

Статистические тесты NIST

Материал из Википедии — свободной энциклопедии

Статистические тесты NIST — пакет статистических тестов, разработанный Лабораторией информационных технологий (англ. *Information Technology Laboratory*), являющейся главной исследовательской организацией Национального института стандартов и технологий (NIST). В его состав входят 15 статистических тестов, целью которых является определение меры случайности двоичных последовательностей, порождённых либо аппаратными, либо программными генераторами случайных чисел. Эти тесты основаны на различных статистических свойствах, присущих только случайным последовательностям.

Содержание

Описание тестов

Частотный побитовый тест

Частотный блочный тест

Тест на последовательность одинаковых битов

Тест на самую длинную последовательность единиц в блоке

Тест рангов бинарных матриц

Спектральный тест

Тест на совпадение неперекрывающихся шаблонов

Тест на совпадение перекрывающихся шаблонов

Универсальный статистический тест Маурера

Тест на линейную сложность

Тест на периодичность

Тест приближительной энтропии

Тест кумулятивных сумм

Тест на произвольные отклонения

Другой тест на произвольные отклонения

См. также

Ссылки

Описание тестов

Частотный побитовый тест

Суть данного теста заключается в определении соотношения между нулями и единицами во всей двоичной последовательности. Цель — выяснить, действительно ли число нулей и единиц в последовательности приблизительно одинаковы, как это можно было бы предположить в случае

истинно случайной бинарной последовательности. Тест оценивает, насколько близка доля единиц к 0,5. Таким образом, число нулей и единиц должно быть примерно одинаковым. Если вычисленное в ходе теста значение вероятности $p < 0,01$, то данная двоичная последовательность не является истинно случайной. В противном случае последовательность носит случайный характер. Стоит отметить, что все последующие тесты проводятся при условии, что пройден данный тест.

Частотный блочный тест

Суть теста — определение доли единиц внутри блока длиной m бит. Цель — выяснить действительно ли частота повторения единиц в блоке длиной m бит приблизительно равна $m/2$, как можно было бы предположить в случае абсолютно случайной последовательности. Вычисленное в ходе теста значение вероятности p должно быть не меньше 0,01. В противном случае ($p < 0,01$) двоичная последовательность не носит истинно случайный характер. Если принять $m = 1$, данный тест переходит в тест № 1 (частотный побитовый тест).

Тест на последовательность одинаковых битов

Суть состоит в подсчёте полного числа рядов в исходной последовательности, где под словом «ряд» подразумевается непрерывная подпоследовательность одинаковых битов. Ряд длиной k бит состоит из k абсолютно идентичных битов, начинается и заканчивается с бита, содержащего противоположное значение. Цель данного теста — сделать вывод о том, действительно ли количество рядов, состоящих из единиц и нулей с различными длинами, соответствует их количеству в случайной последовательности. В частности, определяется быстро либо медленно чередуются единицы и нули в исходной последовательности. Если вычисленное в ходе теста значение вероятности $p < 0,01$, то данная двоичная последовательность не является истинно случайной. В противном случае можно считать последовательность случайной.

Тест на самую длинную последовательность единиц в блоке

В данном тесте определяется самый длинный ряд единиц внутри блока длиной m бит. Цель — выяснить действительно ли длина такого ряда соответствует ожиданиям длины самого протяжённого ряда единиц в случае абсолютно случайной последовательности. Если высчитанное в ходе теста значение вероятности $p < 0,01$ полагается, что исходная последовательность не является случайной. В противном случае делается вывод о её случайности. Следует заметить, что из предположения о примерно одинаковой частоте появления единиц и нулей (тест № 1) следует, что точно такие же результаты данного теста будут получены при рассмотрении самого длинного ряда нулей. Поэтому измерения можно проводить только с единицами.

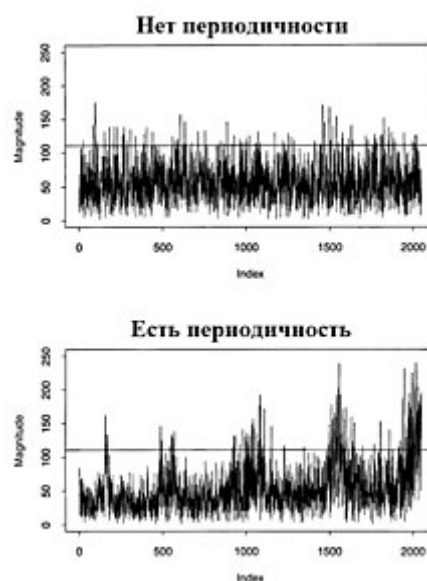
Тест рангов бинарных матриц

Здесь производится расчёт рангов непересекающихся подматриц, построенных из исходной двоичной последовательности. Целью этого теста является проверка на линейную зависимость подстрок фиксированной длины, составляющих первоначальную последовательность. В случае

если вычисленное в ходе теста значение вероятности $p < 0,01$, делается вывод о неслучайном характере входной последовательности бит. В противном случае считаем её абсолютно случайной. Данный тест так же присутствует в пакете DIEHARD.

Спектральный тест

Суть теста заключается в оценке высоты пиков дискретного преобразования Фурье исходной последовательности. Цель — выявление периодических свойств входной последовательности, например, близко расположенных друг к другу повторяющихся участков. Тем самым это явно демонстрирует отклонения от случайного характера исследуемой последовательности. Идея состоит в том, чтобы число пиков, превышающих пороговое значение в 95 % по амплитуде, было значительно больше 5 %. Если вычисленное в ходе теста значение вероятности $p < 0,01$, то данная двоичная последовательность не является абсолютно случайной. В противном случае она носит случайный характер.



Спектральный тест

Тест на совпадение неперекрывающихся шаблонов

В данном тесте подсчитывается количество заранее определенных шаблонов, найденных в исходной последовательности. Цель — выявить генераторы случайных или псевдослучайных чисел, формирующие слишком часто заданные непериодические шаблоны. Как и в тесте № 8 на совпадение перекрывающихся шаблонов для поиска конкретных шаблонов длиной m бит используется окно также длиной m бит. Если шаблон не обнаружен, окно смещается на один бит. Если же шаблон найден, окно перемещается на бит, следующий за найденным шаблоном, и поиск продолжается дальше. Вычисленное в ходе теста значение вероятности p должно быть не меньше 0,01. В противном случае ($p < 0,01$), двоичная последовательность не является абсолютно случайной.

Тест на совпадение перекрывающихся шаблонов

Суть данного теста заключается в подсчете количества заранее определенных шаблонов, найденных в исходной последовательности. Как и в тесте № 7 на совпадение неперекрывающихся шаблонов для поиска конкретных шаблонов длиной m бит используется окно также длиной m бит. Сам поиск производится аналогичным образом. Если шаблон не обнаружен, окно смещается на один бит. Разница между этим тестом и тестом № 7 заключается лишь в том, что если шаблон найден, окно перемещается только на бит вперед, после чего поиск продолжается дальше. Вычисленное в ходе теста значение вероятности p должно быть не меньше 0,01. В противном случае ($p < 0,01$), двоичная последовательность не является абсолютно случайной.

Универсальный статистический тест Маурера

Здесь определяется число бит между одинаковыми шаблонами в исходной последовательности (мера, имеющая непосредственное отношение к длине сжатой последовательности). Цель теста — выяснить может ли данная последовательность быть значительно сжата без потерь информации. В случае если это возможно сделать, то она не является истинно случайной. В ходе теста вычисляется значение вероятности p . Если $p < 0,01$, то полагается, что исходная последовательность не является случайной. В противном случае делается вывод о её случайности.

Тест на линейную сложность

В основе теста лежит принцип работы линейного регистра сдвига с обратной связью (англ. *Linear Feedback Shift Register, LFSR*). Цель — выяснить является ли входная последовательность достаточно сложной для того, чтобы считаться абсолютно случайной. Абсолютно случайные последовательности характеризуются длинными линейными регистрами сдвига с обратной связью. Если же такой регистр слишком короткий, то предполагается, что последовательность не является в полной мере случайной. В ходе теста вычисляется значение вероятности p . Если $p < 0,01$, то полагается, что исходная последовательность не является случайной. В противном случае делается вывод о её случайности.

Тест на периодичность

Данный тест заключается в подсчете частоты всех возможных перекрываний шаблонов длины m бит на протяжении исходной последовательности битов. Целью является определение действительно ли количество появлений 2^m перекрывающихся шаблонов длиной m бит, приблизительно такое же как в случае абсолютно случайной входной последовательности бит. Последняя, как известно, обладает однообразностью, то есть каждый шаблон длиной m бит появляется в последовательности с одинаковой вероятностью. Если вычисленное в ходе теста значение вероятности $p < 0,01$, то данная двоичная последовательность не является абсолютно случайной. В противном случае, она носит случайный характер. Стоит отметить, что при $m=1$ тест на периодичность переходит в частотный побитовый тест (№ 1).

Тест приближенной энтропии

Как и в тесте на периодичность в данном тесте акцент делается на подсчёте частоты всех возможных перекрываний шаблонов длины m бит на протяжении исходной последовательности битов. Цель теста — сравнить частоты перекрывания двух последовательных блоков исходной последовательности с длинами m и $m+1$ с частотами перекрывания аналогичных блоков в абсолютно случайной последовательности. Вычисляемое в ходе теста значение вероятности p должно быть не меньше 0,01. В противном случае ($p < 0,01$), двоичная последовательность не является абсолютно случайной.

Тест кумулятивных сумм

Тест заключается в максимальном отклонении (от нуля) при произвольном обходе, определяемым кумулятивной суммой заданных (-1, +1) цифр в последовательности. Цель данного теста — определить является ли кумулятивная сумма частичных последовательностей, возникающих во входной последовательности, слишком большой или слишком маленькой по сравнению с ожидаемым поведением такой суммы для абсолютно случайной входной последовательности. Таким образом, кумулятивная сумма может рассматриваться как произвольный обход. Для

случайной последовательности отклонения от произвольного обхода должны быть вблизи нуля. Для некоторых типов последовательностей, не являющихся в полной мере случайными подобные отклонения от нуля при произвольном обходе будут достаточно существенными. Если вычисленное в ходе теста значение вероятности $p < 0,01$, то входная двоичная последовательность не является абсолютно случайной. В противном случае она носит случайный характер.

Тест на произвольные отклонения

Суть данного теста заключается в подсчёте числа циклов, имеющих строго k посещений при произвольном обходе кумулятивной суммы. Произвольный обход кумулятивной суммы начинается с частичных сумм после последовательности $(0,1)$, переведённой в соответствующую последовательность $(-1, +1)$. Цикл произвольного обхода состоит из серии шагов единичной длины, совершаемых в случайном порядке. Кроме того такой обход начинается и заканчивается на одном и том же элементе. Цель данного теста — определить отличается ли число посещений определенного состояния внутри цикла от аналогичного числа в случае абсолютно случайной входной последовательности. Фактически данный тест есть набор, состоящий из восьми тестов, проводимых для каждого из восьми состояний цикла: $-4, -3, -2, -1$ и $+1, +2, +3, +4$. В каждом таком тесте принимается решение о степени случайности исходной последовательности в соответствии со следующим правилом: если вычисленное в ходе теста значение вероятности $p < 0,01$, то входная двоичная последовательность не является абсолютно случайной. В противном случае она носит случайный характер.



Другой тест на произвольные отклонения

В этом тесте подсчитывается общее число посещений определенного состояния при произвольном обходе кумулятивной суммы. Целью является определение отклонений от ожидаемого числа посещений различных состояний при произвольном обходе. В действительности этот тест состоит из 18 тестов, проводимых для каждого состояния: $-9, -8, \dots, -1$ и $+1, +2, \dots, +9$. На каждом этапе делается вывод о случайности входной последовательности. Если вычисленное в ходе теста значение вероятности $p < 0,01$, то входная двоичная последовательность не является абсолютно случайной. В противном случае она носит случайный характер.

См. также

- [Генератор псевдослучайных чисел](#)
- [Тестирование псевдослучайных последовательностей](#)
- [AES \(конкурс\)](#)

Ссылки

- [NIST Cryptographic Toolkit \(http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html\)](http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html) (англ.)
- [Statistical Testing of Random Number Generators \(http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf\)](http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf)  (англ.) Proceedings of the 22nd National Information Systems Security Conference, 10/99
- [A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications \(http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf\)](http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf)  (англ.) NIST SP 800-22

- [Dieharder: A Random Number Test Suite \(http://www.phy.duke.edu/~rgb/General/dieharder.php\)](http://www.phy.duke.edu/~rgb/General/dieharder.php) (англ.) Свободная реализация статистических тестов (включая тесты DIEHARD и NIST) на языке Си.
-

Источник — https://ru.wikipedia.org/w/index.php?title=Статистические_тесты_NIST&oldid=114776878

Эта страница в последний раз была отредактирована 8 июня 2021 в 16:38.

Текст доступен по лицензии Creative Commons «С указанием авторства — С сохранением условий» (CC BY-SA); в отдельных случаях могут действовать дополнительные условия.

Wikipedia® — зарегистрированный товарный знак некоммерческой организации Фонд Викимедиа (Wikimedia Foundation, Inc.)