пусть*

$$n < 2M \quad \text{и} \quad (q_1, \ldots, q_{n-1}) \in Q^{n-1} \backslash Q_{n-1}.$$

*Тогда*

$$\mathbf{P}\{A(q_1, \ldots, q_{n-1}; q_0)\} = 0. \tag{20}$$

Доказательство леммы. Очевидно, что из условий леммы вытекает соотношение

$$A(q_1, \ldots, q_{n-1}; q_0) \subseteq \bigcup_{1 \le s < t \le n} \{S(s) = S(t),\, S(n) = q_0\}, \tag{21}$$

а

$$\{S(s) = S(t),\, S(n) = q_0\} = \{X(s+1) + \ldots + X(t) \equiv 0,$$
$$X(1) + \ldots + X(s) + X(t+1) + \ldots + X(n) \equiv 0\}, \tag{22}$$

причем обе суммы не пустые. Так как $n < 2M$, то хотя бы одна сумма в правой части (22) состоит из $n'$, $0 < n' < M$, слагаемых. Но сумма $X(1) + \ldots + X(n')$ такого числа слагаемых не может быть сравнима с нулем в силу определения величины $M$. Поэтому вероятность события в правой части (22) равна нулю. Теперь из (22) и (21) следует (20).

Лемма 2 доказана.

Доказательство теоремы 2. Напомним, что $n < 2M$. Очевидно, что

$$\mathbf{P}\{H_0\} = \sum_{Q_{n-1}} \mathbf{P}\{A(q_1, \ldots, q_{n-1}; q_0)\}.$$

Кроме этого, согласно лемме 2

$$\sum_{Q_{n-1}} \mathbf{P}\{A(q_1, \ldots, q_{n-1}; q_0)\} = \mathbf{P}\{S(n) = q_0\}.$$

Поэтому

$$\mathbf{P}\{H_0\} = \mathbf{P}\{S(n) = q_0\}.$$

Отсюда и из (18) следует равенство (6).

Докажем теперь неравенство (7). Из (3) следует, что

$$\begin{aligned}\mathbf{P}\{q_0 \in C_1(A_{rnd}, n)\} &= \mathbf{P}\{\xi_2 + \ldots + \xi_{n+1} \equiv \bar{0},\\ &\text{векторы } \bar{0}, \xi_1, \xi_1 + \xi_2, \ldots, \xi_1 + \ldots + \xi_n \text{ все различны}\} =\\ &= \mathbf{P}\{\xi_2 + \ldots + \xi_{n+1} \equiv \bar{0},\\ &\text{векторы } \xi_2, \xi_2 + \xi_3, \ldots, \xi_2 + \ldots + \xi_n \text{ все различны},\\ &\xi_1 \notin \{\bar{0}, -\xi_2, -(\xi_2 + \xi_3), \ldots, -(\xi_2 + \ldots + \xi_n)\}\}. \quad (23)\end{aligned}$$

По лемме 2 при $n \leq 2M$ всё векторы $\xi_2, \xi_2 + \xi_3, \ldots, \xi_2 + \ldots + \xi_n$ отличны от $\bar{0}$. Поэтому цепочка соотношений (23) может быть продолжена следующим образом:

$$\begin{aligned}\mathbf{P}\{q_0 \in C_1(A_{rnd}, n)\} &= \mathbf{P}\{\xi_2 + \ldots + \xi_{n+1} \equiv \bar{0},\\ &\text{векторы } \bar{0}, \xi_2, \xi_2 + \xi_3, \ldots, \xi_2 + \ldots + \xi_n \text{ все различны},\\ &\xi_1 \notin \{\bar{0}, -\xi_2, -(\xi_2 + \xi_3), \ldots, -(\xi_2 + \ldots + \xi_n)\}\} \leq\\ &\leq \mathbf{P}\{\xi_2 + \ldots + \xi_{n+1} \equiv \bar{0},\\ &\text{векторы } \bar{0}, \xi_2, \xi_2 + \xi_3, \ldots, \xi_2 + \ldots + \xi_n \text{ все различны},\\ &\xi_1 \neq -(\xi_2 + \ldots + \xi_n) \equiv \xi_{n+1}\} =\\ &= \left(1 - \frac{1}{|\mathcal{K}|}\right) \mathbf{P}\{q_0 + \xi_1 \in C_0(A_{rnd}, n)\} =\\ &= \left(1 - \frac{1}{|\mathcal{K}|}\right) \mathbf{P}\{q_0 \in C_0(A_{rnd}, n)\}. \quad (24)\end{aligned}$$

Из (24) следует неравенство (7).

Заметим, что соотношения

$$\xi_1 \equiv -\xi_2, \quad \xi_1 \equiv -(\xi_2 + \xi_3), \quad \ldots, \quad \xi_1 \equiv -(\xi_2 + \ldots + \xi_{M-1})$$

невозможны. Если выполнено соотношение

$$\xi_2 + \ldots + \xi_{n+1} \equiv \bar{0}, \quad (25)$$

то при $n \leq M + N - 1$ невозможны и соотношения

$$\xi_1 \equiv -(\xi_2 + \ldots + \xi_M), \quad \ldots, \quad \xi_1 \equiv -(\xi_2 + \ldots + \xi_n),$$

поскольку последние в силу (25) эквивалентны соотношениям

$$\xi_1 \equiv \xi_{M+1} + \ldots + \xi_{n+1}, \quad \ldots, \quad \xi_1 \equiv \xi_n + \xi_{n+1}, \quad \xi_1 \equiv \xi_{n+1}.$$

Поэтому при $n \leq M + N - 1$ в цепочке соотношений (24) вместо неравенства выполняется строгое равенство. Теорема 2 доказана.

Доказательство теоремы 3. Из (3) следует, что

$$\mathbf{E}\,|C_0(A_{rnd},n)| \le l_1 l_2\,\mathbf{P}\{\xi_1+\ldots+\xi_n\equiv\bar{0}\} \tag{26}$$

и

$$\begin{aligned}\mathbf{E}\,|C_0(A_{rnd},n)| &\ge l_1 l_2\,\mathbf{P}\{\xi_1+\ldots+\xi_n\equiv\bar{0}\} - \\ &- l_1 l_2 \sum_{1\le i<j<n} \mathbf{P}\{\xi_1+\ldots+\xi_n\equiv\bar{0},\ \xi_{i+1}+\ldots+\xi_j\equiv\bar{0}\} = \\ &= l_1 l_2\,\mathbf{P}\{\xi_1+\ldots+\xi_n\equiv\bar{0}\} - \\ &- l_1 l_2 \sum_{1\le i<j<n} \mathbf{P}\{\xi_1+\ldots+\xi_{n-(j-i)}\equiv\bar{0}\}\,\mathbf{P}\{\xi_1+\ldots+\xi_{j-i}\equiv\bar{0}\}. \end{aligned} \tag{27}$$

Первое из этих неравенств — частный случай неравенства (5). Из (26) и равенства

$$\mathbf{P}\{\xi_1+\ldots+\xi_{l_1+l_2}\equiv\bar{0}\} = \frac{1}{2^{l_1+l_2}} C_{l_1+l_2}^{l_1} \tag{28}$$

следует неравенство (12). При $n = l_1 + l_2$ вычитаемое в (27) не превосходит

$$2\sum_{i=1}^{n} \mathbf{P}\{\xi_1+\ldots+\xi_{l_1}\equiv\bar{0}\}\,\mathbf{P}\{\xi_1+\ldots+\xi_{l_2}\equiv\bar{0}\} = 2(l_1+l_2)2^{-l_1-l_2}.$$

Поэтому из (27) и (28) следует неравенство (13).

Теперь докажем равенства (14) и (15). Заметим, что вычитаемое в правой части цепочки соотношений (27) может быть отлично от нуля только в том случае, если $n$ — сумма двух точек спектра. Поэтому при $n = l_1$ и при $n = l_2$ оно равно нулю, и пара соотношений (26), (27) превращается в одно строгое равенство.

Чтобы вычислить искомую вероятность при $l_1 < l_2$, $n = dl_1$, $d = 1, 2$, заметим, что в этом случае

$$\mathbf{P}\{\xi_1+\ldots+\xi_{dl_1}\equiv\bar{0}\} = \mathbf{P}\{\xi_1^2=\ldots=\xi_{dl_1}^2=0\} = 2^{-dl_1}.$$

Здесь $\xi_m^2$ — вторая координата вектора $\xi_m = (\xi_m^1, \xi_m^2)$. Аналогично рассматривается случай $l_1 < l_2$, $n = dl_2$.

Наконец, при $l_1 = l_2$

$$\mathbf{P}\{\xi_1+\ldots+\xi_{l_1}\equiv\bar{0}\} = \mathbf{P}\{\xi_1^1=\ldots=\xi_{l_1}^1=0\} + \mathbf{P}\{\xi_1^2=\ldots=\xi_{l_1}^2=0\} = 2^{1-l_1}.$$

Теорема 3 доказана.

Доказательство теоремы 4 во многом аналогично доказательству пункта 1 теоремы 3, но заметно более громоздко. Поэтому мы его опускаем.

## СПИСОК ЛИТЕРАТУРЫ

1. *Михайлов В. Г.* Исследование числа циклических точек автомата из регистров с неравномерным движением. — В сб.: Труды по дискретной математике. Т. 5. — М.: ФИЗМАТЛИТ, 2002, с. 167–172.