Математика и ее приложения : ЖИМО. 2012. Вып. 1 (9). С. 9–14

УДК 512.543

А. Е. Веремеенко[1], **В. М. Деундяк**[2]

Экспериментальное исследование влияния сбоев на работу одного семейства перемешивающих автоматов

Ключевые слова: перемешивающий автомат, сбой, режим CFB, время самонастройки, математическое ожидание, дисперсия.

Построена программная реализация одного семейства перемешивающих автоматов, исследованного В. А. Ивановым. Проведен ряд экспериментов по определению асимптотических оценок времени самонастройки автоматов. Исследованы некоторые случаи, для которых не известны теоретические оценки времени самонастройки.

Key words: permutation automaton, failure, CFB mode, self-adjustment time, expectation value, dispersion.

Software implementation of family of permutation automata, researched by V. A. Ivanov, is built, and number of experiments to determine asymptotic estimates of self-adjustment time were carried out. Some cases for which no theoretical estimates of self-adjustment time are known are researched.

1. Введение

Перемешивающие автоматы используются во многих задачах защиты информации, например таких, как генерация псевдослучайных чисел, блочное шифрование в режиме CFB и др. [1]. В работе В. А. Иванова [2] введены несколько семейств перемешивающих автоматов, работа которых рассмотрена в условиях возникновения внешних помех и внутренних сбоев, в частных случаях получены асимптотические оценки времени самонастройки автоматов. Распространению этих результатов на более общую ситуацию посвящена работа [3].

В настоящей работе представлены результаты экспериментов, проведенных над одним из семейств автоматов Иванова. Результаты экспериментов согласуются с асимптотическими оценками математического ожидания и в целом близки к асимптотическим оценкам дисперсии. Кроме того, в настоящей работе представлены результаты экспериментов для сочетаний параметров автоматов, не рассмотренных в [2], [3]. Полученные оценки математического ожидания и дисперсии времени самонастройки

[1]Южный федеральный университет; E-mail: arwer13@gmail.com

[2]Южный федеральный университет; ФГАНУ НИИ «Спецвузавтоматика»; E-mail: vlade@math.rsu.ru

показывают, что случай, рассмотренный Ивановым, является в некотором смысле оптимальным.

2. Семейство перемешивающих автоматов $\mathfrak{A}_{n,\rho,p}$

Приведем необходимые сведения о перемешивающих автоматах из [2]. Рассмотрим два одинаковых автомата A и A' и ситуацию, когда в автомате A' возможно возникновение сбоев, приводящих к изменению его состояния, а в последовательности входных символов возможны искажения типа замены. Пусть сбои и искажения появляются достаточно редко, а в промежутках между ними автомат A' работает исправно. В этом случае для нахождения оценок времени, по прошествии которого автомат A' перестанет испытывать влияние возникшего сбоя или искажения, можно воспользоваться моделью, в которой происходит только сбой автомата и только в начальный момент времени.

Пусть s_t и s'_t – состояния автоматов A и A' в момент времени t соответственно, а в начальный момент времени $s_0 \neq s'_0$. Обозначим $\pi_t = \mathsf{P}(s_t \neq s'_t)$. Автоматы, для каждого из которых $\lim\limits_{t\to\infty} \pi_t = 0$ и не существует такого натурального числа T, что $\pi_T = 0$, называются *почти устойчивыми автоматами*. Помимо почти устойчивых автоматов выделяют *устойчивые*, *частично устойчивые* и *неустойчивые* автоматы.

Рассмотрим один из автоматов, описанных в [2], в удобных для нас обозначениях:

$$A_{n,\,\rho,p} = (X^n, X \times \Gamma, X, \delta, \lambda),$$

где X – алфавит выходных символов, $\Gamma = \{1; 2\}$ – множество управляющих символов, $X \times \Gamma$ – алфавит входных символов, X^n – множество состояний автомата, δ – функция переходов, λ – функция выходов. Далее для произвольного вектора b через b_i обозначим его координату с номером i. Для описания функций переходов и выходов рассмотрим перестановки G_1 и G_2 над словами длины $n+1$:

$$G_1 = (x, s_1, \ldots, s_{n\rho})(s_{n\rho+1}) \ldots (s_n),$$

$$G_2 = (x, s_{n\rho+1}, \ldots, s_n)(s_1) \ldots (s_{n\rho}),$$

где $x \in X$, $s = (s_1, s_2, \ldots, s_n) \in X^n$ – текущее состояние автомата, ρ – некоторое число, такое, что $0 < \rho < 1$ и $n\rho$ – целое. Тогда

$$\delta(x, \gamma, s) = \left(G_\gamma(x|s)_1, \ldots, G_\gamma(x|s)_n\right),$$

$$\lambda(x, \gamma, s) = G_\gamma(x|s)_0,$$

где символ $|$ обозначает конкатенацию.

Будем считать, что на управление автомата поступает последовательность независимых случайных величин $\gamma_1, \gamma_2, \ldots, \gamma_t, \ldots$, принимающих значения из множества $\Gamma = \{1; 2\}$ и имеющих одно и то же распределение

$$\forall t \in N \quad \mathsf{P}(\gamma_t = 1) = p, \quad \mathsf{P}(\gamma_t = 2) = 1 - p.$$

Обозначим через $\mathfrak{A}_{n,\,\rho,p}$ семейство автоматов $A_{n,\,\rho,p}$ со всевозможными допустимыми значениями параметров n, ρ, p.

Число $\min\{t : s_t = s'_t, t = 1, 2, \ldots\}$ назовем *временем самонастройки автомата* $A_{n,\,\rho,p}$ и обозначим $\tau(n, \rho, p)$.

Теорема 1 ([2], Теорема 5). *Пусть* $n \to \infty$, $p = \mathsf{P}(\gamma = 1)$, $q = 1 - p$. *Тогда, если* np *– целое, то при* $\rho = p$ *для оценок математического ожидания* $\mathbf{E}\tau(n, p, p)$ *и дисперсии* $\mathbf{D}\tau(n, p, p)$ *времени самонастройки автомата* $A_{n,p,p}$ *верны равенства:*

$$\mathbf{E}\tau(n, p, p) = n + \sqrt{\frac{n}{2\pi pq}} - \frac{1 - pq}{12pq\sqrt{2\pi pqn}} + O\left(\frac{1}{n^{3/2}}\right),$$

$$\mathbf{D}\tau(n, p, p) = \frac{(\pi(1 - 2pq) - 1)n}{2\pi pq} - \frac{(3pq + 2(p - q)^2)\sqrt{n}}{3pq\sqrt{2\pi pq}} + O\left(\frac{1}{n^{1/2}}\right)$$

при $n \to \infty$.

3. Экспериментальное исследование оценок В. А. Иванова для семейства $\mathfrak{A}_{n,p,p}$

Рассмотрим ряд экспериментов над семейством $\mathfrak{A}_{n,p,p}$ (случай $\rho = p$). Автоматы были программно реализованы на языке Python. Для генерации последовательности управляющих символов использовался ГПСЧ библиотеки PyCrypto [4]. Во время эксперимента на вход автомата подавались 4000 потенциально бесконечных слов, и определялось время самонастройки на таком входе. На основе полученной выборки рассчитывались оценки математического ожидания и дисперсии времени самонастройки, которые будем обозначать $E^e_{n,p}$ и $D^e_{n,p}$ соответственно. Оценки $\mathbf{E}\tau(n, p, p)$ и $\mathbf{D}\tau(n, p, p)$ из теоремы 1 обозначим $E^t_{n,p}$ и $D^t_{n,p}$ соответственно. Пусть $\lambda^E_{n,\rho} = |E^t_n - E^e_n|$ и $\lambda^D_{n,\rho} = |D^t_n - D^e_n|$.

Приведем результаты некоторых экспериментов в форме таблиц.

Таблица 1

$\rho = p = 0.5$										
n	30	60	90	120	150	180	210	240	270	300
$E^t_{n,p}$	34.33	66.15	97.54	128.72	159.75	190.68	221.54	252.34	283.09	313.80
$E^e_{n,p}$	34.01	65.84	97.27	128.26	159.53	190.56	221.09	252.05	282.77	313.60
$\lambda^E_{n,p}$	0.32	0.31	0.27	0.46	0.21	0.12	0.45	0.29	0.32	0.32
$D^t_{n,p}$	6.53	15.62	25.13	34.86	44.73	54.70	64.74	74.85	85.00	95.19
$D^e_{n,p}$	15.61	27.27	40.81	48.88	67.68	80.65	90.09	99.28	112.82	122.01
$\lambda^D_{n,p}$	9.08	11.64	15.68	14.02	22.95	25.95	25.35	24.43	27.82	17.63

Таблица 2

$\rho = p = 0.3$										
n	30	60	90	120	150	180	210	240	270	300
$E^t_{n,p}$	34.71	66.70	98.23	129.51	160.63	191.65	222.59	253.46	284.28	315.06
$E^e_{n,p}$	34.24	66.26	97.95	129.01	160.47	191.01	222.22	252.92	283.83	314.85
$\lambda^E_{n,p}$	0.47	0.44	0.27	0.49	0.16	0.64	0.37	0.54	0.45	0.45
$D^t_{n,p}$	11.50	27.21	43.62	60.38	77.38	94.54	111.82	129.20	146.65	164.18
$D^e_{n,p}$	25.77	44.03	69.45	88.09	114.43	115.72	152.23	160.47	190.23	203.27
$\lambda^D_{n,p}$	14.26	16.82	25.82	27.70	37.04	21.18	40.41	31.27	43.58	26.05

Выводы. 1. Экспериментальная и теоретическая оценки математического ожидания времени самонастройки согласуются. Полученная разница оценок математического ожидания времени самонастройки $\lambda^E_{n,p}$ асимптотически согласуется с оценкой $O\left(\frac{1}{n^{3/2}}\right)$ из теоремы 1.

2. Экспериментальная и теоретическая оценки дисперсии времени самонастройки имеют один и тот же порядок, но $D^e_{n,p}$ во всех экспериментах превосходит $D^t_{n,p}$. Разница оценок $\lambda^D_{n,p}$ при рассмотренных n колеблется около некоторого числа, не зависящего от n, что асимптотически не согласуется с оценкой $O\left(\frac{1}{n^{1/2}}\right)$ из теоремы 1. Однако величина $\dfrac{\lambda^D_{n,p}}{D^e_{n,p}}$ с увеличением n уменьшается для всех рассмотренных значений параметра p $(0.1,\ 0.2,\ \ldots,\ 0,9)$.

4. Экспериментальное исследование семейства $\mathfrak{A}_{n,\rho,p}$

Приведем в форме графиков результаты некоторых экспериментов над семейством $\mathfrak{A}_{n,\rho,p}$. Эксперименты проводились по схеме, описанной в разделе 3. На оси абсцисс отмечена длина слова-состояния автомата n, а на оси ординат – исследуемая величина.

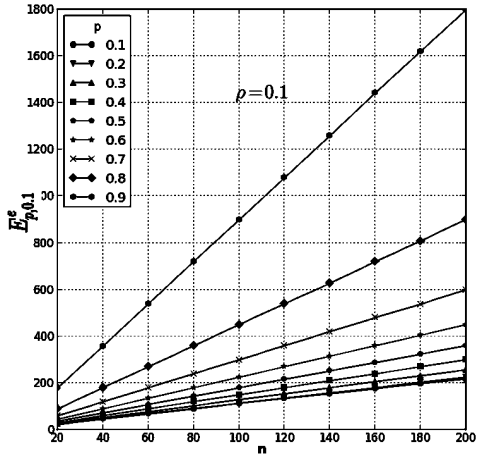

Рис. 1

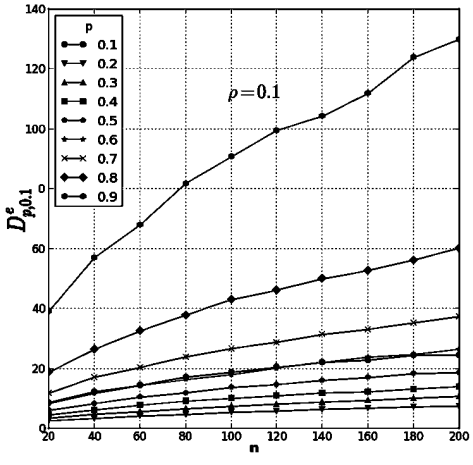

Рис. 2

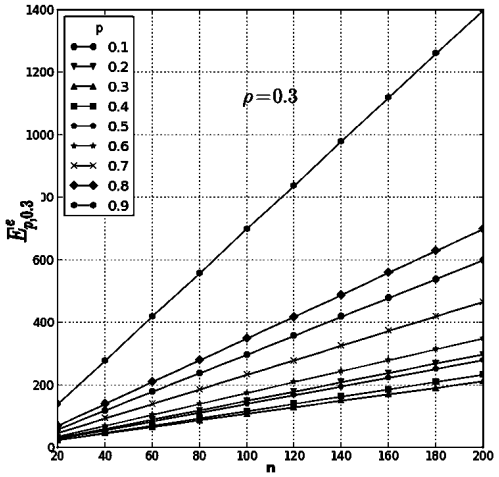

Рис. 3

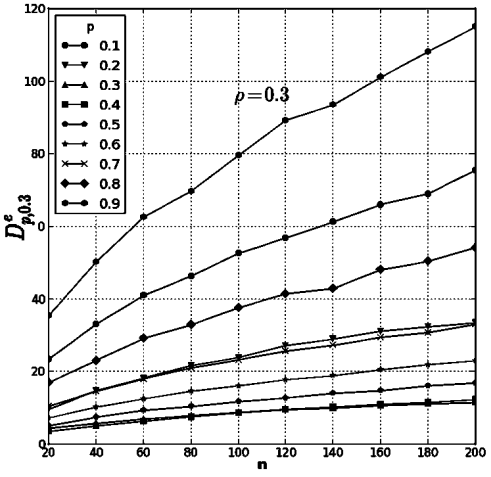

Рис. 4

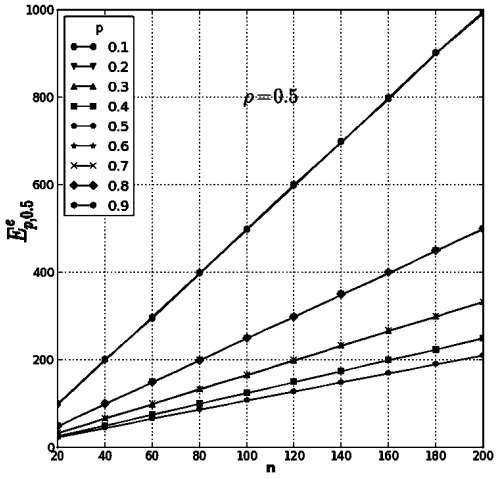

Рис. 5

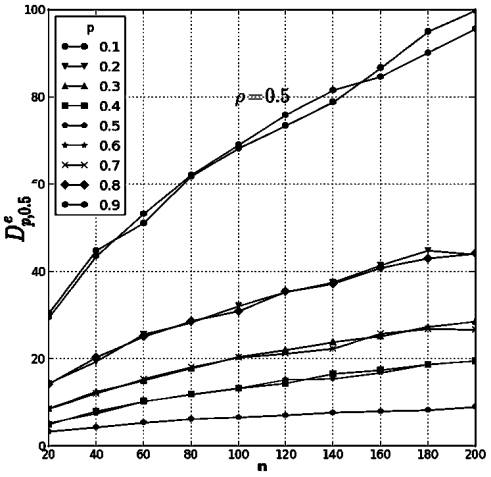

Рис. 6

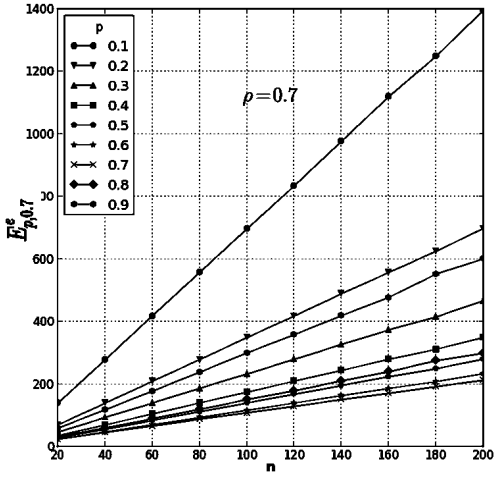

Рис. 7

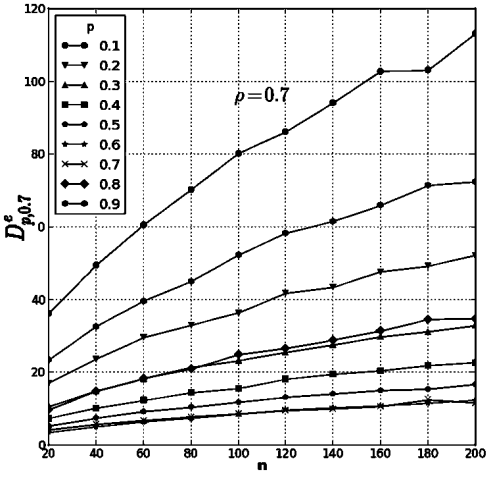

Рис. 8

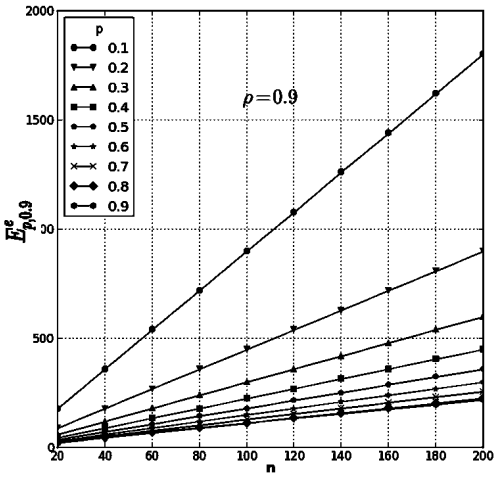

Рис. 9

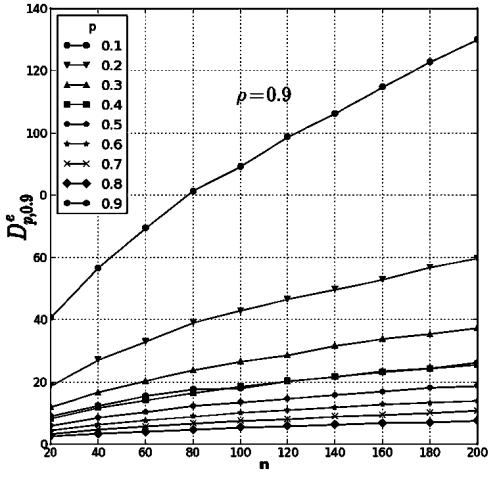

Рис. 10

Выводы. В случае $\rho = 0.5$ значения оценок математического ожидания и дисперсии симметричны относительно p (рис. 5, 6). Оптимальным с точки зрения минимизации времени самонастройки является случай $p = \rho$ (рис. 1, 3, 5, 7, 9). С точки зрения минимизации дисперсии времени самонастройки случай $p = \rho$ является оптимальным в случаях, когда $\rho = 0.3$, $\rho = 0.5$, $\rho = 0.7$ (рис. 4, 6, 8). Когда значение ρ отклоняется от 0.5 на большее число ($\rho = 0.1$, $\rho = 0.9$ – рис. 2, 10), случай $p = \rho$ перестает быть оптимальным.

Список литературы

1. *Бабаш А. В., Шанкин. Г. П.* Криптография. М. : СОЛОН-ПРЕСС, 2007. 512 с.
2. *Иванов В. А.* Автоматные преобразования случайных последовательностей // Труды по дискретной математике. 1998. Т. 2. С. 151 – 168.
3. *Иванов В. А.* Асимптотические оценки вероятностных характеристик времени самонастройки перемешивающих автоматов // Труды по дискретной математике. 2001. Т. 4. С. 57 – 70.
4. *Dwayne C. Litzenberger* The Python Cryptography Toolkit. `URL:https://www.dlitz.net/software/pycrypto/` (дата обращения: 10.11.2012)

Поступила в редакцию 27.11.2012.