УДК 621.391.7

Дважды адаптивный тест для проверки гипотезы о равномерном распределении

В. А. Монарев*

Предлагается новый статистический тест для проверки генераторов случайных и псевдослучайных чисел. Приведены результаты сравнения нового теста с тестами, предложенными Национальным институтом стандартов и технологий США, а также с тестами «стопка книг» и «адаптивным» тестом. Показано, что новый тест на некоторых представляющих интерес генераторах эффективней, чем эти ранее известные тесты. В работе приведены результаты сравнительного тестирования известных генераторов псевдослучайных чисел.

Ключевые слова: генератор псевдослучайных чисел, генератор случайных чисел, статистический тест, проверка на случайность.

1. Введение

Генераторы случайных и псевдослучайных чисел (RNG и PRNG) находят широкое применение в различных областях: моделировании процессов, защите информации и других. Поэтому актуальна задача проверки качества этих генераторов с помощью статистических тестов. Одними из самых известных статистических тестов являются тесты, предложенные Национальным Институтом стандартов и технологий США (NIST), который в 2001 году опубликовал первую версию пакета программ для проверки генераторов случайных и псевдослучайных чисел [1]. В 2005 году опубликована работа [2], в которой описаны тесты, названные «адаптивный» и «стопка книг», которые могут находить отклонения от случайности лучше, чем тесты NIST. Статистические тесты широко используются для проверки криптостойких PRNG (см. [3]–[4]). Существуют криптоаналитические атаки, базирующиеся на статистических тестах (см. [5]–[7]). В данной работе описан тест, для которого показано, что он может находить отклонения от случайности лучше, чем тесты из [1] и [2]. Предварительные сведения о новом тесте были представлены в [12].

2. Описание теста

Для описания предлагаемого теста введем необходимые обозначения. Пусть дана последовательность символов $x_1, x_2, ...$ из алфавита $A = \{0, 1\}$. Требуется по выборке проверить гипотезу H_0 о том, что последовательность порождена источником Бернулли и $P(x_i = 0) = 1/2$ (для всех i), против альтернативной гипотезы H_1, являющейся отрицанием H_0. Как правило, при тестировании выборка разбивается на блоки длины s : $x_1, x_2, ..., x_s; x_{s+1}, ..., x_{2s}; ...$, и проверяется гипотеза H_0^*, что эти блоки имеют равномерное распределение на множестве натуральных чисел $\{0, 1, ..., 2^s - 1\}$. Основная сложность при проверке данной гипотезы возникает при больших значениях s (например, 56 и больше), т. к. для применения многих тестов требуется длина выборки, пропорциональная 2^s, то есть размеру алфавита (например, для теста хи-квадрат и других, см. [1]). Данный тест предназначен для проверки гипотезы H_0^* при больших s и относительно малом объеме выборки, пропорциональном $2^{s/3}$.

*Работа поддержана грантом РФФИ, проект № 14-01-31484 (мол_а) .

Далее полагаем, что выборка $x_1, x_2, ..., x_n$ из алфавита $A = \{0, 1, ..., 2^s - 1\}$ и $|A| = S$. Разобьем выборку на три части размером $m, k, n-k-m$: $x_1, x_2, ..., x_m$; $x_{m+1}, x_{m+2}, ..., x_k$ и $x_{k+1}, x_{k+2}, ..., x_n$, где $n < S$. Первые две части назовем «обучающими» (по аналогии с [2]). Обозначим через B множество чисел, которые встретились в первой части выборки, или формально $B = \{b | b = x_i, i < m + 1\}$. Полагаем, что множество $B = \{b_1, ..., b_{m'}\}$, и оно упорядочено по возрастанию.

Обозначим через R специальный параметр теста (о принципе выбора чисел m, k и R будет сказано ниже). Полагаем, что множество B удовлетворяет следующим условиям:

1) $b_1 > R$;

2) $b_{i+1} - b_i < 2R$;

3) $b_{m'} < S - R$.

Если при заданном R данные условия не выполняются, то удалив из множества B часть элементов, добьёмся выполнения условий.

Второй этап обучения происходит по следующему принципу. Обрабатываем вторую часть выборки $x_{m+1}, x_{m+2}, ..., x_{m+k}$ и формируем множество C по алгоритму:

1. Находим расстояние от x_{m+1} до ближайшего элемента из B (обозначим это расстояние через r_{m+1}) по формуле:

$$r_{m+1} = \min_{1 \le i \le m'} | x_{m+1} - b_i | .$$

2. Если $r_{m+1} < R$, то помещаем r_{m+1} в множество C.

3. Переходим к элементу x_{m+2} и так далее до x_{m+k}.

Полагаем, что 0 содержится в множестве C. По аналогии с адаптивным тестом (называемым RSS, см. [2]) по обучающей части выборки с помощью множеств B и C мы задаем некоторое подмножество алфавита (назовем его D) и проверяем по проверочной части, что вероятность попасть в это множество не отклоняется от теоретического значения. Множество B состоит из элементов алфавита, множество C определяет окрестность этих элементов. Отметим, что по построению эти окрестности не пересекаются. Множество D состоит из всех элементов алфавита, которые удалены от элементов множества B на расстояние C. Легко убедиться, что если верна гипотеза H_0, то вероятность попасть в множество D равна $P^* = 2|B|(|C| - 1)/S$. Далее по третьей части выборки $x_{m+k+1}, x_{m+k+2}, ..., x_n$ проверяем это предположение. Считаем величину ν по следующему алгоритму.

Инициализация алгоритма: полагаем ν равным нулю.

1. Находим расстояние от x_{m+k+1} до ближайшего элемента из B (обозначим это расстояние через r_{m+k+1}).

2. Если число r_{m+k+1} содержится в множестве C, то ν увеличиваем на единицу.

3. Переходим к элементу x_{m+k+2} и т.д.

Ясно, что ν – это частота попадания элементов третьей части выборки в множество D. Если выполнена гипотеза H_0, то вероятность того, что при обработке элемента выборки x частота ν увеличится, равна $P^* = 2|B|(|C| - 1)/S$. Далее, по критерию хи-квадрат проверяется гипотеза H_0^*, что $P^* = 2|B|(|C| - 1)/S$, против альтернативной гипотезы $H_1^* = H_0^*$. Напомним, что при применении критерия хи-квадрат вычисляется величина

$$x^2 = \frac{(\nu - NP^*)^2}{NP^*} + \frac{(N - \nu - N(1 - P^*))^2}{N(1 - P^*)},$$

где N в нашем случае равно $n - k - m$. Известно, что распределение случайной величины x^2 асимптотически приближается к распределению хи-квадрат с одной степенью свободы.

Поскольку процедура обучения нового теста состоит из двух этапов, то назовем новый тест «дважды адаптивным». В таблицах он будет обозначен, как TAT (”twice adaptive test“).

3. Экспериментальное сравнение нового теста с ранее известными методами

В этом разделе мы сравниваем эффективность предлагаемого теста с методами из [1]. Методы из [1] рекомендованы для практического тестирования (псевдо)случайных последовательностей Национальным институтом стандартов США (NIST). Также новый метод сравнивался с тестами «стопка книг» (в таблицах обозначим его через BS) и RSS из [2], где было показано, что данные тесты («стопка книг» и RSS) могут находить отклонения от случайности эффективней, чем тесты из [1]. Большинство рассматриваемых генераторов относятся к линейно-конгруэнтным (LCG). С их помощью получают последовательность целых чисел X_n из диапазона от 0 до $m-1$, где m – параметр. Линейно-конгруэнтный генератор полностью определяется с помощью четырех параметров a, b, m, X_0 по формуле:

$$X_n = (a \cdot X_{n-1} + b) \mod m.$$

Известно, что старшие биты чисел, порождаемых по этой формуле, часто далеки от случайно распределенных, поэтому обычно рекомендуется использовать только младшие биты в качестве случайных чисел (см. [8]). Более подробно процедура извлечения случайных бит описана в [2]. Следуя этой рекомендации, из порождаемых генератором значений выделялся «старший байт» (см. [2] или [11]). Каждый метод применялся к тестированию тридцати выборок (различной длины) и подсчитывались величины Q_α, равные количеству случаев, когда значение статистики x^2 превышало квантиль порядка α распределения этого критерия. В табл.1 приведены результаты тестирования с помощью нового адаптивного теста (TAT) и методов из [1] и [2]. Параметры генераторов LCG-4 и LCG-16 находятся в табл.2. Приведены результаты для выборок длины 2^{20}, 2^{23} и 2^{26} бит (по 10 выборок для каждой длины). В табл.1 указано, для какого числа выборок значение статистики x^2 превысило квантили порядка 0.99 и 0.9999. Из результатов видно, что новый тест может находить отклонения от случайности на выборках меньшего размера, чем другие тесты. Например, последовательность, полученная с помощью генератора LCG-4, на выборке 2^{20} бит будет признана неслучайной, если использовать тест TAT. Для других же тестов требуется выборка больше в 64 раза. Коротко остановимся на выборе параметров для нового теста. Во всех тестах выборка делилась на три равные части. Размер блока s выбирался максимально возможным для данного размера выборки (ограничение $2|B||C|(n-k-m)/S > 5$, см. [1], [2], [8]). После формирования первоначального множества B вычислялось среднее расстояние между соседними элементами множества B, и параметр R приравнивался этому значению.

4. Анализ практически используемых псевдослучайных генераторов

Приведем результаты применения нового метода к тестированию некоторых LCG генераторов. В табл.2 приведен список параметров генераторов и длины последовательностей (в битах), при которых тесты превышали квантиль порядка 0.999. Были проверены выборки длиной до 2^{40} бит. Если генератор проходил тест на данной длине, то в таблицу заносили символ «-». Из таблицы видно, что новый тест требует выборки существенно меньшей длины, чем тесты RSS и «стопка книг» (см. [2]). Данные генераторы были проверены в [9] с помощью серии тестов TestU01 при различных выборках. Генераторы LCG-8 и LCG-10 прошли все тесты при длине 2^{36} бит, то есть новый тест может быть эффективней всех методов, которые описаны в [9] и [2]. Кроме LCG с помощью нового теста был проверен генератор BBS. Это известный криптостойкий генератор случайных чисел [10]. Случайные биты извлекаются из

младших значащих бит последовательности, полученной по формуле:

$$X_n = X_{n-1}^2 \mod M,$$

где $M = P \cdot Q$, P и Q – простые числа.

Таблица 1. Сравнение эффективности тестов NIST с другими методами.

Название теста	$Q_{0.99}/Q_{0.999}$					
	LCG-4			LCG-16		
	2^{20}	2^{23}	2^{26}	2^{20}	2^{23}	2^{26}
TAT	10/6	10/10	10/10	0/0	10/10	10/10
BS	1/0	0/0	10/10	0/0	1/0	10/10
RSS	0/0	0/0	10/7	0/0	0/0	0/0
Frequency	0/0	0/0	0/0	0/0	0/0	0/0
Block Frequency	0/0	0/0	0/0	0/0	0/0	1/0
Cumulative Sums	0/0	0/0	0/0	0/0	0/0	0/0
Runs Longest	0/0	0/0	0/0	0/0	0/0	10/0
Run of Ones	0/0	0/0	0/0	0/0	0/0	0/0
Rank	0/0	0/0	0/0	0/0	0/0	0/0
Discrete Fourier Transform (DFT)	0/0	0/0	10/10	0/0	0/0	2/0
Nonperiodic Template Matchings	0/0	0/0	0/0	0/0	0/0	0/0
Overlapping Template Matchings	0/0	0/0	3/0	0/0	0/0	3/0
Universal Statistical	0/0	0/0	0/0	0/0	0/0	0/0
Approximate Entropy	0/0	0/0	0/0	0/0	0/0	0/0
Random Excursions Random	0/0	0/0	0/0	0/0	0/0	0/0
Excursions Variant	0/0	0/0	0/0	0/0	0/0	0/0
Serial	0/0	0/0	0/0	0/0	1/0	0/0
Lempel–Ziv Complexity	0/0	0/0	0/0	0/0	0/0	0/0
Linear Complexity	0/0	0/0	0/0	1/0	0/0	0/0

В данной работе использовался упрощенный вариант BBS, число M уменьшено и число извлекаемых бит из X_i увеличено до 8. Рассмотрены два варианта: $M - 32$ бита и 48 бит. Показано, что тест TAT находит отклонения от случайности на длинах выборки 2^{25} и 2^{31} бит соответственно. Также экспериментально установлено, что из всех тестов, предложенных NIST, только тест DFT смог обнаружить отклонения для 32-битного BBS, но при увеличении M до 48 бит тесты NIST не находят отклонений. Тесты «стопка книг» и RSS также не находят отклонений. Отметим, что необходимо, чтобы параметр s при тестировании BBS с помощью TAT был равен 48 и 64 бит. Таким образом, можно сделать предположение, что в случае 1024-битного варианта BBS (M – 1024 бита) параметр s должен быть равен 1040, откуда следует, что необходима выборка около 2^{360} бит.

Данные результаты показывают, что новый тест может находить отклонения от случайностей у ряда генераторов эффективней, чем методы, описанные в [1], [2] и [9]. Более того, при длине выборки 2^{31} бит тесты из [1] позволяют проверять гипотезу H_0^*, если параметр s

меньше 25, из [2] – если s меньше 49. Для нового же теста при такой длине выборки можно полагать значение параметра s равным 64.

Т а б л и ц а 2. Сравнение эффективности тестов TAT, BS и RS

Название	a	b	m	TAT	BS	RS
LCG-1	69069	1	2^{32}	2^{20}	2^{26}	2^{26}
LCG-2	1099087573	0	2^{32}	2^{19}	2^{24}	2^{24}
LCG-3	5^{13}	0	2^{46}	2^{26}	2^{34}	2^{34}
LCG-4	25214903917	11	2^{48}	2^{28}	2^{33}	2^{34}
LCG-5	33952834046453	0	2^{48}	2^{28}	2^{33}	2^{33}
LCG-6	44485709377909	0	2^{48}	2^{28}	2^{33}	2^{33}
LCG-7	13^{13}	0	2^{59}	2^{30}	-	-
LCG-8	5^{19}	1	2^{63}	2^{34}	-	-
LCG-9	5^{19}	1	2^{48}	2^{28}	2^{33}	2^{33}
LCG-10	9219741426499971445	1	2^{63}	2^{34}	-	-
LCG-11	16807	0	$2^{31}-1$	2^{22}	2^{27}	2^{28}
LCG-12	$2^{15}-2^{10}$	0	$2^{31}-1$	2^{21}	2^{27}	2^{27}
LCG-13	397204094	0	$2^{31}-1$	2^{22}	2^{25}	2^{26}
LCG-14	742938285	1	$2^{31}-1$	2^{22}	2^{25}	2^{25}
LCG-15	950706376	0	$2^{31}-1$	2^{22}	2^{24}	2^{24}

Литература

1. *Rukhin A. and others* A statistical test suite for random and pseudorandom number generators for cryptographic applications // NIST Special Publication 800-22. `http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf`
2. *Ryabko B., Monarev V.* Using information theory approach to randomness testing //Journal of Statistical Planning and Inference, 2005, v. 133, n.1, pp. 95–110.
3. *Ryabko B. Ya., Stognienko V. S., Shokin Yu. I.* A new test for randomness and its appli-cation to some cryptographic problems // Journal of Statistical Planning and Inference, 2004, v. 123, n. 2 pp. 365–376.
4. *Filiol E.* A New Statistical Testing for Symmetric Ciphers and Hash Functions // Lecture Notes in Computer Science, vol. 2513/2002, 2002, pp 342–353.
5. *Рябко Б. Я., Монарев В. А., Шокин Ю. И.* Новый тип атак на блоковые шифры // Проблемы передачи информации, т. 41, н.4, 2005, с.181–182.
6. *Knudsen L., Meier W.* Correlations in RC6 with a reduced number of rounds // FSE 2000, LNCS 1978(2000), Springer-Verlag, 94–108.
7. *Miyaji A., Nonaka M.* Evaluation of the security of RC6 against the χ^2- attack // IEICE Trans. Fundamentals, vol.E88-A, No.1, 2005.
8. *Knuth D. E.* The Art of Computer Programming, volume 2: Semi numerical Algorithms // Addison-Wesley, Reading, MA, 2nd edition, 1981.

9. *L'Ecuyer P., Simard R.* TestU01: A C Library for Empirical Testing of Random Number Generators // ACM Transactions on Mathematical Software, 33, 4, Article 22, 2007.
10. *Menezes A.* et al., Handbook of Applied Cryptography // CRC Press, Inc., 1997.
11. *Монарев В. А., Рябко Б. Я.* Экспериментальный анализ генераторов псевдослучайных чисел при помощи нового статистического теста // Ж. вычисл. матем. и матем. физ., 44:5 (2004), 812–816.
12. *Монарев В. А.* Новый статистический тест для проверки криптостойких генераторов случайных чисел // Труды XI Международной научно-практическая конференции «Информационная безопасность 2010», 103–108.

Статья поступила в редакцию 23.11.2015;
переработанный вариант – 16.12.2015.

Монарев Виктор Александрович
к.ф.-м.н., научный сотрудник ИВТ СО РАН (630090, г. Новосибирск, просп. Академика Лаврентьева, 6), тел. (383) 330-61-50, e-mail: viktor.monarev@gmail.com .

Twice adaptive method of random testing

V. Monarev

This paper presents a new method for random testing. The results comparing the new test with the test proposed by NIST, USA are provided. It is shown, that the new test, being used on some generators, is more effective than the previously known tests. The paper presents the results of benchmark testing of pseudorandom number generators (PRNG).

Keywords: randomness, statistical testing.