УДК 681.3.06

ОЦЕНКА КАЧЕСТВА СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СТАТИСТИЧЕСКИМИ ТЕСТАМИ

Г.В. ДАВЫДОВ, А.И КУХАРЕНКО

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
nil53@bsuir.edu.by

Описывается метод оценки случайности последовательности чисел статистическими методами. Рассматриваются пакет тестов NIST, определяется роль каждого теста, входящего в него. Тесты используются при оценке и проверке генераторов случайных чисел.

Ключевые слова: генератор случайных чисел, статистические тесты, случайная последовательность, вероятность, программа.

Современные информационные технологии широко используют случайные числа в самых разных приложениях — от имитационного моделирования до криптографии. Случайность чисел в заданных последовательностях оценивается статистическими методами. Для этого используются семейства статистических тестов, например, тесты Д. Кнута, тесты Дж. Марсальи, Национального института стандартов США (тесты NIST) и др. В состав тестов NIST входят 15 статистических тестов, основные требования которых заключаются в следующем.

Частотный побитовый тест (Frequency Test) определяет соотношения между нулями и единицами во всей двоичной последовательности. В этом тесте определяется P-value, являющейся оценкой вероятности того, что вычисленное значение нормированной кумулятивной суммы не превышает заданного порога. Выполнение неравенства P-value < 0,01 (рекомендованное значение), указывает на несоответствие входной последовательности гипотезе о нормальном распределении вероятности. Все последующие тесты проводятся при условии прохождения этого теста.

Частотный блочный тест (Frequency Test within a Block) определяет количество единиц внутри блока длиной k бит. В тесте выясняется, действительно ли частота повторения единиц в блоке длиной k бит приблизительно равна k/2 , как можно было бы предположить в случае абсолютно случайной последовательности.

Тест на последовательность одинаковых бит (Runs Test). Тест на самую длинную последовательность единиц в блоке (Test for the Longest Run of Ones in a Block). Первый тест подсчитывает полное число серий в исходной последовательности, где под серией подразумевается непрерывная подпоследовательность одинаковых бит. Второй определяет самую длинную серию единиц внутри блока. Цель данных тестов – сделать вывод о том, действительно ли серии, соответствуют по числу и по длинам сериям, наблюдаемым в абсолютно случайной последовательности.

Тест рангов бинарных матриц (Binary Matrix Rank Test) рассчитывает ранги непересекающихся подматриц, построенных из исходной двоичной последовательности. Целью этого теста является проверка на линейную зависимость подстрок фиксированной длины, составляющих первоначальную последовательность.

Спектральный тест (Discrete Fourier Transform Test). В данном тесте оценивается высота пиков дискретного преобразования Фурье исходной последовательности. Тест выявляет периодические свойства последовательности, например, наличие повторяющихся участков.

Тест на совпадение неперекрывающихся шаблонов (Non-overlapping Template Matching Test). Тест на совпадение перекрывающихся шаблонов (Overlapping Template Matching Test). Эти 2 теста подсчитывают количество заранее определенных шаблонов, найденных в исходной последовательности. Цель – выявить ГСЧ, формирующие слишком часто заданные непериодические шаблоны.

Универсальный статистический тест Маурера (Maurer's "Universal Statistical" Test) определяет, может ли данная последовательность быть значительно сжата без потерь информации.

Тест на периодичность (Serial Test) подсчитывает частоты всех возможных перекрываний шаблонов длины m бит на протяжении исходной последовательности битов. Целью является определение, действительно ли количество появлений 2m перекрывающихся шаблонов длиной m бит приблизительно такое же, как в случае абсолютно случайной входной последовательности бит.

Тест приблизительной энтропии (Approximate Entropy Test). Как и в тесте на периодичность, в данном тесте акцент делается на подсчете 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.

Тест кумулятивных сумм (Cumulative Sums Test). Тест на произвольные отклонения (Random Excursions Test). Тест на произвольные отклонения состояний последовательности (Random Excursions Variant Test). Эти 3 теста объединяет преобразование последовательности (0,1) в соответствующую последовательность (-1, +1) и подсчет кумулятивных сумм. Первый тест определяет максимальное отклонение от нуля кумулятивной суммы при произвольном обходе и определяет, является ли сумма слишком большой или слишком маленькой по сравнению с ожидаемым поведением такой суммы у абсолютно случайной входной последовательности, для которой отклонение должно быть вблизи нуля. Второй тест подсчитывает число циклов, имеющих строго k посещений при произвольном обходе кумулятивной суммы. Третий тест подсчитывает общее число посещений определенного состояния при произвольном обходе кумулятивной суммы. Определяется, отличаются ли результаты от аналогичных результатов в случае абсолютно случайной последовательности.

Тесты NIST, ввиду наличия подробной документации и открытых исходных кодов программной реализации тестов, получили широкое распространение. Чтобы воспользоваться этими тестами, необходимо скомпилировать исходный код в исполняемый EXE файл. Программа представляет собой консольное приложение, в котором задается тестируемый файл, указывается количество бит в последовательности (рекомендуется не менее 1000000 бит), выбираются необходимые тесты и настройки по каждому тесту. После выполнения расчетов, программа сохраняет результаты тестирования в текстовый файл. Далее необходимо произвести обработку результатов тестов, например, построить гистограмму распределения P-value, которая должна иметь равномерное распределение, и, в конечном итоге, определить качество тестируемой случайной последовательности.

Список литературы

1. *Rukhin A.* A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications// NIST. 2010. P.131.

2. *Juan Soto*. Statistical Testing of Random Number Generators// National Institute of Standards and Technology. P. 12.