Способен ли человек на случайность?

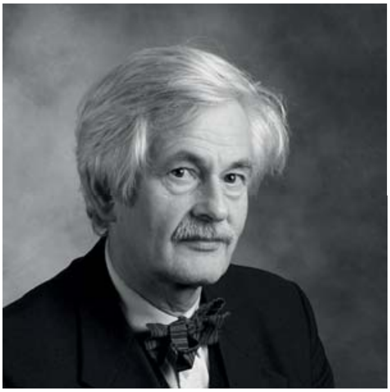
Многочисленные исследования показали, что для большинства людей задача вести себя случайно, к примеру, выписать произвольную последовательность чисел или расположить карточки в произвольном порядке, оказывается непосильной. Как правило, они не способны различать случайные и неслучайные события, по сути их восприятие смещено в определённых направлениях. Возможно, эта неспособность к распознаванию случайности заключается в неправильных представлениях о ней.

На примере правильной монеты последовательности типа ООРОРРРО кажутся более случайными, чем последовательности типа ОООООО (О – Орёл, Р – Решка), хотя оба типа могут быть сгенерированы процессом, который выбирает О или Р с одинаковой вероятностью. Этот пример часто используется, чтобы проиллюстрировать отличие нашего интуитивного понимания о случайности от нормы, установленной теорией вероятностей.

Ганс Рейхенбах был первым, кто предположил, что люди не способны генерировать случайные последовательности. Последующие исследования подтвердили этот факт. Данным вопросом заинтересовались математики, философы, а также психологи. Наиболее полный обзор экспериментов был дан **Виллемом Вагенаром**. В работе он использовал три подхода.

Ганс Рейхенбах, немецко-американский учёный

Испытуемых просили сгенерировать случайные последовательности. В серии этих тестов последователь-



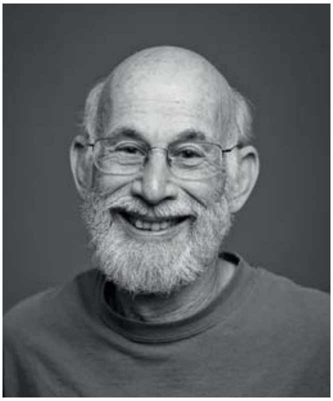
Виллем Вагенар,
голландский психолог

ности содержали разные символы (цифры, буквы), различное количество альтернатив выбора (от 2 до 26) и различную длину последовательности (от 20 до 2520). Другим подходом были эксперименты, которые заключались в том, что испытуемых просили расположить предметы (к примеру, 50 синих карт и 50 жёлтых карт) в случайном порядке. Третий подход основывался на суждении о случайности. Испытуемым показывали последовательности разной длины и просили назвать случайные.

Человек не смог справиться ни с одним из этих тестов. В ходе экспериментов было выявлено две закономерности.

Во-первых, люди предпочитают чаще чередовать символы. При этом количество одинаковых подряд идущих символов уменьшается. Вторая особенность состоит в том, что в последовательностях малой длины люди предпочитают сбалансированное появление различных символов, то есть появление их с одинаковой вероятностью.

Со временем было сформулировано несколько теорий, которые отвечали на вопрос: «Почему человек не может быть случайным?» Наиболее известная из них утверждает, что люди пытаются генерировать последовательности, которые отражают их интуитивное понятие о случайности. Однако Вагенар показал, что между тестами на генерирование случайных последовательностей и тестами на выбор случайных последовательностей связь уровня отклонения от случайности слаба. Этот вывод опровергает данную теорию. Также «неслучайное» поведение людей пытались объяснить ограниченными возможностями памяти и запоминанием предыдущих ответов, что делает невозможной независимую запись. Проанализировав каждое из этих ограничений, Вагенар нашёл их достаточно расплывчатыми. Кроме того, эмпирические данные не подтверждали ни одно из них.



Аллен Ньюрингер,
американский психолог

Аллен Ньюрингер в 1986 году показал, что за достаточно большой промежуток времени людей можно научить поступать случайно. Он составил компьютерную программу, обеспечивавшую испытуемым обратную связь по 5 или 10 статистическим оценкам случайности, например процентное отношение попыток, в которых был сделан правильный выбор, и т.п. Испытуемые должны были нажимать одну из двух кнопок на клавиатуре, а компьютер давал оценку их ответам. Сначала испытуемые начинали с неслучайных решений, но, дав несколько тысяч ответов и получив за них оценки, они смогли вырабатывать длинные ряды (до 6000), которые полностью подходили под параметры случайных последовательностей согласно всем статистическим показателям, использовавшимся Ньюрингером при составлении своей программы. Другими словами, он доказал, что люди могут вести себя случайно, но только если они специально на это натренированы.

Тест

Отличительной чертой тестов на генерацию случайных последовательностей является то, что испытуемым предстоит выполнять их без каких-либо правил, кроме одного – стараться быть случайным. Следование этому простому правилу на деле оказывается весьма сложной задачей. Генерация случайных чисел состоит как минимум из двух шагов. На первом шаге человек придумывает подходящие числа. Чаще всего они являются фрагментами цепочек, сгенерированных нашей памятью. Далее эти числа сравниваются с уже придуманной последовательностью, после чего делается выбор.

Такая картина позволяет предположить, что тест на генерирование случайных цифр может помочь выявить определённые закономерности в нашем сознании. Примерами таких закономерностей могут служить числа в порядке возрастания (0-1-2-3-...) и последовательности чётных чисел (2-4-6-8-...). Существуют и более сложные закономерности. Некоторые из них могут быть присущи культурному или индивидуальному подсознанию.

Опыт ВМК

В 2010 году Юрий Максимов под руководством профессора кафедры математической статистики В.В Ульянова провёл тест с 73 студентами факультета ВМК, 46 студентами исторического факультета и 23 студентами факультета журналистики. Рассматривались последовательности цифр от 0 до 9. При этом тест должен был удовлетворять следующим требованиям:

Испытуемых просят писать случайные последовательности цифр.

Последовательности должны быть достаточно большими.

Во время эксперимента испытуемых нельзя отвлекать.

Данные были разбиты на две группы по две выборки. В первую группу были включены 69 студентов ВМК и 69 студентов исторического факультета и факультета журналистики. Вторая группа была разделена по гендерному типу. В неё входили выборки из 50 юношей и 50 девушек. В результате у нас получились 4 выборки из 238 последовательностей. Испытуемых просили генерировать в течение пяти минут 200 цифр.

На графиках (рис. 1) показана частота цифр для данных выборок. Горизонтальной линией показана частота цифр в случае идеальной генерации цифр.

Рассмотрим зависимость между соседними числами. Запишем разность между ними: $d_i = s_{i+1} - s_i$. Обычно выделяют следующие основные характеристики:

Пары с $|d_i| = 0$ встречаются очень редко.

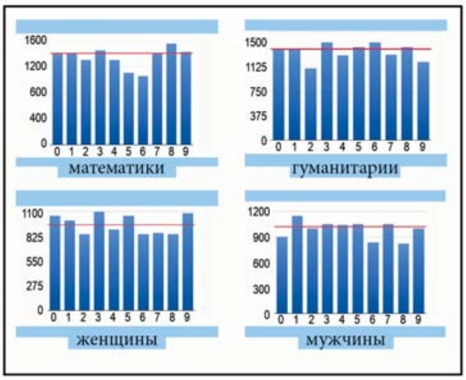


Рис. 1

Пары с маленькой разностью $|d_i|$, обычно $|d_i| = 1$ или $|d_i| = 2$, встречаются чаще, чем в случае идеальной генерации случайных чисел.

Пары со средней разностью $|d_i|$ встречаются реже, чем в случае идеальной генерации случайных чисел.

Пары с высокой отрицательной разностью $|d_i|$, к примеру $d_i = -9$, встречаются чаще, чем ожидается.

На графиках (рис. 2) показана частота d_i. Сплошной линией показан случай идеальной генерации цифр.

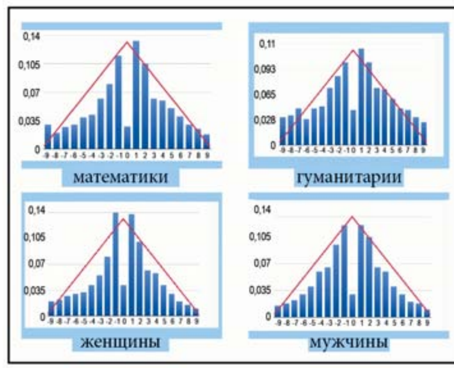


Рис. 2

Некоторые особенности случайных последовательностей

Пары с $|d_i| = 0$ встречались очень редко, что свидетельствует о том, что люди предпочитают больше альтернатив, генерируя выборки. Во всех четырёх случаях пары с маленькой разностью $|d_i|$ и пары с высокой отрицательной разностью d_i встречались чаще, чем в случае идеальной генерации случайных чисел. В гуманитарной выборке пары со средней разностью встречались чаще, чем в остальных трёх выборках. Отличительных особенностей в группе, разделённой по гендерному типу, выявлено не было. У выборки математиков наблюдается сбалансированное чередование возрастающих последовательностей и последовательности чётных чисел. Гуманитарии отдают предпочтение последним. Также в выборке математиков была замечена частая цепочка 1-8-1, в гуманитарной – 2-7-5.

Благодарим выпускника ВМК Юрия Максимова за предоставленные материалы дипломной работы и профессора кафедры математической статистики В.В. Ульянова за помощь в поиске информации.

Материал подготовила ***Маргарита Владимировна Зайцева,***
факультет ВМК МГУ им. М.В. Ломоносова.

Генерация случайных чисел

Всегда ли можно получить последовательность псевдослучайных чисел, совершая «сложные» математические операции над исходным числом?

В книге «Искусство программирования» Дональд Кнут приводит пример генератора случайных чисел, построенного им в 1959 году на основе такого предположения. Вот его алгоритм:

Пусть задано 10-значное число X.

К1. □ Присвоить Y наибольшую значащую цифру X. (Мы выполним шаги К2 – К13 точно $Y + 1$ раз, т.е. применим преобразования «случайное» число раз.)

К2. □ Присвоить Z следующую наибольшую значащую цифру X. Переходим к шагу К$(3 + Z)$, т.е. к «случайно» выбранному шагу в программе.

К3. □ Если $X < 5 \times 10^9$, присвоить X значение $X + 5 \times 10^9$.

К4. □ Заменить X серединой квадрата X (применить алгоритм фон Неймана).

К5. □ Заменить X числом $(1001001001 \times X) \bmod 10^{10}$.

К6. □ Если $X < 10^8$, то присвоить X значение $X + 9814055677$; иначе присвоить X значение $10^{10} - X$.

К7. □ Поменять местами пять младших по порядку знаков со старшими.

К8. □ Выполнить шаг К5.

К9. □ Уменьшить каждую не равную нулю цифру десятичного представления числа X на единицу.

К10. □ Если $X < 100000$, присвоить X значение $X^2 + 99999$; иначе присвоить X значение $X - 99999$.

К11. □ Если $X < 109$, то умножить X на 10.

К12. □ Заменить X на средние 10 цифр числа $X \times (X - 1)$.

К13. □ Если $Y > 0$, уменьшить Y на 1 и возвратиться к шагу К2. Если $Y = 0$, алгоритм завершён.

Программа, реализующая данный алгоритм на машинах того времени, была чрезвычайно сложной и запутанной. Тем не менее, этот метод при первом же запуске моментально сошёлся к числу, которое уже через шесть итераций вновь преобразовывалось само в себя!

Пример показывает, что не следует относиться легкомысленно к генерации последовательностей. Но какие методы используются на практике? Наиболее известным считается линейный конгруэнтный метод, предложенный Д.Г. Лемером ещё в 1949 году, но до сих пор не теряющий своей актуальности: метод входит в стандартные библиотеки многих компиляторов. Его идея состоит в использовании рекуррентной формулы

$$X_{n+1} = (aX_n + c) \bmod m.$$

Очевидно, что полученная последовательность тоже будет периодической, но длину периода можно изменять за счёт выбора конкретных параметров a, c, m. Можно показать, что длина периода в точности равна m, если выполнены условия:

- Числа c и m взаимно простые.
- Число $(a - 1)$ кратно всем простым делителям числа m.
- Если m кратно 4, то $(a - 1)$ кратно 4.

Однако оказалось, что метод не является криптографически устойчивым, т.е. можно довольно быстро вычислить параметры преобразования, исходя из полученной последовательности. Потому в 1986 году Ленор Блюм, Мануэль Блюм и Майкл Шуб предложили свой вариант генерации псевдослучайных чисел:

$$X_{n+1} = (X_n)^2 \bmod pq,$$

где p и q – два простых числа. Примечательным является тот факт, что существует явная формула для вычисления X_n. Впрочем, из-за низкого быстродействия алгоритма этот метод рекомендуется использовать только в криптографии.

Ещё один подход предложил Джордж Марсаглия в 2003 году. Члены последовательности получаются с помощью побитовых операций сдвига и исключающего «или». Приведём простой пример:

```
static int y = 123456789;
static int a = 13, b = 17, c = 5;
int xorshift()
{
     y ^= (y << a);
     y ^= (y >> b);
return y ^= (y << c);
}
```

Этот пример нуждается в доработке, чтобы успешно пройти статистические тесты. Тем не менее, он не требует больших вычислительных мощностей, а его реализация довольно проста. В настоящее время алгоритм является одним из наиболее быстрых способов получения псевдослучайных чисел.

Разумеется, всё многообразие методов не исчерпывается приведёнными здесь примерами. Каждый алгоритм имеет множество модификаций, а математики не перестают создавать новые. Ведь как говорил американский математик Роберт Кавью, «генерация случайных чисел слишком важна, чтобы оставлять её на волю случая».

Материал подготовил ***Чистяков Иван Александрович,***
студент факультета ВМК МГУ им. М.В. Ломоносова.