MASARYK
UNIVERSITY

FACULTY OF INFORMATICS

Improvements of the Randomness Testing Toolkit

Bachelor's Thesis

TOMÁŠ MAREK

Brno, Spring 2023

MASARYK UNIVERSITY

FACULTY OF INFORMATICS

Improvements of the Randomness Testing Toolkit

Bachelor's Thesis

TOMÁŠ MAREK

Advisor: Ing. Milan Brož, Ph.D.

Department of Computer Systems and Communications

Brno, Spring 2023


FACULTAS ARTIS INFORMATICÆ
UNIVERSITAS MASARYKIANA

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.

Tomáš Marek

Advisor: Ing. Milan Brož, Ph.D.

Acknowledgements

These are the acknowledgements for my thesis, which can span multiple paragraphs.

Abstract

This is the abstract of my thesis, which can
span multiple paragraphs.

Keywords

keyword1, keyword2, ...

Contents

Introduction

1 Randomness testing

Explanations of principles, ideas, some figures are expected here.

1.1 Motivation

Why do we use this tests, some examples of usage

1.2 First level testing

test statistics - what is it, why is it important, different distributions

p-values - explanation - what does it mean, how to get them and how to interpret them

1.3 Second level testing

Motivation why first-level testing is not enough

basic principle how does it work - mentioning uniform distribution of first-level p-values

explanations of at least KS-statistic and χ^2-test

2 Available solutions

This chapter serves to describe various works and programs this thesis connects to.

2.1 Statistical testing batteries

Might be moved to separate chapter.

More or less deep description of each battery. Should contain information about test parameters/settings.

If there are any problems with the battery (e.g. tests which read different amount of data from DieHarder).

2.1.1 Dieharder

2.1.2 NIST STS

2.1.3 Test U01

2.1.4 BoolTest

2.2 Randomness Testing Toolkit

principles of work - separate execution of batteries

2.2.1 Settings and input

describing the format of at least configs

2.2.2 Disadvantages

The problems/weak points we want to improve with this thesis. Namely at least non machine-machine readable format, running only one battery at time, maybe re-calculation of results

2.3 Randomnes Testing Toolkit in Python

Roughly the same things as in RTT

Disadvantages - less info in results (missing first-level p-values), creating better machine-readable format

3 Improvements of the rtt-py

This part will probably be split into more chapters. Will depend on what and how exactly will be done. Some of the expected parts:

3.1 Changes done to rtt-py

3.2 Tests for rtt-py

4 Conclusion

A An appendix

Here you can insert the appendices of your thesis.