

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет прикладной математики и информатики
Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

**“Исследование эффективности источников энтропии на основе оценок
минимальной энтропии”**

Бородина Дарья Евгеньевна

Научный руководитель — кандидат физико-математических наук, доцент
кафедры математического моделирования и анализа данных Пирштук И. К.

Минск, 2024

РЕФЕРАТ

Дипломная работа: 50 страниц, 5 глав, 18 рисунков, 11 таблиц, 6 использованных источников.

Ключевые слова: ЭНТРОПИЯ, СЛУЧАЙНЫЕ ЧИСЛА, NIST, НЕЗАВИСИМЫЕ И ОДИНАКОВО РАСПРЕДЕЛЕННЫЕ СЛУЧАЙНЫЕ ВЕЛИЧИНЫ, АЛГОРИТМЫ, PYTHON.

Объект исследования: методы и алгоритмы оценки минимальной энтропии для последовательностей случайных величин.

Цель работы: описание и анализ методов и алгоритмов тестирования выходных последовательностей (iid и no-iid) источников случайности на основе документа NIST SP 800-90B, разработка собственного программного обеспечения на языке python, реализующего данные тесты и сравнение полученных результатов с готовым программным обеспечением на языке c++.

Методы исследования: а) теоретические: изучение источников, посвященных алгоритмам оценки минимальной энтропии; изучение характеристик и возможностей применения данных алгоритмов;

б) практические: разработка программного обеспечения на языке python с реализацией алгоритмов тестирования выходных последовательностей на основе оценки минимальной энтропии.

Результат: разработанное на языке python программное обеспечение с открытым исходным кодом для оценки качества случайных последовательностей на основе оценок минимальной энтропии.

Область применения: оценка качества случайных последовательностей.

ABSTRACT

Diploma thesis: 50 pages, 5 chapters, 18 figures, 11 tables, 6 sources50 pages, 5 chapters, 18 figures, 11 tables, 6 sources.

Keywords: ENTROPY, RANDOM NUMBERS, NIST, INDEPENDENT AND IDENTICALLY DISTRIBUTED RANDOM VARIABLES, ALGORITHMS, PYTHON.

Object of study: methods and algorithms for estimating minimum entropy for sequences of random variables.

Purpose of work: description and analysis of methods and algorithms for testing output sequences (iid and no-iid) of randomness sources based on document NIST SP 800-90B, development of custom software in python that implements these tests and comparison of the obtained results with the results of ready-made software in C++.

Research methods: a) theoretical: studying of sources devoted to algorithms for estimating minimum entropy; studying of characteristics and the possibilities of using these algorithms;

b) practical: software development in python with implementation of algorithms for testing output sequences based on minimum entropy assessment.

Result: open source software developed in python for assessing the quality of random sequences based on minimum entropy estimates.

Scope: assessing the quality of random sequences.