УДК 519.21

ДИНАМИЧЕСКИЙ ТЕСТ ГПСЧ ПО КРИТЕРИЮ МАКСИМАЛЬНОГО ЛОКАЛЬНОГО ТРЕНДА

Шашкина Е. А., Плотников А. Н.

Самарский национальный исследовательский университет
имени академика С. П. Королёва, г. Самара

Алгоритмический генератор псевдослучайных чисел (АГПСЧ) служит одним из базовых элементов информационных технологий, включая компютерную криптографию. При этом, поскольку алгоритмическая природа принципиально несовместима с истинной случайностью [1,2], крайне актуальной является задача обеспечения (и соответственно контроля) корректности генерируемой последовательности. Проблема случайности также актуальна для многих приложений теории вероятностей, в частности, для анализа временных рядов [1,2]. Одним из наиболее удобных элементов статистики критериев случайности являются серии [1,2], в частности, повторяющиеся знаки последовательных разностей. Последние выглядят как локальный монотонный тренд. Не ограничивая общность результатов [1-3], рассмотрим выборку из совокупности $R(0,1)$. Обозначая 0 отрицательные значения разностей, $\mathbf{1}$ - положительные, вероятность любого отрезка последовательности теперь однозначно определится через повторный интеграл вида $P\underbrace{\{01...01\}}_{n-1}=\int_0^1 dx_n\int_0^{x_n} dx_{n-1}\int_{x_{n-1}}^1 dx_{n-2}...\int_0^{x_3} dx_2\int_{x_2}^1 dx_1$, т.е. $P_n=\int_0^1\varphi_n(x)dx$. Вероятности $P\{L_n^+<l\}=q_n^{(l)}$ будет соответствовать рекуррентный многочлен, порядка $\boldsymbol{l}-1$:

$$\begin{cases}\varphi_n^{(l)}(x)=\int_0^x\overline{\varphi}_{n-1}^{(l)}(x)dx+...+\underbrace{\int_0^x...\int_0^x}_{l-2}\overline{\varphi}_{n-l+2}^{(l)}(x)\underbrace{dx...dx}_{l-2}\\ \varphi_2^{(l)}(x)=...=\varphi_{l-1}^{(l)}(x)=x\end{cases};\quad \overline{\varphi}_n^{(l)}(x)=\varphi_n^{(l)}(1-x).\quad (1)$$

Закон распределения L_n^+ имеет вид $P\{L_n^+=l\}=P\{L_n^+=l\}=v_n(l)=q_n^{(l+1)}-q_n^{(l)}$. Числовые характеристики и границы доверительных интервалов для $L_n=\max\{L_n^+,L_n^-\}$ посчитанные согласно (1) с последующим удвоением, приведены в таблице 1. [2]. Используя интегральное представление, стационарную вероятность формирования L_n^+ получаем в виде $P\left\{*\,0\underbrace{1...1}_{l-1}0\,*\right\}=\int_0^1\int_x^1\underbrace{\int_0^x...\int_0^x}_{l-1}\int_x^1 dx=\frac{l^2+l-1}{(l+2)!}$, и предельная форма распределения длины максимального локального тренда составит:

$$v_n(l)=\exp\left\{-(n-1)\frac{l+1}{(l+2)!}\right\}-\exp\left\{-(n-1)\frac{l}{(l+1)!}\right\},2\le l\le n\ .\qquad (2)$$

Как показано в [3], (2) эволюционирует циклами от вырожденного при длине последовательности $n_1(l)=\lfloor(l-1)!\ln l\rfloor$ до симметричного динарного при $n_2(l)=\lfloor l!\cdot\ln 2\rfloor$.

При установлении закона больших чисел для длины максимального локального тренда воспользуемся пуассоновской асимптотикой и взаимной независимостью длинных трендовых серий. Для верхней границы получим:

$$P\{L_n > l\} = 1 - \exp\left\{-(n-1)\sum_{m>l}\left(\frac{m}{(m+1)!} - \frac{m+1}{(m+2)!}\right)\right\} = 1 - \exp\left\{-(n-1)\left(\frac{l+1}{(l+2)!}\right)\right\} < (n-1)\frac{l+1}{(l+2)!} \quad .$$

(3)

Подставив в (3) $n_1(l)$ и $l+1$, получаем оценку $P\{L_n > l+1\} < \ln(l)/(l-1)(l+3) \sim \ln(l)/l^2$.

Данный ряд сходится. Следовательно, при $n \le (l+1)!\ln(l)/(l-1)$ граница допустимых значений не превосходит $l+1$, т.е. $L_{n_1} \le l+1$. Для нижней границы получим

$$P\{L_n < l\} = \exp\left\{-(n-1)\sum_{m\ge l}\left(\frac{m}{(m+1)!} - \frac{m+1}{(m+2)!}\right)\right\} = \exp\left\{-(n-1)\left(\frac{l}{(l+1)!}\right)\right\} . \quad (4)$$

Таблица 1. Числовые характеристики и границы 90%-х доверительных интервалов для максимального локального тренда (в скобках даны границы 95%-х доверительных интервалов).

n	μ	σ	НГ	ВГ	n	μ	σ	НГ	ВГ
2	2.00	0.00	1	2	**18**	3.92	0.78	3	5(6)
3	2.33	0.47	1	3	**20**	3.99	0.78	3	5(6)
4	2.67	0.62	1	4	**25**	4.14	0.77	3	5(6)
5	2.90	0.68	1	5	**30**	4.27	0.77	3	6
6	3.08	0.70	2(1)	5(6)	**40**	4.45	0.76	3	6
7	3.22	0.71	2	5(6)	**50**	4.58	0.76	4	6
8	3.33	0.71	2	6	**100**	4.99	0.76	4	6(7)
9	3.42	0.72	2	6(7)	**200**	5.39	0.73	4	7
10	3.50	0.73	2	6(7)	**300**	5.61	0.72	5	7
12	3.63	0.75	2	7	**500**	5.88	0.73	5	7
14	3.74	0.76	2	7(8)	**700**	6.06	0,71	5	7(8)
16	3.83	0.77	3(2)	7(8)	**1000**	6.25	0.69	5	7(8)

Подставляя в (4) $n_2(l)$, получаем оценку вероятности выхода за нижнюю границу

$P\{n > n_2(l), L_n < l\} \sim 2^{-l}$.

Объединяя обе оценки, убеждаемся, что при $l_1 = l, l_2 = l+2$ интервалы $(l+1)!\ln(2) < n-1 < (l+3)!\ln(l+2)/(l+1)$ покрывают все множество N, пересекаясь между собой. Следовательно, согласно первой лемме Бореля - Кантелли [1], множество допустимых значений максимальной трендовой серии содержит не более четырех соседних значений: $L_n \in \{l(n), l(n)+1, l(n)+2, l(n)+3\}$. При $l_2 = l_1 + 1$ интервалы $(l+1)!\ln(2) < n-1 < (l+2)!\ln(l+1)/l$ не пусты. Следовательно, внутри каждого такого интервала множество сокращается до трех: $L_n \in \{l(n), l(n)+1, l(n)+2\}$. На Рис.1. показан отрезок экспериментальной траектории случайного блуждания L_n^+ в последовательности белого шума. Нижняя и верхняя границы L_n заданы в виде обратной функции $n_1(l) = 1 + \ln(l-2)(l-1)!/(l-3)$, $n_2(l) = 1 + \ln(2)(l+1)!$.

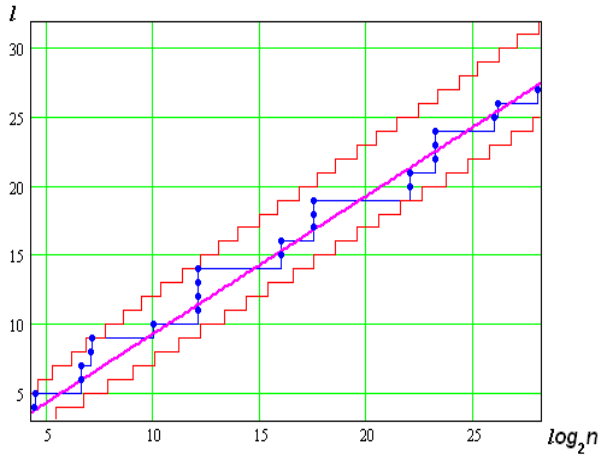

Рис.1. Отрезок траектории случайного блуждания длины максимального локального тренда.

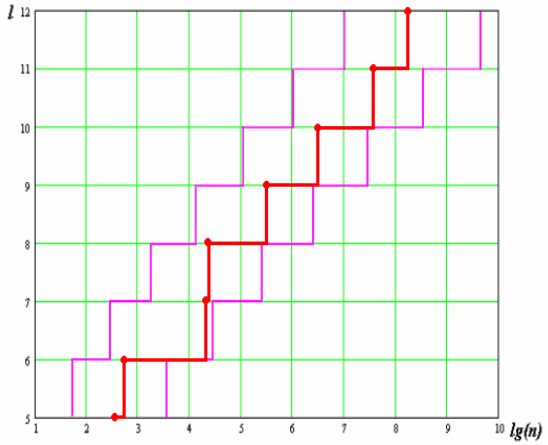

Рис.2. Отрезок траектории случайного блуждания длины максимальной серии орлов при игре в орлянку.

Кроме того, при разделении цепи кодированных последовательных разностей на четную и нечетную подпоследовательности образуются две битовых цепи, каждая из которых состоит из невзаимодействующих битов, т.е. совпадает с орлянкой. Каждый бит одной цепи связан с двумя ближайшими битами соседней. Таким образом, паралельный мониторинг максимальной серии в цепи кодированных разностей;, а так же в её нечетной и четной подпоследовательностях образует шесть фильтрующих ступеней, повышая тем самым надежность теста.

Библиографический список

1. В. Феллер. Ведение в теорию вероятнностей и её приложения т.1, М. Мир, 1984г.
2. А.Н.Плотников. Элементарноая теория анализа и статистическое моделирование временных рядов. ЛАНЬ, С-Пб., 2016г.
3. А.Н.Плотников. Ободном парадоксе закона больших чисел для максимальных серий в последовательной выборке Известия СНЦ РАН, 2008, вып.1, с. 122-126.