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 Previous works

Rather quick description of batteries, RTT, RTT PY and why we want to improve them.

1.1 Randomness testing

Motivation for randomness testing in general.

1.2 Tests batteries

Mentioning Dieharder, NIST etc directly

1.3 RTT

1.4 RTT PY

2 Theoretical part - how testing works

The theory behind the randomness testing - how the tests work, explanation of p-values and how to interpret the results.

2.1 First level testing

P-values, different probability distributions

2.2 Second level testing

KS-statistic, χ^2-test etc.

3 Practical part - describing current status

Deeper description of both the RTT and RTT PY. How they work, their outputs etc... Maybe some of the individual tests batteries.

4 Practical part - what was the plan and what was done

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

4.1 Changes done to RTT PY

4.2 Tests for RTT PY

A An appendix

Here you can insert the appendices of your thesis.