Методологический подход к оценке качества случайных чисел и последовательностей

Г. П. Акимова, Е. В. Пашкина, А. В. Соловьев

В статье изложен методологический подход к определению вероятности формирования различными генераторами случайных чисел и последовательности случайных чисел на примере лототронов.

Введение

Хорошо известны различные жеребьевки и лото, проводящиеся по принципу выпадения случайных чисел. Самый простой из них — игральная кость с шестью гранями, более сложный — лототрон с хитрой системой бесконтактной загрузки и перемешивания шаров с помощью сложной пневматики. Все эти устройства предназначены для того, чтобы выпавший номер или шар был случайным, или, по крайней мере, выглядел таким.

В последнее время в нашей стране на случайности выпадения номера при использовании лототрона строится ряд технологий принятия решения. В частности, в МГУ в 2007 году определение комплекта заданий по математике, тем сочинений и заданий по обществознанию, а также ряду экзаменов по иностранному языку, проходило по системе лототрона [7]. Аналогичные мероприятия проводились в различных регионах России. В ноябре 2007 г. механический лототрон, специально приобретенный ЦИК, использовался при проведении жеребьевки для установления порядка, в котором партии будут следовать в избирательных бюллетенях. На прошлых федеральных выборах для этого использовался электронный аппарат. «Раньше машина, предварительно перемешав шары, сама „выкидывала“ один из них. Теперь лототрон крутили вручную, а представители

политических партий в присутствии членов ЦИК и журналистов сами по очереди вытаскивали пластиковые шары со скрытыми в них номерами» [8].

Но тогда возникает вопрос, как проверить, что выпавший номер в лото или последовательность номеров при жеребьевке, действительно получены случайным образом. С одной стороны любая последовательность выпавших чисел будет случайной, хотя бы потому, что случайной может быть любая последовательность чисел. С другой стороны, если в процессе работы генератора случайных чисел выпадают всегда только определенные числа, то возникает подозрение в некоей закономерности таких выпадений.

В настоящее время существуют серьезные организации, например, Национальный Институт Стандартов и Технологий США (НИСТ) [1, 2], которые разрабатывают Руководства по проведению статистических испытаний генераторов последовательностей псевдослучайных чисел. Таких испытаний стандартно около двух–трех десятков, расчеты по данным руководствам занимают достаточно много времени.

В данной статье предлагается методология сравнительно быстрой проверки генераторов случайных чисел и последовательностей, которая может выполняться при ограниченных материальных и временных ресурсах с помощью несложных программ обработки результатов статистических испытаний генераторов случайных чисел. Для более точной проверки наличия скрытых зависимостей необходимо дополнительно использовать тесты NIST и критерии Колмогорова—Смирнова, Андерсона—Дарлинга, Жака—Бера, Шапиро—Вилка [11].

1. О подходе к оценке качества случайных чисел и последовательностей

Для начала определим, что под генератором случайных или псевдослучайных чисел понимается любая программа или устройство, которое с достаточно высокой вероятностью будет производить случайные числа или последовательности случайных чисел, описать которые какими-либо закономерностями, по крайней мере, затруднительно, если не невозможно.

Согласно [9, 10] случайные и псевдослучайные числа — это числа, которые могут рассматриваться в качестве реализации некоторой случайной величины. Как правило, имеются в виду реализации случайной величины, равномерно распределенной на промежутке (0, 1), или приближения к таким реализациям, имеющие конечное число цифр в своем представлении.

При такой узкой трактовке случайное число можно определить как число, составленное из случайных цифр. Случайная цифра в p-ричной системе счисления является результатом эксперимента с p равновероятными исходами (каждому из исходов соответствует одна из p цифр).

Оценить одно отдельно взятое число на случайность, конечно невозможно, поэтому в любом случае речь пойдет об оценке некоторой последовательности чисел. Далее, при упоминании оценки случайных чисел, мы будем иметь в виду оценку выпадения одного числа из некоторого ряда чисел (например, первого шара в лото). Назовем это экспериментом типа «лото». Под последовательностью случайных чисел будем иметь в виду порядок выпадения всех чисел последовательности (например, шаров при жеребьевке, когда от номера шара, например, зависит порядковый номер какого-либо действия, выступления участника и т. д.). Назовем это экспериментом типа «жеребьевка».

При этом будем рассматривать только случай, когда последовательности чисел выбираются из конечного ряда простых чисел (например, от 1 до 16 включительно).

Достаточно сложно оценить качество компьютерной программы, производящей генерацию случайных чисел и последовательностей. Великий русский математик А. Н. Колмогоров [3] так сформулировал требование к такой программе: программа генерации случайных последовательностей не может быть короче самой последовательности случайных чисел. Пожалуй, сложно что-либо добавить к такому подходу.

Как же можно оценить качество последовательностей чисел с точки зрения их случайности? Как было сказано выше: любая последовательность чисел может быть случайной, так как случайной может быть любая последовательность чисел.

В данной статье авторы предполагают, что единственным способом оценки того, что последовательности чисел получаются действительно случайными, является проведение вероятностного анализа этих последовательностей на отсутствие каких-либо «предпочтений» в выпадении чисел в последовательности и отсутствие явных периодических закономерностей в таких числах.

Такой анализ, как правило, дает весьма приблизительную оценку и полностью не гарантирует, что последовательность чисел перед нами действительно случайная. Однако, может отсечь многие грубые подтасовки и ошибки, которые не заметны простым наблюдением.

Наверное, многие помнят, что во времена СССР была игра «Спортлото», причем наиболее популярной была игра «5 из 36». В работе [4] приводятся результаты около 6,9 МИЛЛИАРДОВ попыток угадать выиг-

рышные комбинации в тиражах Спортлото «5 из 36» за 12 лет, причем обнаружено систематическое превышение экспериментальной вероятности угадывания над теоретической с доверительной вероятностью 99 %.

2. Методы быстрой проверки качества случайных чисел и последовательностей

Что же можно предложить для быстрой проверки сформированных случайных чисел и последовательностей простых рядов чисел (например, от 1 до 16)?

Во-первых, определяющим принципом проверки должно являться формирование случайных последовательностей чисел (номеров шаров) в серии испытаний. Исследуются зависимости: генерация случайных чисел, генерация случайных последовательностей.

Во-вторых, для механических устройств генерации случайных чисел, например, лототронов, должны быть исследованы, хотя бы приблизительно, весовые и геометрические характеристики шаров для исключения возможности влияния физических и аэродинамических свойств на генератор случайных чисел.

В-третьих, желательно для исследования случайных чисел выбирать количество вариантов выпадения чисел (число шаров для лототрона) из ряда чисел 2^K. Это необходимо для удобства разложения чисел в двоичную форму (почему, будет понятно далее из текста).

И, наконец, нужно определить достаточное количество статистических испытаний для проведения оценки. Необходимо заметить, что от количества таких испытаний зависит точность оценки вероятности подтверждения гипотезы о случайности последовательности чисел, формируемых данным генератором случайных чисел.

Статистические испытания (метод Монте-Карло [9, 10]) характеризуются основными параметрами:

Δ — заданная точность эксперимента;

P — вероятность достижения заданной точности;

M — количество необходимых экспериментов для получения заданной точности с заданной вероятностью.

Определим необходимое количество экспериментов M:

$(1 - \Delta)$ — вероятность того, что при одном испытании результат не достигает заданной точности Δ;

$(1 - \Delta)$ N — вероятность того, что при M испытаниях мы не получим заданной точности Δ.

Таблица 1

Определение количества испытаний

Точность Δ	Вероятность P получения заданной точности Δ			
	0,8	0,9	0,95	0,99
0,1000	16	24	32	48
0,0500	32	48	64	96
0,0250	64	96	128	192
0,0125	128	192	320	512
0,0063	320	512	640	960

Тогда вероятность получения заданной точности P и необходимое минимальное количество испытаний M можно найти по формулам:

$$P = 1 - (1 - \Delta)^M$$

$$M = \frac{\log(1 - P)}{\log(1 - \Delta)}$$

В табл. 1 приведено минимальное количество испытаний (M), которые необходимо провести, чтобы получить заданную точность эксперимента (Δ) с заданной вероятностью (P). По данной таблице определяется количество испытаний для экспериментов типа «лото» и «жеребьевка».

Для дальнейшей обработки статистики необходимо провести эксперименты типа «жеребьевка» и «лото», результаты экспериментов записать в табл. 3 и 2 соответственно. В табл. 2 для каждой из M попыток в колонки друг за другом заносятся выпавшие числа из ряда от 1 до N при последовательной выборке всех чисел ряда (в табл. 2 $N = 16$). А во вторую колонку табл. 3 — первое выпавшее число в каждом эксперименте из ряда от 1 до N.

После проведения необходимого количества испытаний типа «лото» и «жеребьевка» необходимо провести обработку полученных результатов, при этом необходимо провести на основе полученных экспериментальных данных (табл. 2 и 3) серию приведенных ниже тестов. Тесты приведены в порядке возрастания сложности, при этом отрицательный результат на любом из этапов считается достаточным, что бы признать испытуемый генератор случайных чисел непригодным.

1. Наиболее простой проверкой на случайность является проверка гипотезы равномерного распределения случайной величины, т. е. равной

Таблица 2

Таблица результатов эксперимента «жеребьевка»

№ п/п	Порядковый номер числа															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
...	.....															
M																

Таблица 3

Номер попытки	Значение выпавшего числа
...	.....
M	

вероятности выпадения чисел. Проще всего провести такую проверку, если сравнить расчетную и теоретическую вероятности выпадения всех N чисел из простого ряда от 1 до N, формируемых генератором случайных чисел (табл. 3).

Считается, что генератор случайных чисел является таковым с вероятностью не менее 90 %, если расчетная вероятность выпадения для всех чисел P_i не превысила правой или левой границы доверительного интервала $\Delta P_i'(90\%)$.

Прогностическая вероятность такого выпадения определяется как $P_i = n_i/M$, где n_i — частота выпадения числа в M случаях.

Теоретическая вероятность выпадения каждого числа определяется как $P_i' = 1/N$ для всех $i = [1, N]$, где N — количество чисел. На основании этой вероятности определяется доверительный интервал

$$\Delta P_i'(90\%) = \left(\frac{1}{N + \frac{1}{2\sqrt{3}}(N-1)}, \frac{1}{N - \frac{1}{2\sqrt{3}}(N-1)} \right).$$

Пример использования данного теста показан на рис. 1. В частности, из рисунка следует, что шар лототрона с номером 11 по неизвестным при-

Рис. 1. Пример сравнения расчетной и теоретической вероятности выпадения чисел для каждой выборки (колонки) чисел по табл. 2

чинам выпадает чаще остальных. Такое поведение шара на достаточно большом количестве экспериментов наводит на мысль, что его физические или аэродинамические характеристики чем-то отличаются от других шаров.

2. Более надежной проверкой равномерности распределения является проверка, учитывающая не только сами значения измеренных частот выпадения тех или иных значений случайной величины, но и распределение отклонений этих значений от ожидаемых теоретических значений. Наиболее распространенным критерием такой проверки является критерий Пирсона (χ^2 — Хи-квадрат).

При проверке рассчитывается:

$$\chi^2 = \sum_{i=1}^{N} \frac{(n_i - n_i')^2}{n_i'},$$

где n_i и n_i' эмпирические и теоретические частоты выпадения числа с соответствующим номером i (от 1 до N, где N — количество чисел) для каждой последовательности случайных чисел (одна колонка табл. 2).

После проверки 1, впрочем, достаточно приблизительной, можно воспользоваться данной проверкой по критерию Пирсона, при этом одновременно повысив доверительную вероятность.

Рис. 2. Пример расчетов по критерию Пирсона для каждой выборки (колонки) чисел по табл. 2

Считается, что генератор случайных чисел является таковым с вероятностью не менее 95 %, если рассчитанное значение χ^2 для всех N чисел не превысило критические точки распределения χ^2 для доверительной вероятности 95 % и $k = N - 2 - 1$ (k — число степеней свободы, 2 — число параметров, по которому оценивается равномерное распределение, 1 — константа в критерии Пирсона). Таблицы критических значений χ^2 можно посмотреть в любом справочнике по статистике, например [5].

3. Дополнительным критерием проверки является оценка математического ожидания (среднего значения) каждой выборки случайных чисел. Такая проверка позволяет исключить смещения «центра масс» измерения в сторону больших или меньших чисел, т. е. исключить возможность того, что при отсутствии предпочтения на конкретное число в целом, к примеру, большие числа, будут выпадать чаще.

При проверке предполагается, что каждая колонка в табл. 2 представляет собой случайную последовательность целых чисел W_i, с равномерным распределением на отрезке $[0, N]$ (так как позиция числа в каждой реализации должна быть случайной). Экспериментально измеренное математическое ожидание такой выборки определяется как

$$\sum_{i=1}^{M} \frac{W_i}{M},$$

Рис. 3. Пример оценки математического ожидания для каждой выборки (колонки) чисел по табл. 2

теоретическое же математическое ожидание определяется как

$$\sum_{i=1}^{N} \frac{i}{N}.$$

Считается, что генератор случайных чисел является таковым с вероятностью не менее 90 %, если рассчитанное математическое ожидание не отклоняется от теоретического, более чем на 10 %.

4. Одной из наиболее неприятных особенностей многих разновидностей генераторов квазислучайных чисел является цикличность — тенденция повторять одни и те же значения через фиксированные промежутки. Ни один из предыдущих тестов не исключает такой возможности, поэтому при проверке величины на случайность крайне необходимо провести набор частотных тестов. Наиболее простым является частотный монобитный тест.

Для проведения этого теста сплошная последовательность чисел представляется в двоичном виде. Для этого сами числа должны быть выбраны из ряда $N = 2^{\mathrm{K}}$. Оптимальное количество N равно 16.

Считается, что генератор случайных чисел является таковым с вероятностью не менее 95 %, если соотношение нулей и единиц в двоичном

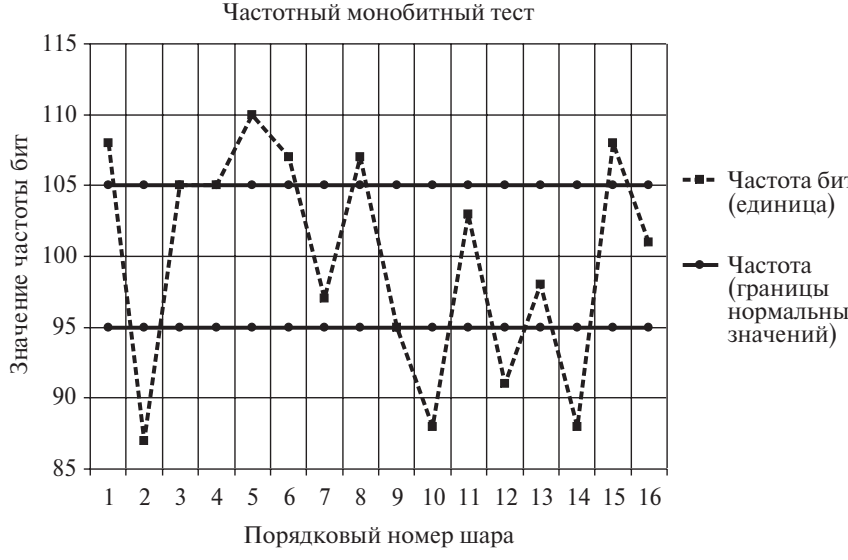

Рис. 4. Пример оценки результатов частотного монобитного теста количества единиц для каждой выборки (колонки) чисел по табл. 2

представлении весов (W_i) чисел в случайных последовательностях чисел (одна колонка табл. 2) не отличаются от среднего ожидаемого значения (общее число бит нулей и единиц, деленное на 2) более, чем на 5 % для каждой последовательности чисел.

5. Провести частотный периодический тест.

Считается, что генератор случайных чисел является таковым с вероятностью не менее 95 %, если количество и периодичность повторений непрерывных последовательностей нулей и единиц в случайных последовательностях чисел, веса которых представлены в двоичной форме, попадают в допустимый диапазон частот.

Для последовательностей 20000 бит допустимые количества последовательностей нулей и единиц представлены ниже в табл. 4 (данные по [2]).

6. Провести частотный тест на длинные последовательности.

Является дополнительным к тесту 5.

Считается, что генератор случайных чисел является таковым, если не выявлено длинных последовательностей нулей и единиц в случайных последовательностях чисел, веса которых представлены в двоичной форме. Например, для последовательности 20 000 бит не допускаются последовательности более 34 нулей или единиц подряд.

Таблица 4

Допустимое количество последовательностей

Длина последовательности нулей или единиц	Допустимое количество последовательностей
1	2267–2733
2	1079–1421
3	502–748
4	223–402
5	90–223
6	90–223

7. Провести покер-тест случайных последовательностей.

Для каждой случайной последовательности (одна колонка Таблицы 2), представленной в двоичном виде, выполнить расчет критерия:

$$\Pi_x = \frac{N \log_2 N}{L_x} \left(\sum_{i=1}^{N} (W_i - 1)^2 \right) - \frac{L_x}{\log_2 N},$$

где L_x — длина двоичной последовательности, N — количество чисел, W_i равен значению числа.

Считается, что генератор случайных чисел является таковым с вероятностью не менее 95 %, если $4{,}11 < \Pi_x < 27{,}7$ для всех N чисел (допустимые границы Π_x указаны для частного случая, когда количество чисел N равно 16, длина последовательности L_x равна 20 000 бит).

8. При высоких требованиях к работе генератора случайных чисел в качестве дополнительных проверок последовательностей чисел на случайность рекомендуется использовать также критерии Колмогорова—Смирнова, Андерсона—Дарлинга, Жака—Бера, Шапиро—Вилка, детально описанные в работе [11].

Например, критерий Колмогорова—Смирнова о проверке гипотезы однородности двух эмпирических законов распределения используется для того, чтобы определить, подчиняются ли два эмпирических распределения одному закону, либо определить, подчиняется ли полученное распределение предполагаемой модели. Критерий является одним из основных и наиболее широко используемых непараметрических методов, так как достаточно чувствителен к различиям в исследуемых выборках.

Генератор случайных чисел является таковым с высокой вероятностью, если выполнены условия успешного прохождения тестов 1–8.

Заключение

Описанная в статье методология проверки случайности последовательности чисел, выпадающих в лототроне, не является универсальным и точным методом исследования. Однако, она позволяет достаточно быстро, без особых временных затрат сделать первое приближение в расчетах и может быть использована для начальной проверки непрерывных последовательностей простых чисел на случайность.

Методология была опробована на примере двух конкретных моделях лототрона. По результатам проведенных испытаний и последующих расчетов было выявлено, что лототрон первой модели не пригоден для серьезного использования. Одним из критериев такой оценки явилось необъяснимо частое выпадение шарика с определенным номером. Такой результат оказался достаточным для принятия решения о невозможности использования лототрона без проведения более глубоких исследований. Следует отметить при этом, что при одноразовом использовании приборов подобного рода, заметить такое явление невозможно.

Результаты данной работы были использованы при выборе лототрона, с помощью которого 31 июля 2007 года на совещании с политическими партиями проводилась тренировочная жеребьевка распределения мест политических партий в избирательном бюллетене.

Литература

1. Random number generation. [Электронный ресурс] http://mandala.co.uk/links/random/
2. NIST. Cryptographic Toolkit. Random number generation. [Электронный ресурс] http://csrc.nist.gov/rng/
3. А.Н.Колмогоров. [Электронный ресурс] http://slovari.yandex.ru/search.xml?text=Колмогоров
4. А. В. Антипин. О возможности получения информации из Будущего // Физическая мысль России. 1999. № 1/2. М., 1999. С. 80–103. [Электронный ресурс] http://www.chronos.msu.ru/RREPORTS/antipin_o_vozmozhnosti/title.html
5. *Болшев Л. Н.*, *Смирнов Н. В.* Таблицы математической статистики. М.: Наука, 1983. 416 с.
6. Методика проверки лототронов. ИСА РАН, 2007.
7. Лототрон для поступающих. МК. [Электронный ресурс] http://www.mk.ru/blogs/MK/2007/07/01/srochno/297811/
8. 8. Номера партий в избирательных бюллетенях определит лототрон. РИА Новости. [Электронный ресурс] http://www.rian.ru/politics/parties/20071031/86013463.html
9. *Ермаков С. М.* Метод Монте-Карло и смежные вопросы. М., 1971.
10. *Соболь И. М.* Численные методы Монте-Карло. М., 1973.
11. Нормальное распределение. Википедия. [Электронный ресурс] http://ru.wikipedia.org/wiki/Нормальное распределение