На правах рукописи

ШИРШОВА ДАРЬЯ ВАДИМОВНА

МЕТОД И КОМПЛЕКС ПРОГРАММ НАХОЖДЕНИЯ МАКСИМАЛЬНОЙ ДЛИНЫ ВЫБОРКИ СТАТИСТИЧЕСКИ ОДНОРОДНЫХ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Специальность:

05.13.18 – Математическое моделирование, численные методы и комплексы программ

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

Казань 2019

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования (ФГБОУ ВО) «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ» (КНИТУ-КАИ) на кафедре компьютерных систем.

Научный руководитель: **Кузнецов Валерий Михайлович**
доктор технических наук, доцент, ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ», профессор кафедры «Компьютерных систем»

Официальные оппоненты: **Латыпов Рустам Хафизович**
доктор технических наук, профессор, ФГАОУ ВО «Казанский (Приволжский) федеральный университет»
заведующий кафедрой «Системного анализа и информационных технологий»

Кирпичников Александр Петрович
доктор физико-математических наук, профессор, ФГБОУ ВО «Казанский национальный исследовательский технологический университет», заведующий кафедрой «Интеллектуальных систем и управления информационными ресурсами»

Ведущая организация: ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

Защита состоится «13» декабря 2019 г. в $15^{\underline{00}}$ часов на заседании диссертационного совета Д 212.079.10, созданного на базе ФГБОУ ВПО «Казанский национальный исследовательский технический университет им. А.Н.Туполева – КАИ», по адресу: 420111, г. Казань, ул. К. Маркса, 10.

С диссертацией можно ознакомиться в научной библиотеке и на сайте КНИТУ-КАИ. Электронные варианты диссертации и автореферата размещены на сайте КНИТУ-КАИ (http://old.kai.ru/science/disser/).

Автореферат разослан «_____» _____ 2019 г.

Ученый секретарь
диссертационного совета 212.079.10
кандидат технических наук, доцент — Анна Викторовна Каляшина

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Сфера применения случайных и псевдослучайных процессов в виде последовательностей чрезвычайно широка: методы статистических испытаний (Монте-Карло), защита информации, контроль неисправностей, стохастические вычисления, испытания на надежность, тренажеры-симуляторы, широкополосная связь и т.п.

В качестве элементарной основы последовательностей используются двоичные формы как универсальные стохастические компоненты дискретных функций времени. Генерация таких последовательностей и контроль их характеристик представляют достаточно сложные научные задачи. Существует много алгоритмов формирования псевдослучайных последовательностей с разными характеристиками, исследованными М.А. Ивановым, А.П. Кирпичниковым, Б.Ф. Кирьяновым, В.М. Кузнецовым, Р.Х. Латыповым, В.А. Песошиным, В.Б. Пестряковым, Е.Л. Столовым, И.В. Чугунковым и другими. Особенно разнообразны по статистическим характеристикам последовательности, применяемые для имитационного моделирования. На практике, как правило, ограничиваются заданием и контролем вероятностных параметров в пределах моментов первого и второго порядков, что отвечает понятию стационарности процессов в широком смысле. Для двоичных последовательностей это математическое ожидание, совпадающее с вероятностью появления единицы, и корреляционные функции с аргументом временного сдвига, включая дисперсию.

В общем случае значения вероятностей и виды корреляционных зависимостей в каждой задаче имитационного моделирования могут варьироваться в произвольно допустимых формах и диапазонах. Современная тенденция усложнения имитационного эксперимента, кроме расширения разнообразия требуемых статистических свойств, диктует применение все более наполненных (мощных) множеств имитирующих воздействий. Большое количество отдельных последовательностей и чисел в них вызывает существенную перегрузку ресурсов ЭВМ, создавая ограничения в реализации логической и аналитической частей машинной модели. Вполне очевидно возникновение намерения в объективном сравнении применяемых последовательностей по основным статистическим свойствам с учетом конкретных длин выборок. Результатом такого анализа могут стать процедуры минимизации ресурсных издержек на формирование отдельных чисел и уменьшение количества выборок за счет их объединения или замены альтернативными фрагментами по свойствам, но более простыми в алгоритмическом смысле. Однако существующая практика выбора случайных и псевдослучайных последовательностей основана на их сравнении по статистическим характеристикам, определенным на полных периодах или при бесконечных длинах выборок, тогда как реальное использование этих имитирующих воздействий происходит за счет фрагментов конкретной длины. Естественно, подобное сопоставление математически не корректно, а в отношении задачи имитации – не адекватно.

Широкое развитие и применение статистических методов сравнения объектов естественным образом коснулось и числовых последовательностей. Идеальные модели случайности в виде «Белого шума» в статистической радиофизике и схемы независимых испытаний Бернулли в теории вероятностей нашли свое отражение в трех постулатах Голомба, выразивших необходимые признаки случайности для числовых последовательностей.

Субъективная оценка качества формирования случайных последовательностей возможна на основе графических тестов, что не может удовлетворить пользователей, нуждающихся в численных оценках случайности. Практически применимые алгорит-

мы оценки качества случайных последовательностей в статистически измеримой форме впервые предложил Д. Э. Кнут применительно к методам Монте-Карло. Однако, несмотря на получаемые количественные показатели качества последовательностей, в трактовке окончательного результата допускалась неопределенность.

Формирование пакета (набора, батареи) статистических тестов сделало возможным международное распространение методов сопоставительного исследования качества случайных и псевдослучайных последовательностей. Наиболее известные и апробированные в мировой практике тестовые наборы – NIST и DIEHARD. Они состоят из отдельных, не связанных между собой статистических критериев определения качества случайности в формально корректной и математически обоснованной постановке. Однако имеется часть тестов, лишенная научной строгости оформления и интерпретации результата. Это, например, тесты «Дни рождений», «Обезьяньи тесты», «Тест на парковку» и другие, ситуативно сформулированные и нацеленные на общий результат лишь косвенно. Отсутствие минимально достаточного наполнения тестовыми процедурами послужило причиной дальнейшего появления аналогичных пакетов таких, как TestU01, RaBiGeTe, PractRand, CRYPT-X, Тест «Стопка книг». Судя по публикациям, процесс создания средств оценки случайности еще далек от завершения.

Описанные пакеты тестов для криптографических приложений, а также алгоритмы Д.Э. Кнута, настроены на простейшие формы проявления идеальной случайности через равномерный закон распределения и отсутствия корреляционных связей между элементами последовательности. Несмотря на наибольшее распространение и использование этого типа случайности, в задачах имитационного моделирования они составляют только первый этап формирования внешних воздействий. Окончательно имитацию внешней среды реализуют через трансформации равномерного закона и независимых расположений элементов имитирующих последовательностей в требуемые формы закона распределения вероятностей и автокорреляционной функции. В отношении таких последовательностей указанные тесты неприменимы.

В фундаментальных трудах таких основоположников математической статистики как К. Пирсон и А.Н. Колмогоров содержатся базисные принципы построения критериев для принятия гипотез о заданных свойствах генеральной совокупности. Научная и учебная литература содержит многочисленные описания и формальные обоснования гипотез о значимой однородности. В частности, широко представлены в работах Кендалла М., Крамера Г., Тёрнера Д., Стьюарта А., Гмурмана В.Е. Дунин-Барковского И.В., Налимова, В.В. Орлова А.И., Смирнова Н.В. и др. примеры построения статистических критериев однородности последовательностей по математическому ожиданию и вероятности (моментов первого порядка), не обязательно полагая вероятностное распределение равномерным. В отношении однородности по автокорреляционным связям (моментной функции второго порядка) также допускается отклонение от схемы независимых испытаний Бернулли.

Однако известные статистические тесты однородности узко ориентированы либо только на момент первого порядка при независимых элементах выборки, либо только на автокорреляцию, как моментной функции второго порядка, чаще всего при нормальном распределении. Как правило, длина анализируемой выборки фиксируется. Отмеченные особенности реально применяемых критериев однородности не позволяют их применить в существующей постановке к имитирующим последовательностям с совместно заданными или ожидаемыми вероятностными и корреляционными свойствами при переменной длине выборок.

Таким образом, создание инструмента выявления неразличимости и по вероятности, и по автокорреляции двоичных последовательностей при заданной длине выборок актуально, так как позволит адекватно сопоставлять любые пары имитирующих воздействий по вероятностным моментам первого и второго порядков.

Объектом исследования являются методы и средства оценки статистических характеристик двоичных последовательностей.

Предметом исследования являются метод, алгоритмическое обеспечение и комплекс программ процедур критерия статистической однородности двух последовательностей на всех длинах частных выборок до заданной максимальной или критической.

Целью работы является синтез алгоритма и создание комплекса программ критерия статистической однородности двоичных последовательностей для значимого сравнения их по моментным функциям первого и второго порядков при заданных ограничениях на длину выборки.

Научная задача работы заключается в разработке и алгоритмической реализации метода оценки статистической однородности двоичных последовательностей при заданных ограничениях объема выборки.

Ввиду закрытости математической сущности, громоздкости, узкой направленности и фиксированности длин выборок, известные пакетные тесты типа NIST, DIEHARD и другие аналогичные, использовать для решения сформулированной задачи невозможно. Напротив, строгая и формально обоснованная структура разработанных в математической статистике критериев однородности вполне может быть использована для достижения поставленной цели. Для этого необходимо решить следующие подзадачи:

1) провести анализ существующих методов оценивания однородности последовательностей по вероятностным моментам. Разработать и обосновать аналитическую форму – модель – для численного метода определения эмпирической статистики критерия значимой однородности тестируемых двоичных последовательностей;

2) сформулировать метод оценивания статистической неразличимости двоичных последовательностей по вероятностному моменту заданного порядка на основе адаптации критерия значимой однородности двух частных выборок с учетом наличия зависимости элементов последовательностей и многократного испытания гипотез на всех длинах выборок, не превышающих заданного или критического значения, реализованного численным методом;

3) оценить возможность теоретического подхода к решению задачи анализа однородности двоичных последовательностей;

4) разработать численный метод в виде набора алгоритмических процедур для реализации статистических критериев однородности тестируемых последовательностей как эмпирического характера в общем случае, так и теоретического для ряда характерных примеров;

5) разработать алгоритмическое обеспечение и комплекс программ моделирования типичных псевдослучайных последовательностей для демонстрации работы критериев статистической однородности. Привести характерные примеры применения критерия однородности, как на основе эмпирических значений статистики, так и в случае теоретически вычислимого аналога этой статистики.

Методы исследований. Для решения перечисленных задач в диссертационной работе использовались: аппарат теории вероятностей и математической статистики,

методы алгоритмизации, математическое моделирование, методы разработки программного обеспечения и экспериментальные исследования.

Обоснованность и достоверность Обоснованность и достоверность определяются использованием известных положений фундаментальных наук, корректностью применяемой модели, ее адекватностью реальным объектам и процессам, совпадением теоретических результатов с данными экспериментов, экспертизами ФИПС с признанием программного обеспечения для ЭВМ.

Новизна полученных результатов заключается в следующем:

1. Разработана расчетная модель эмпирической статистики для нахождения максимальной длины выборок двух последовательностей, обладающих значимой статистической однородностью по моментам первого и второго порядков.
2. Разработан метод критериальной оценки статистической однородности двоичных последовательностей по моментным функциям первых двух порядков как модернизация известных критериев с учетом кратности испытаний гипотез для всех длин частных выборок, не превышающих заданной максимальной или критической.
3. Предложены аналитические решения критерия, позволяющие получить точные значения критических длин выборок, в пределах которых обеспечивается однородность без использования эмпирического материала частных выборок, а также получить общие теоретические выражения в виде функций от параметров последовательностей.
4. Разработаны алгоритмическое обеспечение, комплекс программ моделирования линейных и нелинейных псевдослучайных последовательностей и реализации варианта статистического критерия значимой однородности с многократной поверкой гипотез.

Теоретическая значимость работы заключается в развитии методов определения статистической неразличимости числовых последовательностей, а также формировании комплекса алгоритмических процедур, образующих критерий значимой однородности двух последовательностей на всех длинах частных выборок до заданной максимальной или критической.

Практическая ценность работы заключается в:

- разработке комплекса программ для оценки статистической однородности зависимых двоичных последовательностей на всех длинах частных выборок до заданной максимальной или критической;
- разработке программ моделирования типичных псевдослучайных последовательностей для демонстрации работы критериев статистической однородности;
- проведении пробных экспериментальных исследований случайных и псевдослучайных последовательностей на предмет их статистической однородности заданной значимости.

Публикации. Основное содержание диссертационной работы отражено в 18 печатных работах, из них 5 статей в журналах, рекомендованных ВАК РФ, 1 статья в журнале, который входит в базу данных Scopus, 3 свидетельства об официальной регистрации программы для ЭВМ, 9 работ в материалах и трудах конференций, 1 публикация на международном симпозиуме, проиндексированном в базе Scopus.

Апробация работы. Основные положения и результаты диссертационной работы докладывались и обсуждались на международных научно-практических конференциях «Наука сегодня», г. Вологда, 2015 г.; «XXII Туполевские чтения (школа молодых ученых)», г. Казань, 2015 г.; Наука сегодня: проблемы и пути решения, г. Вологда, 2016 г.; Наука сегодня: вызовы и решения, г. Вологда, 2016 г.; НТК по итогам

совместного конкурса фундаментальных исследований РФФИ – РТ, г. Казань, 2018г .; и в симпозиуме 16th IEEE East-west design & test symposium (EWDTS – 2018), г. Казань, 2018 г.

Реализация результатов работы:

- программа оценивания значимой однородности использована в выработке обоснования замены числовых последовательностей при решении задачи методом Монте-Карло по определению площадей фигур картографических объектов в ООО NEXTGIS (г. Москва, 2018 г.), что привело к экономии таких ресурсов ЭВМ, как память и время генерации элементов ПСП;

- результаты диссертационных исследований использованы в 2018 и 2019 гг. при выполнении НИР по гранту РФФИ – АН РТ №18-47-160001 «Методы, алгоритмы и технические средства формирования последовательностей вероятностно-статистической природы для математического моделирования и защиты информации»;

- результаты проведенных исследований по теме диссертации внедрены и используются в Казанском национальном исследовательском техническом университете им. А.Н. Туполева-КАИ (г. Казань, 2018 г.).

Внедрения и использования результатов диссертационной работы подтверждаются соответствующими актами.

Пути дальнейшей реализации результатов работы. Научные и практические результаты, полученные в диссертации, могут быть в дальнейшем использованы в средствах защиты информации, в имитационном моделировании, в тренажерах-симуляторах, а также в системах с широкополосной связью.

На защиту выносятся:

- модель нахождения максимальной длины выборок двух последовательностей, обладающих значимой статистической однородностью по моментам первого и второго порядков;

- двухэтапный критерий статистической однородности выборок случайных или псевдослучайных последовательностей по вероятностным моментам первого и второго порядков, реализованный численным методом;

- метод реализации критерия путем многократного испытания гипотез на всех длинах выборок, не превышающих заданного или критического значения;

- алгоритмическое обеспечение, комплекс программ моделирования псевдослучайных последовательностей и программу реализации эмпирического варианта критерия статистической однородности частных выборок двоичной последовательностей.

Структура и объем диссертации. Диссертационная работа изложена на 200 страницах машинописного текста и содержит 65 рисунков и 21 таблицу, состоит из введения, четырех глав основного текста, заключения и списка литературы из 89 наименований.

Личный вклад автора состоит в следующем:

– выполнен анализ существующих методов статистического оценивания однородности выборок случайных последовательностей на основе их типичных характеристик;

– предложена формулировка метода оценивания статистической неразличимости альтернативных последовательностей на основе существующих критериев значимой однородности;

– разработан способ критериальной оценки статистической однородности зависимых двоичных последовательностей на всех длинах частных выборок до заданной максимальной или критической;

– разработано алгоритмическое обеспечение и комплекс программ критерия статистической однородности двоичных последовательностей;

– проведены экспериментальные исследования на характерных примерах применения критерия однородности, а также исследования псевдослучайных последовательностей, использующихся для определения площадей фигур картографических объектов методом Монте-Карло, для ООО NEXTGIS, сделаны выводы.

Диссертация соответствует паспорту специальности 05.13.18 «Математическое моделирование, численные методы и комплексы программ» по пунктам:

3. Разработка, обоснование и тестирование эффективных вычислительных методов с применением современных компьютерных технологий.

4. Реализация эффективных численных методов и алгоритмов в виде комплексов проблемно-ориентированных программ для проведения вычислительного эксперимента.

7. Разработка новых математических методов и алгоритмов интерпретации натурного эксперимента на основе его математической модели.

8. Разработка систем компьютерного и имитационного моделирования.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертации, формулируются объект, предмет, цель и задача исследования, отмечены методы исследования, достоверность и новизна полученных результатов, их теоретическая значимость и практическая ценность, приведены данные о публикациях, апробации и реализации результатов, сформулированы научные положения, выносимые на защиту. Приведены данные о структуре и объеме диссертации, дается краткий обзор диссертации по главам.

В первой главе произведен анализ предметной области. Рассмотрены основные подходы к определению однородности выборок. Рассмотрены классические подходы к интервальному оцениванию, произведен обзор методов статистического оценивания однородности параметров нескольких случайных функций. Произведен анализ статистических характеристик типичных случайных и псевдослучайных последовательностей, их восприятие имитационной моделью в условиях малых выборок, а также предложены формулировки метода оценивания статистической неразличимости альтернативных последовательностей на основе существующих критериев значимой однородности.

Для двоичных последовательностей, стационарных в широком смысле, достаточно, например, воспользоваться в качестве начального момента первого порядка вероятностью появления единицы, а второго порядка – вероятностью появления двух единиц, разнесенных интервалом времени τ. Первое представление соответствует математическому ожиданию, а второе вместе с первым – корреляционной функции от аргумента τ. Следовательно, выбор параметров критериального поиска статистической однородности в любом смысле можно свести к набору соответствующих вероятностей.

Назовем случайную последовательность, удовлетворяющую условиям имитационного эксперимента, базовой (БП), а претендента на эквивалентную обозначим как альтернативную (АП). Двоичные последовательности признаются статистически однородными, если дисперсионный разброс оценок выбранных вероятностей не позво-

ляет их значимо различить как на заданной длине частных выборок, так и на всех предыдущих меньших.

Признаком отличия ПСП как моментом первого порядка является математические ожидания БП и АП. Фактом значимого отличия является возможность статистически наблюдать оригинальные вероятностные свойства по моментам первого и второго порядков каждой последовательности. Существующие классические критерии проверки гипотез о виде распределения или однородности выборок использовать для решения данной задачи нельзя ввиду невозможности аппроксимации реального распределения практически апробированными распределениями по генеральной выборке, а также ввиду наличия внутренних зависимостей исходных исследуемых выборок.

Эти зависимости подразумевают создание нового двухэтапного критерия, основная часть которого – сравнение исследуемых выборок на предмет схожести по моментам первого порядка, а дополнительная часть – по моментам второго порядка с использованием в качестве «калибровки» функцию СКО оценок АКФ, определяющей внутренние зависимости ПСП.

Во второй главе рассмотрены основные подходы к формированию общего вида критерия значимой однородности ПСП. Постановка критерия определяется задачей нахождения максимальной длины двоичных последовательностей <*a*> и <*b*>при условии их статистической однородности с заданным уровнем значимости α. Пусть a_i, $b_i \in \{0, 1\}$ – элементы этих последовательностей, <*a*> – БП, удовлетворяющая условиям имитационной модели; <*b*> – заданная тестируемая АП. В общем случае элементы последовательностей зависимы, что выражается необходимой для имитационной модели формой АКФ.

Признак однородности – это математические ожидания P и $\widetilde{P}$ БП и АП, соответственно. В качестве признака однородности выберем средние значения последовательностей, которые при указанном двоичном алфавите совпадают со средней частотой появления символа 1. На генеральных выборках они представляются вероятностями P_a и P_b, где индексы обозначают принадлежность к соответствующей последовательности. Основная независимая переменная, максимальное значение которой надо найти, n – длина частной выборки, заданная независимо от периодических свойств БП и АП. Глубина корреляционного анализа по аргументу сдвига τ_{max}. Величина n_{max}ограничивает n в тестовом эксперименте ($n = \overline{1, n_{max}}$). Заданный уровень значимости критерия α – вероятность ошибки первого рода. Для выборок, состоящих из зависимых элементов, тестируемым параметром однородности служит автокорреляционная функция АКФ. В общем случае для двух выборок, в том числе и зависимых, определение их однородности по математическому ожиданию можно осуществить на основе статистики, пропорциональной эмпирическому расхождению средних значений обеих последовательностей и обратно пропорциональной стандартному отклонению этих расхождений вида

$$t_{эмп} = \frac{M^*[\Delta P^*]}{\sqrt{D_{\Delta P^*}}}, \qquad (1)$$

где $\Delta P^* = P_a^* - P_b^*$ и $D_{\Delta P^*}$ – разности средних значений и дисперсия этой разности.

Завершается процедура одной итерации статистического критерия однородности сравнением полученной эмпирической статистики $t_{эмп}$ с критическими значениями $t_{кр}(\alpha)$ на основании принятия подходящего закона распределения случайных величин ΔP^* и уровня значимости α. Тогда

$$\text{если}\quad t_{\text{эмп}}\begin{cases} < t_{\text{кр}}(\alpha), \text{ то } \mathrm{H}_0, \\ \geq t_{\text{кр}}(\alpha), \text{ то } \mathrm{H}_1, \end{cases} \tag{2}$$

где H_0 – принятие нуль-гипотезы об однородности с вероятностью ошибки α; H_1 – отклонение H_0, т.е. принятие альтернативной гипотезы о неоднородности.

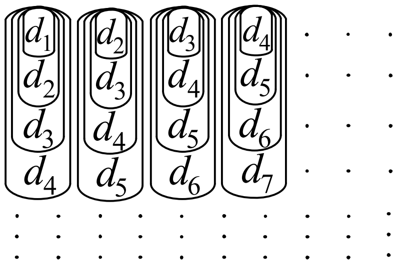
В предлагаемой постановке задачи анализа однородности необходимо проследить на заданном уровне значимости α многократные факты принятия нуль-гипотезы H_0 при всех значениях n от 1 до $n_{\text{кр}}$, где $n_{\text{кр}} \leq n_{\max}$. Полученная величина $n_{\text{кр}} - 1$ характеризует размерность имитационной модели в отношении использования данной имитирующей последовательности.

При традиционном статистическом подходе рабочие для (1) признаки однородности по математическому ожиданию выражены для обеих двоичных последовательностей оценками P_a^* и P_b^*, придающих статистике эмпирический характер. Тогда все компоненты выражения (1) находятся численными методами математической статистики на основании заданных для испытания на однородность частных выборок последовательностей <*a*> и <*b*>.

Пусть <*d*> = <*a*> – <*b*>. Тогда образуем из выборки

$$d_1\, d_2\, d_3 \ldots d_j \ldots d_N, \tag{3}$$

полученной разностной последовательности <*d*> множества D_n в количестве $n_{\max}$, состоящие из N_0 частных выборок по n элементов согласно следующей схеме (фрагмент из начальных элементов $d_1 \ldots d_7$):



Тогда

$$D_1 = \{(d_1), (d_2), (d_3), (d_4), \ldots, (d_{N_0})\},$$
$$D_2 = \{(d_1 d_2), (d_2 d_3), (d_3 d_4), (d_4 d_5), \ldots, (d_{N_0} d_{N_0+1})\},$$
$$D_3 = \{(d_1 d_2 d_3), (d_2 d_3 d_4), (d_3 d_4 d_5), (d_4 d_5 d_6), \ldots, (d_{N_0} d_{N_0+1} d_{N_0+2})\},$$
$$D_4 = \{(d_1 d_2 d_3 d_4), (d_2 d_3 d_4 d_5), (d_3 d_4 d_5 d_6), (d_4 d_5 d_6 d_7), \ldots, (d_{N_0} d_{N_0+1} d_{N_0+2} d_{N_0+3})\},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots ,$$
$$D_{n_{\max}} = \{(d_1 d_2 d_3 \ldots d_{n_{\max}}), (d_2 d_3 d_4 \ldots d_{n_{\max}+1}), (d_3 d_4 d_5 \ldots d_{n_{\max}+2}), \ldots, (d_{N_0} d_{N_0+1} d_{N_0+2} \ldots d_{N_0+n_{\max}-1})\}.$$

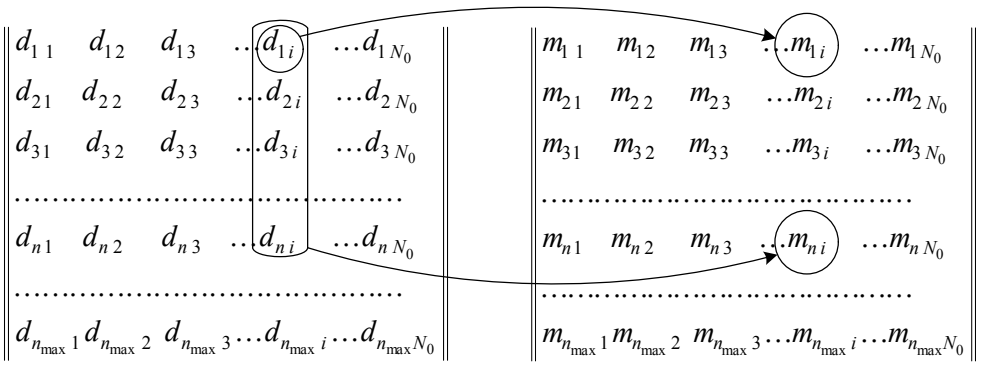
Для полного использования заданной выборки необходимо обеспечить

$$N = N_0 + n_{\max} - 1. \tag{4}$$

Из алгоритмических соображений реализации описанной схемы заданную выборку (3) представим матрицей $n_{\max} \times N_0$:

$$\left\|\begin{matrix} d_1 & d_2 & d_3 & \dots & d_i & \dots & d_{N_0} \\ d_2 & d_3 & d_4 & \dots & d_{i+1} & \dots & d_{N_0+1} \\ d_3 & d_4 & d_5 & \dots & d_{i+2} & \dots & d_{N_0+2} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ d_n & d_{n+1} & d_{n+2} & \dots & d_{i+n-1} & \dots & d_{N_0+n-1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ d_{n_{\max}} & d_{n_{\max}+1} & d_{n_{\max}+2} & \dots & d_{i+n_{\max}-1} & \dots & d_N \end{matrix}\right\| \Rightarrow \left\|d_{ni}\right\| = \left\|\begin{matrix} d_{11} & d_{12} & d_{13} & \dots d_{1i} & \dots d_{1N_0} \\ d_{21} & d_{22} & d_{23} & \dots d_{2i} & \dots d_{2N_0} \\ d_{31} & d_{32} & d_{33} & \dots d_{3i} & \dots d_{3N_0} \\ \dots & \dots & \dots & \dots & \dots \\ d_{n1} & d_{n2} & d_{n3} & \dots d_{ni} & \dots d_{nN_0} \\ \dots & \dots & \dots & \dots & \dots \\ d_{n_{\max}1} & d_{n_{\max}2} & d_{n_{\max}3} & \dots d_{n_{\max}i} & \dots d_{n_{\max}N_0} \end{matrix}\right\| \quad (5)$$

Образуя суммы вида $m_{ni} = \sum_{h=1}^{n} d_{hi}$, нетрудно выразить оценки погрешности совпадения по вероятности $\Delta P_i^* = P_i^* - \widetilde{P}_i^* = m_{ni}/n$ для каждого $n = \overline{1, n_{\max}}$. Слагаемыми в сумме являются элементы частных выборок длиной *n*. В качестве примера для m_{1i} и m_{ni}, связь этих сумм с элементами матрицы $||d_{ni}||$ как слагаемыми показана на следующей схеме:



(6)

Обозначим матрицу сумм $||m_{ni}||$.

Несмотря на то, что величины *P* и $\widetilde{P}$ являются непрерывными, их оценки P_i^* и $\widetilde{P}_i^*$, строго говоря, при конечном *n* дискретны. Дискретной является и их разность ΔP_i^* как оценка абсолютной погрешности совпадения вероятностей, которую в усредненном виде $\overline{\Delta P^*}$ удобно использовать в роли функции различия (неоднородности) в числителе формулы статистики (1) $\overline{M}_{m_d}$. Дробно-рациональные значения перечисленных оценок определяются алфавитом $d_{ni} \in \{-1, 0, 1\}$, формирующим алфавит $m_n \in \{-n, -(n-1), ..., 0, (n-1), n\}$ независимо от эмпирических данных.

Однако для выражения знаменателя этой статистики через дисперсию D_{m_d} в большинстве практических случаев достаточных аналитических оснований найти не удается. Ограничимся заменой дисперсии на ее оценку $\overline{D}_{m_d}$, превращающую знаменатель (1) также в эмпирическую функцию. Рабочий вариант критериальной статистики представим в следующей форме:

$$t_{\text{эмп}} = \frac{\overline{M}_{m_d}}{\sqrt{\overline{D}_{m_d}}}. \quad (7)$$

Возможность выполнения нуль-гипотезы H_0 реализуется при несмещенном от нуля математическом ожидании числителя. Если выполнено аналогичное требование к знаменателю через исправленную выборочную дисперсию в виде

$$\overline{D}_{m_d} = \frac{N_0}{N_0 - 1} D_{m_d}^*, \quad (8)$$

то эта статистика входит в класс методов статистической проверки гипотез по критерию Стьюдента.

Закон распределения последовательностей на выборках, не кратных периоду, однозначно определить нельзя. Типичный подход в известных конструкциях критериев безальтернативно подразумевает применение критерия Стьюдента при неизвестной дисперсии оценки числителя критерия.

В процессе проведения тестовых испытаний каждое значение аргумента n предполагает фактическое формирование нескольких одинаковых сумм m_n.Число таких сумм обозначим ν_{m_n}, для которого справедливо равенство $\sum_{m_n=-n}^{n} \nu_{m_n} = N_0$.

Количественное распределение

$$\left\langle \nu_{m_n} \,\middle|\, m_n = \overline{-n, n} \right\rangle \text{ для каждого } n = \overline{1, n_{\max}} \qquad (9)$$

представлено в общей форме в табл. 1.

Численные значения средней разности и выборочной оценки ее дисперсии выражаются через усреднения сумм частных выборок. Как функции от n они представлены в табл. 2 эквивалентными математическими формулами на основе элементов матрицы $||m_{ni}||$ и табл. 1. Выбор конкретной вычислительной формулы производится с учетом алгоритмических предпочтений при программной реализации критерия.

Таблица 1

Общий вид количественного распределения сумм элементов частных выборок

ν_{m_n}	ν_{-n}	ν_{-n+1}	…	ν_{-1}	ν_0	ν_1	…	ν_{n-1}	ν_n
m_n	$-n$	$-n+1$	…	-1	0	1	…	$n-1$	n

Таблица 2

Варианты выборочной средней разности и оценки ее дисперсии

Выборочные оценки	**По строкам матрицы $\|\|m_{ni}\|\|$**	**По табл. 1**
$\overline{M}_{m_d}(n)$	$\frac{1}{N_0}\sum_{i=1}^{N_0} m_{ni}$	$\frac{1}{N_0}\sum_{m_n=-n}^{n} m_n \nu_{m_n}$
$D^*_{m_d}(n)$	$\frac{1}{N_0}\sum_{i=1}^{N_0}\left[m_{ni} - \overline{M}_{m_d}(n)\right]^2$	$\frac{1}{N_0}\sum_{m_n=-n}^{n}\left[m_n - \overline{M}_{m_d}(n)\right]^2 \nu_{m_n}$
$D^*_{m_d}(n) = \overline{\alpha}_2(n) - \overline{M}^2_{m_d}(n)$	$\overline{\alpha}_2(n) = \frac{1}{N_0}\sum_{i=1}^{N_0} m_{ni}^2$	$\overline{\alpha}_2(n) = \frac{1}{N_0}\sum_{m_n=-n}^{n} m_n^2 \nu_{m_n}$

С учетом (8) расчетная модель эмпирической статистики по вероятности (7) примет вид:

$$t_{\text{эмп}}(n) = \overline{M}_{m_d}(n)\sqrt{\frac{N_0 - 1}{N_0 D^*_{m_d}(n)}}.$$

Используя элементы матрицы $||m_{ni}||$ и запись выборочной оценки дисперсии через оценку второго начального момента $\overline{\alpha}_2(n)$, получаем расчетную формулу статистики, выражающую случайную величину для сравнения с границами двусторонней критической области:

$$t_{\text{эмп}}(n)=\frac{\sum\limits_{i=1}^{N_0} m_{ni}}{\sqrt{\dfrac{N_0}{N_0-1}\left[N_0\sum\limits_{i=1}^{N_0} m_{ni}^2-\left(\sum\limits_{i=1}^{N_0} m_{ni}\right)^2\right]}}=\frac{\Sigma_m}{\sqrt{\dfrac{N_0}{N_0-1}\left[N_0\,\Sigma_{m^2}-\Sigma_m^2\right]}}. \qquad (10)$$

Математически эквивалентную форму статистики также можно получить на основе распределения (9) по табл. 1 через переменные m_n и ν_{m_n}.

Цепочка алгоритмических процедур в общей постановке образует численный метод нахождения максимальной длины выборок двух последовательностей, обладающих значимой статистической однородностью по вероятности:

$$\left.\begin{array}{l}
\alpha,\ n_{\max},\ N_0,\ N,<a>,<b>\Rightarrow\\
<a>-<b>=<d>\Rightarrow\\
\|d_{ni}\|\Rightarrow\\
\|m_{ni}\|\Rightarrow\\
\Sigma_m,\Sigma_{m^2},\Sigma_m^2\Rightarrow\\
\begin{cases}|t_{\text{эмп}}|<t_{\text{кр}},\mathrm{H}_0,\ \max\lfloor n(|t_{\text{эмп}}|<t_{\text{кр}})\rfloor=n_{\text{кр}},\\ |t_{\text{эмп}}|\ge t_{\text{кр}},\mathrm{H}_1,\ n=\overline{1,n_{\max}}.\end{cases}
\end{array}\right\}, \qquad (11)$$

где $\Sigma_m=\sum\limits_{i=1}^{N_0} m_{ni}$, $\Sigma_{m^2}=\sum\limits_{i=1}^{N_0} m_{ni}^2$ и $\Sigma_m^2=\left(\sum\limits_{i=1}^{N_0} m_{ni}\right)^2$ – целочисленные переменные, образованные элементами матрицы $\|m_{ni}\|$ и представляющие в (11) исходные переменные $M^*_{\Delta P^*}(n)$, $\alpha_2^*[\Delta P^*(n)]$ и $M^{*2}_{\Delta P^*}(n)$ из таблицы 2 соответственно;

$\lfloor\bullet\rfloor$ – целое $\bullet$, если иначе, то ближайшее к $\bullet$ меньшее целое.

Вероятностное распределение $\Delta P^*(n)$ основано на оценках

$$\mathbf{P}^*\left\{\Delta P^*(n)=\frac{\hat m_{nj}}{n}\right\}=\frac{\hat\nu_{m_{nj}}}{N_0}, \qquad (12)$$

Возможно упростить обозначения этих параметров в виде

$$\mathbf{P}^*\left\{\Delta P^*(n)=\frac{\hat m_{nj}}{n}\right\}=\mathbf{P}^*\left\{m_n=\hat m_{nj}\right\}=\mathbf{P}^*_{nj}$$

для всех $j=\overline{1,r_n}$. Также справедлива нормировка $\sum\limits_{j=1}^{r_n}\mathbf{P}^*_{nj}=1$ для каждого $n=\overline{1,n_{\max}}$.

Расчетная модель эмпирической статистики по корреляции имеет вид:

$$t_{\text{эмп}}(n)=\overline{M}_{m_{d_\tau}}(n)\sqrt{\frac{N_0-1}{N_0 D^*_{m_{d_\tau}}(n)}}. \qquad (13)$$

Цепочка алгоритмических процедур, схожих с (11) в общей постановке, но относящихся к сдвиговой последовательности $<d>_{\tau=1}=<a>_{\tau=1}-<b>_{\tau=1}$, образует численный метод нахождения максимальной длины выборок двух последовательностей, обладающих значимой статистической однородностью по корреляции.

В третьей главе представлены введение в аналитический подход к решению задач однородности ПСП, фактор конечности апериодической выборки и экономия ре-

сурсов аппаратного построения ГПСП на примере двух М-последовательностей разных порядков:

Тестируются две М-последовательности. Длинная основная (исходная), порядка $l_2 = 10$. Короткие альтернативные с $l_1 = \overline{2,\ 10}$. Общая формула теоретического аналога статистики

$$t = \frac{\left(2^{l_2-1} - 2^{l_1-1}\right)n}{\sqrt{2^{l_1-2} n_1 \left(2^{l_1} - 1 - n_1\right)\left(2^{l_2} - 1\right)^2 + 2^{l_2-2} n_2 \left(2^{l_2} - 1 - n_2\right)\left(2^{l_1} - 1\right)^2}},$$

где $n_1 = n \bmod \left(2^{l_1} - 1\right)$ и $n_2 = n \bmod \left(2^{l_2} - 1\right)$.

Разрешить эту формулу относительно *n* невозможно из-за сложной трансцендентной формы. Представляет интерес обзорный анализ выражения при условии многопериодического режима работы альтернативного ГПСП в пределах первого периода длинной последовательности. Для этого примем $n_2 = n$ при одном значении $n_1 = 2^{l_1} - 1$ в каждом коротком цикле в пределах первого периода исходной длинной последовательности.

Нетрудно заметить, что левое слагаемое подкоренного выражения в знаменателе вырождается в ноль, так как $\left(2^{l_1} - 1 - n_1\right) = 0$. Тогда формула значительно упрощается, а именно:

$$t = \frac{\left(2^{l_2-1} - 2^{l-1}\right)\sqrt{n}}{\sqrt{2^{l_2-2}\left(2^{l_2} - 1 - n\right)\left(2^{l} - 1\right)^2}},$$

где обозначено $l_1 = l$. Разрешив полученную формулу относительно *n*, получим

$$n = \frac{2^{l_2-2}\left(2^{l_2} - 1\right)\left(2^{l} - 1\right)^2 t^2}{\left(2^{l_2-1} - 2^{l-1}\right)^2 + 2^{l_2-2}\left(2^{l} - 1\right)^2 t^2},$$

для счета по которой положим $\left(2^{l_2} - 1\right) = 1023$, $l = \overline{2,\ 10}$ и $t = 2$. Применяя эти данные, получим расчетную формулу для критического значения границы однородности:

$$n = \frac{1047552\left(2^{l} - 1\right)^2}{\left(512 - 2^{l-1}\right)^2 + 1024\left(2^{l} - 1\right)^2}.$$

Результаты представлены в табл. 3.

Таблица 3

Расчетные данные по примеру тестирования двух М-последовательностей

l	1	2	3	4	5	6	7	8	9	10
$\frac{l}{l_2}100\%$	10	20	30	40	50	60	70	80	90	100
n	3,996	35,007	166,53	486,56	818,40	968,118	1010,72	1020,739	1022,749	1023
$\lfloor n \rfloor$	3	35	166	486	818	968	1010	1020	1022	1023
$\frac{n}{n_{\max}}100\%$	0,4	3,4	16,3	47,6	80,0	94,6	98,8	99,8	99,98	100
$\frac{l_2 - l}{l_2}100\%$	90	80	70	60	50	40	30	20	10	0

Эффект экономии ячеек регистровой памяти в альтернативном генераторе МП порядка *l* относительно исходного генератора порядка l_2

$$\frac{l_2 - l}{l_2} 100\%, \qquad (12)$$

где $l_2 \geq l$.

Интервал однородности n (в действительных числах) двух МП относительно длины периода $n_{\max}$ исходной МП (в примере $n_{\max} = 1023$):

$$\frac{n}{n_{\max}} 100\% . \qquad (13)$$

При этом $\lfloor n \rfloor$ − критическое значение целочисленной границы однородности.

Основной аргумент графического представления функций экономии и интервала однородности в относительной форме

$$\frac{l}{l_2} 100\% . \qquad (14)$$

На рис.1. графически представлены функции эффективности минимизации за счет использования фактора конечности выборки.

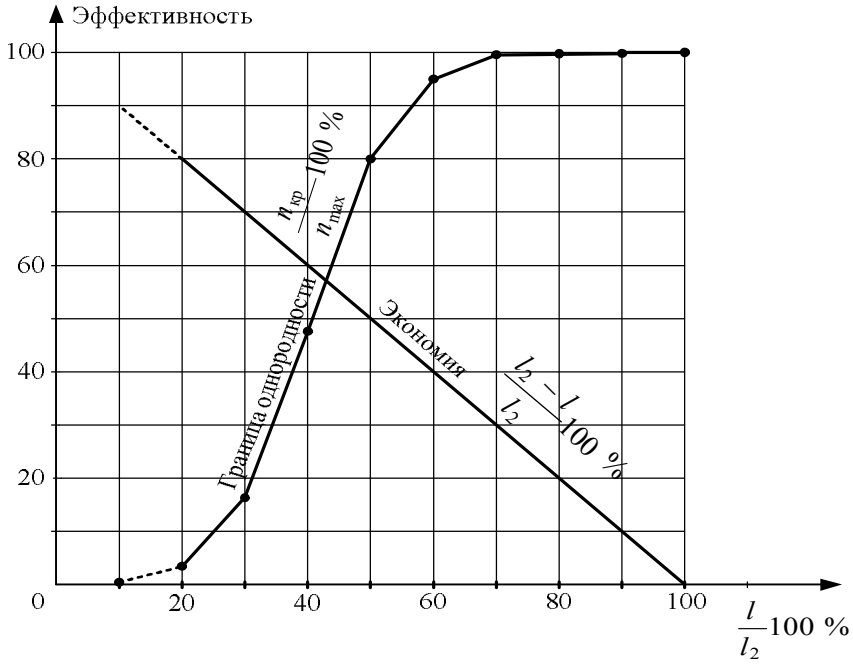


Рис. 1. Функция эффективности минимизации

Пример. Требуется обеспечить значимую однородность тестируемых М-последовательностей в пределах 95% длины периода исходной последовательности (13). Для этого необходимо затратить 63% ресурсов исходного генератора (14), что составит 37% экономии (12).

В четвертой главе описывается разработанное алгоритмическое обеспечение и комплекс программ предложенного в диссертации критерия, а также ряд вспомогательных программных продуктов, необходимых для построения программного комплекса и организации его работы.

В процессе написания данной диссертационной работы были разработаны следующие комплекса программ:

Pseudo Random Number Generator (Element Base) – это комплекс программ,

позволяющий сгенерировать последовательность по физической (схемотехнической) реализации генератора.

Размещая элементы генератора на рабочей области системы и подключая их между собой соединениями, пользователь получает рабочую схему, с выводов которой считываются логические значения сигналов, которые и формируют последовательность. В дальнейшем, эта последовательность может быть подвергнута корреляционному анализу или критериальному.

Distributions Criteria For Difference – комплекс программ (рис. 2), позволяющий проводить исследования критериальных зон псевдослучайных последовательностей, а также делать выводы о принятии гипотез H_0 и H_1 о статистической неразличимости и различимости эмпирических характеристик псевдослучайных последовательностей.

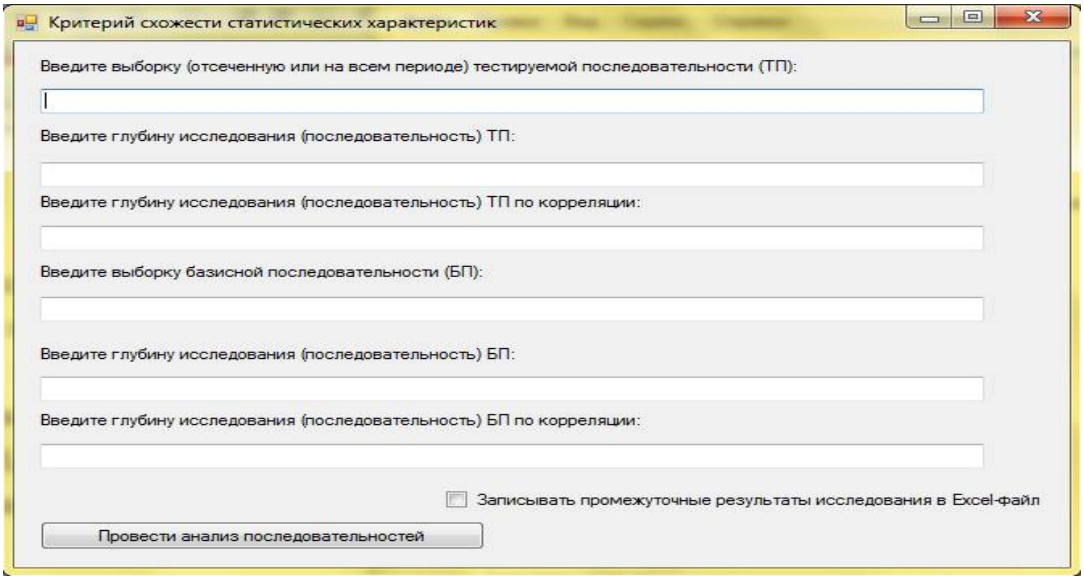


Рис. 2. Интерфейс системы Distributions Criteria For Difference

Sequences Creating – ПО, позволяющее сгенерировать последовательность по «маске» генератора, которая строится на основе характеристического многочлена последовательности.

Эта система создания последовательностей была написана в целях экономии времени для сборки многоразрядных схем генераторов, количество элементов которых превышает сотню.

Pseudo Random Number Generator (Analysis) – комплекс программ, позволяющий проводить корреляционный анализ, то есть получать значения и строить графики корреляционных функций ПСП, их дисперсий и СКО, как на всей величине периода, так и в апериодическом режиме, рассматривая только отдельную часть последовательности.

Raspredelenie – ПО, позволяющее вычислять значения асимметрии и эксцесса для всех длин выборки, начиная от единички и вплоть до периода. Вычисление данных параметров ПСП проводилось для уточнения теоретического закона распределения, с целью последующей аппроксимации им эмпирических законов распределения исследуемых последовательностей.

Выходные данные записываются системой в созданный предварительно Excel-файл в виде таблиц.

Результаты работы программы записываются в виде таблиц в Excel-файл, где можно в последующем произвести оценку критических зон схожести последовательностей, а также построить графики для большей наглядности экспериментальных

данных.

В заключении формулируются выводы и приводится перечень основных результатов, полученных в диссертационной работе.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В диссертационной работе решена актуальная научная задача алгоритмической реализации методов оценки статистической однородности двоичных последовательностей при заданных ограничениях объема выборки, имеющая значение для развития математического моделирования и защиты информации.

1. Проведен анализ существующих методов оценивания однородности последовательностей по вероятностным моментам. Разработана и обоснована аналитическая форма – модель – для численного метода определения эмпирической статистики, как критерия значимой однородности тестируемых двоичных последовательностей.

2. Сформулирован метод оценивания статистической неразличимости двоичных последовательностей по вероятностному моменту заданного порядка на основе адаптации критерия значимой однородности двух частных выборок с учетом наличия зависимости элементов последовательностей и многократного испытания гипотез на всех длинах выборок, не превышающих заданного или критического значения, реализованного численным методом.

3. Произведена оценка возможности теоретического подхода к решению задачи анализа однородности двоичных последовательностей. Путем исследований выявлено, что подход работает не на всех классах псевдослучайных последовательностей. Так как количество различных корреляционных пиков (М-3)–последовательности невозможно выразить через величину выборки *n,* аналитический метод решения задачи анализа однородности ПСП для данного класса последовательностей не подходит.

4. Разработан численный метод в виде набора алгоритмических процедур для реализации статистических критериев однородности тестируемых последовательностей как эмпирического характера в общем случае, так и теоретического для ряда характерных примеров.

5. Разработано алгоритмическое обеспечение и комплекс программ моделирования типичных псевдослучайных последовательностей для демонстрации работы критериев статистической однородности. Приведены характерные примеры применения критерия однородности, как на основе эмпирических значений статистики, так и в случае теоретически вычислимого аналога этой статистики.

Основные результаты диссертации опубликованы в следующих работах:

Статьи в журналах из списка, рекомендованного ВАК РФ

1. Кузнецов, В.М. Статистическая неразличимость шумоподобных сигналов при имитационном моделировании на малых выборках. Бернуллиевские последовательности/ В.М. Кузнецов, В.А. Песошин, Д.В. Ширшова// Вестник КГТУ им. А.Н. Туполева, – 2016. – №3. – С. 122-127.

2. Кузнецов, В.М. Статистическая неразличимость шумоподобных сигналов при имитационном моделировании на малых выборках. Случайные последовательности с внутренними связями/ В.М. Кузнецов, В.А. Песошин, Д.В. Ширшова// Вестник КГТУ им. А.Н. Туполева. – 2017. – №1. – С. 141-147.

3. Кузнецов, В.М. Статистическая неразличимость шумоподобных сигналов при имитационном моделировании на малых выборках для псевдослучайных последова-

тельностей/ В.М. Кузнецов, В.А. Песошин, Д.В. Ширшова// Вестник КГТУ им. А.Н. Туполева, – 2017.– №3. – С. 97-104.

4. Ширшова, Д.В. Критерий значимой однородности двоичных последовательностей / Д.В. Ширшова// Вестник Чувашского университета, – 2018.– №3. – С. 120-132.

Публикации в изданиях, входящих в базу данных Scopus

5. Pesoshin, V.A. Generators of the equiprobable pseudorandom nonmaximal-length sequences based on linear-feedback shift registers / V.A. Pesoshin, V.M. Kuznetsov, D.V. Shirshova //Automation and remote control.– 2016.– Vol. 77, No 9. – p. 1622-1632.

Объекты интеллектуальной собственности

6. Свидетельство № 2015614945 о государственной регистрации программы для ЭВМ. Программа моделирования аппаратных генераторов псевдослучайных последовательностей в апериодическом режиме Pseudo random Number Generator/ Д.В. Ширшова – Зарег. в Реестре программ для ЭВМ 30.04.2015.

7. Свидетельство № 2017610987 о государственной регистрации программы для ЭВМ. Программа статистического критерия сходства двоичных последовательностей по вероятности и автокорреляции на основе разности эмпирических вероятностных моментов Distributions' Criteria/ Д.В. Ширшова – Зарег. в Реестре программ для ЭВМ 19.01.2017.

8. Свидетельство № 2017661222 о государственной регистрации программы для ЭВМ. Программа статистического критерия сходства псевдослучайных последовательностей по вероятности и автокорреляции на основе разности их двоичных представлений Distribution's Criteria For Difference Of Two Binary Sequences/ Д.В. Ширшова – Зарег. в Реестре программ для ЭВМ 06.10.2017.

Материалы конференций

9. Ширшова, Д.В. Система моделирования генераторов псевдослучайных чисел и псевдослучайных последовательностей/ Д.В. Ширшова // VI Камские чтения: сборник докладов всероссийской научно-практической конференции студентов, аспирантов и молодых ученых, г. Н. Челны, 25 апреля 2014 г./ Набережночелнинский институт Казанского (Приволжского) федерального университета. – Н. Челны, 2014. – Ч. I. – С.129-130.

10. Ширшова, Д.В. Программная реализация алгоритмов статистических критериев согласия и значимости в задачах исследования случайных последовательностей/Д.В. Ширшова// Наука сегодня: сборник научных трудов по материалам международной научно-практической конференции, г. Вологда, 23 сентября 2015 г.: в 4 ч. Часть 1. – Вологда: ООО «Маркер», 2015.– Ч. I.– С.84-85.

11. Ширшова, Д.В. Комплекс программ для построения доверительного интервала оценки вероятности применительно к М-последовательностям/ Д.В. Ширшова/ Сборник докладов конференции XXII Туполевских чтений (Школа молодых ученых), г. Казань, 19-21 октября 2015 г. – Казань: изд-во КНИТУ-КАИ, 2015. – С. 382-386.

12. Ширшова, Д.В. Программа вычисления значений эксцесса и асимметрии для периодических последовательностей/Д.В. Ширшова//Наука сегодня: вызовы и решения: материалы международной научно-практической конференции, г. Вологда, 27 января 2016 г. – Вологда: ООО «Маркер», 2016. – С. 30-31.

13. Ширшова, Д.В. Программа получения псевдослучайных последовательностей по маске генератора /Д.В. Ширшова // Наука сегодня: вызовы и решения: материалы международной научно-практической конференции, г. Вологда, 27 января 2016 г. – Вологда: ООО «Маркер», 2016. – С. 32-33.

14. Ширшова, Д.В. Параллельная программа получения значений эксцесса для периодических последовательностей /Д.В. Ширшова// Наука сегодня: проблемы и пути решения: материалы международной научно-практической конференции, г. Вологда, 30 марта 2016 г.: в 2 ч. – Вологда: ООО «Маркер», 2016. – ч. 1. – С. 83-84.

15. Ширшова, Д.В. Параллельная программа проверки типа периодической последовательности по значениям АКФ на периоде /Д.В. Ширшова //Наука сегодня: проблемы и пути решения: материалы международной научно-практической конференции, г. Вологда, 30марта 2016 г.: в 2 частях. Часть 1. – Вологда: ООО «Маркер», 2016. С. 84-85.

16. Песошин, В.А. Теоретические основы аппаратного формирования линейных двоичных псевдослучайных последовательностей не максимальной длины / В.А. Песошин, В.М.Кузнецов, А.И. Гумиров, А.Х. Рахматуллин, Д.В. Ширшова // НТК по итогам совместного конкурса фундаментальных исследований РФФИ – РТ в 2018 г.: тезисы докладов региональной НПК. – Казань: Изд-во АН РТ, 2018. – С. 89.

17. Песошин, В.А. Теоретические основы аппаратного формирования линейных двоичных псевдослучайных последовательностей не максимальной длины / В.А. Песошин, В.М.Кузнецов, А.И. Гумиров, А.Х. Рахматуллин, Д.В. Ширшова // НТК по итогам совместного конкурса фундаментальных исследований РФФИ – РТ в 2018 г.: сборник докладов региональной НПК. – Казань: Изд-во АН РТ, 2018. – С. 397-400.

Материалы Scopus-конференции

18. Pesoshin,V.A. Generators of the binary inverse-segment pseudo-random sequences/ V.A. Pesoshin, V.M. Kuznetsov, A.I. Gumirov, D.V. Shirshova // Proseedings of IEEE East-west design & test symposium (EWDTS' – 2018).–Kazan, 2018. – p. 268-275.

Подписано в печать 03.10.19

Формат 60×84 1/16. Бумага офсетная. Печать цифровая.

Усл. печ. л. 0,93. Тираж 100 экз. Заказ Г75

Издательство КНИТУ-КАИ

420111, г. Казань, ул. К. Маркса, 10