УДК 519.221

Анализ чувствительности статистических тестов Diehard при оценке качества последовательности случайных чисел

Фирстов Артём Дмитриевич
Сибирский федеральный университет
Студент

Аннотация
В статье описан эксперимент по анализу чувствительности статистических тестов Diehard при оценке качества последовательности случайных чисел. Построены аналитические таблицы, сделан вывод.
Ключевые слова: числовая последовательность, diehard, статистический тест, закон распределения

Analysis of the sensitivity of statistical tests Diehard to evaluate the quality of a sequence of random numbers

Firstov Artyom Dmitrievich
Siberian Federal University
Student

Abstract
The article describes the experiment on the analysis of the sensitivity of statistical tests Diehard in assessing the quality of a sequence of random numbers. Analytic tables are constructed, and a conclusion is drawn.
Keywords: numerical sequence, diehard, statistical test, distribution law

Перешедшие на новый качественный уровень, информационные технологии расширяют возможности эффективного управления, предоставляя менеджерам, руководителям производства всех уровней новейшие методы обработки и анализа экономической информации, необходимой для принятия решений.

Менеджерам часто приходиться принимать решения в условиях большой неопределенности (инфляция, нестабильный курс валют, изменение налоговых и правовых условий работы и т. д.). В этом случае преимуществом вычислительной техники является быстрый просчет вариантов и выдача ответов на вопросы типа «что, если?».

Применение современных информационных технологий в сфере управления обеспечивает повышение качества экономической информации, ее точности, объективности, оперативности и как результат – возможность принятия своевременных управленческих решений [4].

Использование многих современных статистических пакетов ограничено в силу их высокой стоимости (профессиональные статистические

пакеты обычно стоят от 1 до 10 тыс. долларов), а также в силу сложности их освоения, в основном подобные пакеты предназначены только для опытных пользователей.

В настоящее время существует несколько пакетов статистических тестов для измерения качества набора случайных чисел. Наиболее известным и эффективным считается Diehard.

1 Статистический пакет Diehard

Статистический пакет Diehard был разработан американским математиком и информатиком Джорджем Марсальей [1]. Распространялся на CD-ROM.

Данный пакет включает в себя 12 тестов:

1. Birthday Spacings.
2. Overlapping Permutations.
3. Ranks of matrices.
4. Monkey Tests.
5. Count the 1st.
6. Parking Lot Test.
7. Minimum Distance Test.
8. Random Spheres Test.
9. The Squeeze Test.
10. Overlapping Sums Test.
11. Runs Test.
12. The Craps Test.

Для оценки результатов тестов используется отдельный коэффициент P (p-value). P-value — это вероятность того, что абстрактный генератор случайных чисел сгенерировал бы последовательность менее случайную, чем исследуемая [2]. Когда P = 0, это значит, что последовательность чисел неслучайна, а когда P = 1, то последовательность близка к совершенно случайной. На практике значение P должно быть больше, чем уровень достоверности теста. Например, при P > 0,01 проверяемая последовательность случайна в 99% случаев [4] (если достоверность теста a = 0.01, то одна из ста последовательностей будет неслучайной).

2 Анализ чувствительности

В качестве исходного файла выступает последовательность случайных чисел, подготовленная генератором Multiply-With-Carry (MWC) I — пример «хорошего» генератора случайных чисел [1].

В качестве помехи выступает последовательность случайных чисел, сгенерированная по равномерному закону распределения и последовательность единиц.

Исходный файл размером 11 468 800 байт будет поделен следующим образом:

- Для добавления 0,28% шума — на 350 равных частей размером 32 768 байт каждая (т.е. в исходной выборке будет заменено 8 192 чисел).

- Для добавления 6,25% шума — на 16 равных частей размером 716 800 байт каждая (т.е. в исходной выборке будет заменено 179 200 чисел).

После разрезания исходного файла по описанному сценарию, замены части и последующего склеивания, будет получен файл точно такой же размерности – 11 468 800 байт, который пригоден для тестирования.

В таблице 1 приведены результаты работы в разрезе по добавленному шуму.

Таблица 1 – Первые 13 значений p-value для полученных случайных чисел

MWC I + 1,1,1,…m		**MWC I + Равн. распр.**	
0,28%	**6,25%**	**0,28%**	**6,25%**
0,075232	0,000000	0,075232	0,000000
0,523600	0,000000	0,523600	0,000000
0,165570	0,000000	0,165570	0,000000
0,123238	0,000000	0,123238	0,000000
0,748064	0,000000	0,748064	0,000000
0,290372	0,000000	0,290372	0,000000
0,536651	0,000000	0,536651	0,000000
0,171687	0,000000	0,171687	0,000000
0,213637	0,000000	0,213637	0,000000
0,079262	0,000000	0,079262	0,000000
0,000000	0,000000	0,979082	0,997850
0,001114	0,001114	0,001114	0,001114
0,000000	0,000000	0,000000	0,000000

Для анализа чувствительности изменений p-value было принято решение рассчитать расстояние от исходных значений до полученных по формуле (1):

$$D = \sum_{i=1}^{n} (a_i - b_i)^2, \qquad (1)$$

где a_i – p-value исходной последовательности случайных чисел, b_i – p-value полученной последовательности случайных чисел.

В таблицах 3 и 4 приведены результаты расчетов.

Таблица 2 – Расстояние от последовательности MWC I до всех остальных

Распределение	**MWC I**
MWC II	42,760914
1,1,1,…m	73,700658
1,2,3,…m	73,700658
Норм. распр.	65,362705
Равномерн. распр.	62,813740

Таблица 3 – Расстояние от исходной последовательности MWC I до MWC I с помехой

Распр.	**MWC I + 1,1,1,…m**		**MWC I + Равн. распр.**	
	0,28%	6,25%	0,28%	6,25%
MWC I	47,845770	61,422362	43,327891	44,400280

По числовым характеристикам из таблицы 2 и 3 можно сделать следующий вывод: статистические тесты из набора Diehard крайне чувствительны к изменению содержимого файла. Добавление 0,28% шума вызывается отказ нескольких тестов и приводит к значительному изменению основных числовых характеристик.

Библиографический список

1. Марсалья, Д. DIEHARD Statistical Tests [Электронный ресурс] – Режим доступа: http://goo.gl/seqY82.
2. Чайковский, Ю. В. Ступени случайности и эволюция // Вопросы философии. 1996. №9. С.32-47.
3. Федорова А.В. Информационные технологии управления. Красноярск: Сибирский федеральный университет, 2010. 124 с.
4. Рубан А.И. Теория вероятностей и математическая статистика. Красноярск: Сибирский федеральный университет; 2012