Masaryk University
Faculty of Informatics

The automated testing of randomness with multiple statistical batteries

Master's Thesis

Ľubomír Obrátil

Brno, Spring 2017

Replace this page with a copy of the official signed thesis assignment and the copy of the Statement of an Author.

Declaration

Hereby I declare that this paper is my original authorial work, which I have worked out on my own. All sources, references, and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Ľubomír Obrátil

Advisor: RNDr. Petr Švenda, Ph.D.

Acknowledgement

TODO

Abstract

TODO

Keywords

TODO

Contents

1 Introduction

- Randomness, why should we test it (defects, low entropy, etc...)
- Statistical testing of randomness

2 Used third-party statistical software

2.1 Terminology

In this thesis we are using certain expressions in the context of Randomness Testing Toolkit and the tools it uses. We list these expressions along with their explanations here.

(Statistical) Battery
Program developed by a third party serving as a tool for evaluation of randomness of arbitrary binary data. Statistical battery usually contains one or multiple statistical tests. Final result of the evaluation is based on the results of the tests. Examples of statistical batteries are NIST Statistical Test Suite, Dieharder or TestU01.

(Statistical) Test
Single unit in statistical battery that measures some property of the tested binary stream (e.g. number of zeroes). Based on this measurement, first level p-value of the test is calculated. The test can be repeated, resulting in multiple p-values. From these p-values are obtained one or multiple second level p-values. Result of the test can then be either first level p-value or one or more second level p-values called statistics.

Variant of a test
Many tests can be parametrized in some ways, possibly giving different results with the same input data. We don't treat multiple executions of single test with different settings as separate units but rather as a variants of that test.

Subtest
Some tests, even when executed only once, may measure multiple properties of the data thus providing multiple results. For example, Serial Test from Dieharder battery will measure frequencies of all 1, 2, .., 16-bit patterns in the data. We treat these measurements separately - as a subtests of the test. Therefore subtest is smallest unit in the battery, providing only single result.

Statistic
Value obtained by certain calculation from first level p-values. Multiple statistics can be obtained from one set of p-values e.g. when testing the set for uniformity we can use Kolmogorov-Smirnovov Test or Chi-Square test.

p-value
We refer to first level p-values as to simply p-values and second level p-values as to statistics. P-value is obtained as a result of single execution of a test. This p-value tells us the probability that the input data was truly random. Hence obtaining p-value very close to 1 means that the data was almost certainly produced by TRNG. When the p-value is close to 0 it means that it

is almost impossible to obtain such data from TRNG; the data is probably not random.

2.2 Batteries supported by RTT

2.2.1 NIST Statistical Test Suite

The battery of statistical tests was developed by National Institute of Standards and Technology (cit.). The battery implements 15 statistical tests for evaluating randomness of input data.

The reference implementation is not used in RTT because it is considerably slower than its optimized counterparts. The optimized version of NIST STS used in RTT was developed by Zdeněk Říha and Marek Sýs(cit.).

2.2.2 Dieharder

Dieharder is a battery developed by Robert G. Brown at the Duke University (cit.). The battery features user friendly console interface with possibility of fine-grain modification of the test parameters. The fact that Dieharder is included in repositories of some Linux distributions (cit manpage) adds to its popularity and ease of use. Dieharder includes all tests from older statistical battery Diehard (cit.), three tests from NIST STS and several other tests implemented by the author.

Since original Dieharder implementation doesn't output all of the information we needed for interpretation and evaluation of the results, we had to modify source code of the battery. RTT uses this modified Dieharder.

2.2.3 TestU01

This library of statistical batteries was developed at Université de Montréal by Pierre L'Ecuyer et al (cit.). It contains wide range of tests from NIST STS, Dieharder and literature. It also implements numerous pseudo-random number generators. The statistical tests are grouped into multiple categories each intended for different use-case scenario. We will treat these categories of tests as separate batteries. TestU01 includes following 10 batteries.

Small Crush, Crush, Big Crush
Small Crush battery is very fast and needs relatively small amount of data to run - around 250 megabytes. Small Crush is also the only battery that can be natively used for analysis of data in binary file, for use of Crush and Big Crush, the user has to implement PRNG with TestU01 interface. Crush and Big Crush batteries are more stringent and need gigabytes of data and a few hours to finish while Big Crush is more time and data demanding.

Rabbit, Alphabit, Block Alphabit
Tests in these batteries are suited for testing hardware bit generators and are applicable to arbitrary amount of data. Data can be provided either as a binary file or PRNG implementing TestU01 interface.

PseudoDIEHARD, FIPS_140_2
Tests in PseudoDIEHARD imitate DIEHARD battery and FIPS_140_2 battery implements small suite of tests in NIST standard(cit.) Randomness Testing Toolkit doesn't support these two batteries since they are subsets of other supported batteries.

Since TestU01 is available only as a ANSI C library, we developed a console interface for it. The interface implements a dummy number generator that provides data from a supplied binary file to the battery. This allows us to apply batteries to arbitrary binary data even when the batteries don't support this feature natively.

2.3 Known errors in the batteries

To examine the boundary behavior of the above-listed tools, we used them to process extremely non-random data streams. The data streams that were used as the input to the batteries were two binary data files consisting only of zeroes and ones respectively. The settings of the batteries remained set to default.

Below we list observed behavior that differ from execution of the batteries with non-extreme input.

NIST Statistical Test Suite

Tests Random Excursions and Random Excursions Variant are not applicable to all possible data streams. In a normal run with reasonably varied data, this doesn't matter much, as the tests are repeated multiple times and the final result will simply be calculated from lesser number of p-values.

Neither of the tests is applicable to a stream full of zeroes or ones. This causes absence of results when analyzing such data. The user can find out the fact that the tests are not applicable to provided stream after he inspects logs of the program, otherwise the interpretation of the missing results is left to him.

Dieharder

Our findings are summarized in Table 2.1.

Test name	All zero stream	All ones stream
STS Runs	No result	No result
DAB Monobit 2	Passing	Passing
Diehard Minimum Distance (2D Circle)	Timeout	-
Diehard 3D Sphere (Minimum Distance)	Timeout	-
Marsaglia and Tsang GCD	Timeout	-
RGB Generalized Minimum Distance	Timeout	-
RGB Kolmogorov-Smirnov	Timeout	-
Diehard Craps	-	Timeout
RGB Bit Distribution	-	Timeout

Table 2.1: Flawed tests in Dieharder battery

TestU01

Our findings are summarized in Table 2.2.

Test name	All zero stream	All ones stream
sstring_Run	No result	No result
sknuth_Gap	No result	-
snpair_ClosePairs	Timeout	Timeout
snpair_ClosePairsBitMatch	-	Timeout
svaria_SumCollector	-	Timeout
smarsa_GCD	-	Timeout
svaria_SampleProd	Full pass	Full pass
svaria_AppearenceSpacings	Full pass	Full pass
scomp_LinearComp	Full pass	Full pass
svaria_SampleCorr	-	Full pass
scomp_LempelZiv	Full, part pass	Full, part pass
sknuth_MaxOft	Part pass	Part pass
svaria_SampleMean	Part pass	Part pass
sspectral_Fourier3	Part pass	Part pass
sstring_HammingWeight2	Part pass	Part pass
sstring_AutoCor	Part pass	Part pass
smultin_MultinomialBitsOver	Part pass	Part pass
sstring_LongestHeadRun	-	Part pass

Table 2.2: Flawed tests in TestU01 library

3 Randomness Testing Toolkit

- Motivation - unified interface to batteries, ease of use, unified result format/representation
- Local execution of RTT - battery and toolkit configuration, installation, brief implementation and interface overview - more thorough in documentation and comments
- Local result format - either database or file output storage
- Remote execution of RTT - toolkit deployed on server infrastructure, system overview (database, frontend, backend(s), storage), accessible through ssh on limited system or via web interface (django), results in database
- Remote results of RTT - email notification, webpage layout

4 Interpretation of results of RTT

- Grouping subtests together - eliminating intertest bias
- How grouping works - theory, Sidak correction, partial p-value, fail/-pass of a test

5 Analysis of outputs of cryptographic functions, comparison with EACirc

- How the data were tested
- List functions
- List interesting (differing) results - Dieharder, NIST STS, TestU01, EACirc, polynomials(???)

6 Analysis of DIEHARDER results on quantum random data

- Statistical intro, uniformity, first vs. second level p-value, etc...
- Two experiments - continuous p-values, blocks of 2nd level
- Results - non-uniform, where it will begin to show on 2nd level results

7 Conclusions

- Developed user-friendly tool for easy analysis of arbitrary binary data - Randomness Testing Toolkit
- Interpretation of results
- Comparison of batteries with EACirc, polynomials
- Defects in Dieharder, their relevance, etc...
- Future work, same analysis on TestU01, dependence between tests(?), continuous development of RTT, call for flawless statistical battery (:))

A An appendix

TODO