Masaryk University
Faculty of Informatics

WORK TITLE: The automated testing of randomness with multiple statistical batteries

Master's Thesis

Ľubomír Obrátil

Brno, Spring 2017

This is where a copy of the official signed thesis assignment and a copy of the Statement of an Author is located in the printed version of the document.

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 Overview of statistical batteries

- Terminology related to batteries - battery, test, variant of a test, subtest, statistics, p-values
- nist sts, dieharder, testu01
- Each battery: overview, tests, tests into (subtests, default parameters, variants in default run), known defectes

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