СТАТИСТИЧЕСКИЕ ТЕСТЫ

1. Универсальные тесты

Критерий χ^2. Критерий χ^2 с v степенями свободы позволяет оценить случайность последовательности исходов большого числа независимых случайных экспериментов, результаты которых относятся к одному из $k = v + 1$ классов (категорий). При этом используются вероятности различных исходов. Например, при одновременном бросании двух костей при игре в кости результатом является одно из 11 значений суммы выпавших чисел (от 2 до 12). При этом известны вероятности выпадения конкретных сумм, они представлены в таблице.

Сумма	$s =$	2	3	4	5	6	7	8	9	10	11	12
Вероятность	$p_s =$	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$	$\frac{5}{36}$	$\frac{1}{9}$	$\frac{1}{12}$	$\frac{1}{18}$	$\frac{1}{36}$

если бросать кости n раз, то можно ожидать, что сумма s выпадет в среднем np_s раз.

В действительности получаются несколько иные результаты, например, в одной из серий, включавшей 144 эксперимента фактическое и среднее число выпадение определенных сумм получилось следующим:

Сумма	$s =$	2	3	4	5	6	7	8	9	10	11	12
Фактическое число выпадений	$Y_s =$	2	4	10	12	22	29	21	15	14	9	6
Среднее число выпадений	$np_s =$	4	8	12	16	20	24	20	16	12	8	4

Любая последовательность может выпасть в серии испытаний, но эти последовательности имеют разные вероятности, наиболее вероятны те, для которых средние числа выпадений близки (но не полностью) совпадают со средними числами, приведенными в таблице. Степень совпадения удобно выразить, используя среднее квадратическое отклонение:

$$V = \frac{(Y_2 - np_2)^2}{np_2} + \frac{(Y_3 - np_3)^2}{np_3} + \cdots + \frac{(Y_{12} - np_{12})^2}{np_12}.$$

Обобщая, положим, что результаты испытаний распределяются по k категориям $1, 2, \ldots s \ldots k$ с вероятностями p_s, что соответствует $v = k-1$ степеням свободы. Обозначим Y_s числа испытаний, результаты которых действительно попали в категорию s. Применение всякого критерия основано на использовании

статистики – действительной функции, определенной для заданной случайной последовательности и ожидаемого распределения таких последовательностей по категориям.

Статистика для применения критерия χ^2 формулируется следующим образом:

$$V = \sum_{1 \le s \le k} \frac{(Y_s - np_s)^2}{np_s}.$$

С учетом равенств

$$Y_1 + Y_2 + \cdots + Y_k = n \quad p_1 + p_2 + \cdots + p_k = 1,$$

эту формулу можно преобразовать в следующую:

$$V = \frac{1}{n} \sum_{i \le s \le k} \left(\frac{Y_s^2}{p_s} \right) - n. \tag{1}$$

Для оценки пригодности полученной статистики пользуются таблицами T распределения χ^2. В таких таблицах строки $v = k - 1$ соответствуют числам степеней свободы, а столбцы – вероятностям p того, что $V > x$, где $x = T(v, p)$ – элемент $k - 1$-ой строки и p-го столбца,

Избранные персентильные значения приведены в таблицах 1,2. Например, $T(10, 0.05) = 18.307,\ T(10, 0.99) = 2,558$ Отсюда значение $V > 18.307$ статистики возможно лишь для 5% последовательностей случайных величин, распределенных по 11 категориям с заданным ожидаемым распределением вероятностей. С другой стороны значение статистики $V < 2.556$ возможно лишь для 1% таких последовательностей случайных величин.

Таблица 1. Избранные персентильные значения для распределения χ^2

v	$p =$ 0.100	$p =$ 0.050	$p =$ 0.025	$p =$ 0.010	$p =$ 0.005	$p =$ 0.001
1	2.705	3.841	5.024	6.635	7.879	10.828
2	4.605	5.992	7.378	9.210	10.597	13.816
3	6.251	7.815	9.349	11.345	12.838	16.272
4	7.779	9.488	11.143	13.278	14.860	18.467
5	9.236	11.070	12.833	15.086	16.750	20.516
6	10.645	12.592	14.449	16.812	18.548	22.458
7	12.017	14.067	16.013	18.475	20.278	24.322
8	13.362	15.507	17.535	20.090	21.955	26.125
9	14.684	16.919	19.023	21.666	23.589	27.877
10	15.987	18.307	20.483	23.209	25.188	29.588

Итак, проверка с помощью критерия χ^2 включает следующие этапы.

1. Проводится n испытаний, где n – достаточно велико.

2. Подсчитывается числа испытаний, результаты которых относятся к каждой из k категорий.

3. По формуле (1) вычисляется значение V статистики.

4. Число V сравнивается с числами в строке $v = k - 1$ таблицы.

5. а) Если V меньше значения, соответствующего p=99%, или больше значения, соответствующего p=1%, то результаты бракуются как недостаточно случайные.

б) Если значение V лежит между значениями, соответствующими p=99% и p=95%, или p=1% и p=5%, то результаты считаются *подозрительными.*

в) Если значение V лежит между значениями, соответствующими p=95% и p=90%, или p=5% и p=10%, то результаты считаются *слегка подозрительными.*

Часто критерий применяют к трем различным подпоследовательностям. Последовательность бракуется, если в двух случаях результат окажется подозрительным.

Критерий Колмогорова-Смирнова (КС-критерий) позволяет избежать "лингвистической"оценки результатов испытаний.

Таблица 2. Избранные персентильные значения для распределения χ^2

v	$p =$ 0.99	$p =$ 0.95	$p =$ 0.75	$p =$ 0.50	$p =$ 0.25
1	0.0002	0.004	1.102	0.455	1.323
2	0.002	0.103	0.375	1.386	2.773
3	0.115	0.352	1.213	2.366	4.108
4	0.297	0.711	1.923	3.357	5.385
5	0.554	1.146	2.675	4.351	6.626
6	0.872	1.635	3.455	5.348	7.841
7	1.239	2.167	4.255	6.346	9.037
8	1.646	2.733	5.071	7.344	10.22
9	2.066	3.325	5.899	8.343	11.39
10	2.558	3.940	6.737	9.342	12.55

В таблице 3 приведены некоторые персентильные значения для нормального распределения $N(0,1)$: если X – случайная величина имеющая стандартное нормальное распределение, то $\Pr(X > x) = p$.

Таблица 3. Избранные персентильные значения для распределения $N(0,1)$

p	0.1	0.05	0.025	0.01	0.005	0.0025	0.001	0.0005
x	1.282	1.645	1.960	2.326	2.576	2.807	3.090	3.291

2. Тесты для бинарных псевдослучайных последовательностей

Постулаты Голомба для равномерно распределенной случайной последовательности. Постулаты Голомба были одной из первых попыток формулировки необходимых условий, при которых периодическая псевдослучайная последовательность выглядит как равномерно распределенная. Эти условия далеки от того, чтобы их считать достаточными. Ниже рассматриваются бинарные последовательности, если не определено иное.

Пусть $s = s_0, s_1, s_2 \ldots$ – бесконечная последовательность. Подпоследовательность, образованную первыми n ее элементами, будем обозначать $s^n = s_0, s_1, \ldots, s_n$.

Последовательность $s = s_0, s_1, s_2 \ldots$ называется *N-периодической*, если $s_i = s_{i+N}$ для всех $i \geq 0$.

Последовательность s называется *периодической,* если она N-периодическая при некотором N. *Периодом* периодической последовательности называется наименьшее число N, для которого она N-периодическая. Если период периодической последовательности s равен N, то подпоследовательность s^N называется ее *циклом.*

Нулевой (единичный) блок последовательности s есть подпоследовательность, состоящая из нулей (единиц), которой предшествует 1 (0) и которую продолжает 1 (0). Блоком мы называем единичный или нулевой блок.

Пусть $s = s_0, s_1, s_2 \ldots$ – периодическая последовательность периода N. *Автокорреляционная функция* последовательности s определяется как целочисленная функция

$$C(t) = \frac{1}{N} \sum_{i=0}^{N-1} (2s_i - 1) \cdot (2s_{i+t} - 1),$$

для $0 \leq t \leq N - 1$.

Пусть s – периодическая последовательность периода N. *Постулаты Голомба* для равномерно распределенной периодической случайной последовательности следующие:

R1. Количества нулей и единиц в цикле s^N различаются не более, чем на единицу.

R2. В цикле s^N, не менее половины блоков имеют длину 1, не менее четверти блоков имеют длину 2, не менее восьмой доли имеют длину 4, и так далее, пока число блоков определенной длины не будет равно 1. Более того, количества нулевых и единичных блоков определенной длины почти одинаковы. (Постулат R1 является следствием данного постулата.)

R3. Автокорреляционная функция принимает ровно два значения: для некоторого целого K

$$N \cdot C(t) = \sum_{i=0}^{N-1} (2s_i - 1) \cdot (2s_{i+t} - 1) = \begin{cases} N, & \text{если } t = 0, \\ K, & \text{если } 1 \leq t \leq N - 1. \end{cases}$$

Автокорреляционная функция $C(t)$ определяет степень сходства последовательности s и последовательности, получаемой из s сдвигом на t позиций.

Бинарная последовательность, удовлетворяющая постулатам Голомба, называется *псевдо-шумовой* (*pseudo-noise*), последовательностью, или *рп-*

последовательностью. Такие последовательности порождаются линейными регистрами сдвига с обратной связью максимальной длины.

Пример 1 Последовательность s, имеющая период

$$s^{15} = 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1,$$

является pn-последовательностью:

R1: число нулей равно 7, число единиц равно 8,

R2: числа блоков длины 1,2,3 и 4 равны соответственно 4,2,1,1

R3: Автокорреляционная функция принимает два значения: $C(0) = 1$ и $C(t) = \frac{-1}{15}$ при $1 \leq t \leq 14$.

3. Пять базовых тестов

Опишем пять базовых тестов, применяемых к конечной бинарной последовательности $s = s_0, s_1, s_2, \ldots, s_{n-1}$ длины n, и определяющих, обладает ли эта последовательность некоторыми специфическими свойствами, характерными для равномерно распределенной случайной конечной последовательности. Результат тестирования имеет вероятностный характер, и прохождение последовательностью s^n всех пяти тестов не гарантирует, что она порождена генератором равномерно распределенной случайной последовательности.

Частотный тест. Этот тест определяет, действительно ли числа n_0 и n_1 нулей и единиц в последовательности S^n примерно одинаковы. Используется статистика

$$V_1 = \frac{(n_0 - n_1)^2}{n} \tag{2}$$

которая аппроксимирует распределение χ^2 с одной степенью свободы при $n \geq 10$ (на практике $n >> 10000$).

Тест проверки серий (двух битовый тест). Этот тест определяет, действительно ли числа n_{00}, n_{01} n_{10} и n_{11} подпоследовательностей 00,01,10 и 11, соответственно, в последовательности S^n примерно одинаковы, как это ожидается в равномерно распределенной последовательности. Допускается выделение подпоследовательностей с перекрытием, поэтому $n_{00} + n_{01} + n_{10} + n_{11} = n - 1$. Используется статистика

$$V_2 = \frac{4}{n-1}(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2) - n + 1, \tag{3}$$

, которая аппроксимирует распределение χ^2 с двумя степенями свободы, если $n \geq 21$.

Покер-тест (проверка комбинаций). Пусть m – положительное целое, такое, что $\lfloor \frac{n}{m} \rfloor \geq 5 \cdot (2^m)$ и $k = \lfloor \frac{n}{m} \rfloor$. Разобьем последовательность s на k не перекрывающихся частей длины m каждая. Обозначим n_i числа встречаемости частей i-го типа, $1 \leq i \leq 2^m$. Покер-тест проверяет гипотезу о том, что части различного типа встречаются в последовательности примерно одинаковое количество раз, как это ожидается от равномерно распределенной последовательности. Используется следующая статистика:

$$V_3 = \frac{2^m}{k} \left(\sum_{i=1}^{2^m} n_i^2 \right) - k \tag{4}$$

которая аппроксимирует распределение χ^2 с $2^m - 1$ степенями свободы.

Проверка блоков. Тест проверяет гипотезу о том, что количества блоков различной длины соответствуют количествам, ожидаемым в равномерно распределенной случайной последовательности.

Ожидаемое в равномерно распределенной последовательности количество e_i блоков длины i равно $e_i = \frac{n-i+3}{2^{i+2}}$. Обозначим k наибольшее целое, для которого $e_k \geq 5$. Пусть B_i и G_i количества единичных и нулевых блоков длины i, $1 \leq i \leq k$ в последовательности s.

Используется следующая статистика

$$V_4 = \sum_{i=1}^{k} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(C_i - e_i)^2}{e_i}, \tag{5}$$

которая аппроксимирует распределение χ^2 с $2k - 2$ степенями свободы.

Автокорреляционный тест. Тест предназначен для проверки корреляции между последовательностью s и ее сдвинутой (не циклически) версией. Пусть d – конкретное число, $1 \leq d \leq \lfloor \frac{n}{2} \rfloor$. Число элементов в s, не равных соответствующим элементам сдвинутой на d позиций версии последовательности определяется как $A(d) = \sum_{i=0}^{n-d-1} s_i \oplus s_{i+d}$, где $\oplus$ обозначает сумму по модулю 2.

Используется статистика

$$V_5 = \frac{2\left(A(d) - \frac{n-d}{2}\right)}{\sqrt{n-d}}, \tag{6}$$

которая аппроксимирует нормальное распределение $N(0,1)$, если $n-d>10$. Поскольку в равномерно распределенной последовательности малые значения $A(d)$ так же маловероятны как и большие, используется двусторонний тест.

Пример 2, [2]. Рассмотрим неслучайную последовательность длины $T=160$, полученную четырех кратным повторением последовательности

$$1110001100010001010011101111001001001001.$$

Применяя различные тесты, получаем:

1. Для частотного теста $n_0=84,\ n_1=76$. Значение статистики $V_1=0.4$.

2. Для теста проверки серий $n_{00}=44,\ n_{01}=40,\ n_{10}=40,\ n_{11}=35$. Значение статистики $X_2=1.025$.

3. Для покер-теста имеем $m=3,\ k=53$, подпоследовательности 000, 001, 010, 011, 100, 101, 110, 111 встречаются 5,10,6,4,12,3,6 и 7 раз соответственно. Значение статистики $V_3=9.6415$.

4. Для теста проверки блоков имеем $e_1=20,25,\ e_2=10,0625,\ e_3=5$ и $k=3$. Имеется 25,4,5 единичных блоков длины 1,2,3, соответственно, и 8,20,12 нулевых блоков длины 1,2,3, соответственно. Значение статистики $V_4=31,7913$.

5. Для автокорреляционного теста если $d=8$, то $A(8)=100$. Значение статистики $V_5=3.8933$.

Для уровня $\alpha=0.05$ пороговыми значениями для статистик V_1,V_2,V_3,V_4 и V_5 являются значения 3.8415, 5.9915, 14.0671, 9.4877 и 1.96 соответственно. Таким образом, анализируемая последовательность проходит частотный тест, тест проверки серий и покер-тест. Она не прошла тест проверки блоков и автокорреляционный тест.

4. Контрольные вопросы

1. Убедитесь, что формулы (2),(3),(reftestpoker) и (reftestblokow) получаются из формулы (1) как частные случаи.

2. Убедитесь,что линейная рекуррентная последовательность максимального периода соответствует постулатам Голомба.

Литература.

1. Фомичев В.М. Дискретная математика и криптология. М:ДиалогМИФИ. 2003.

2. Кнут Д. Искусство программирования для ЭВМ. Т.2. Получисленные алгоритмы. М.:Мир. 1977.

3. Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone. SRS Press, 1996.